



Communications
Security Establishment

Centre de la sécurité
des télécommunications

CANADIAN CENTRE^{FOR} **CYBER SECURITY**

Cyber security and privacy risk management series: A lifecycle approach **Security and privacy controls and assurance activities catalogue**

Practitioner

Foreword

The Security and privacy controls and assurance activities catalogue is an UNCLASSIFIED publication issued under the authority of the Head, Canadian Centre for Cyber Security (Cyber Centre).

This publication supersedes IT security risk management: A lifecycle approach (ITSG-33) Annex 3A – Security control catalogue.

For more information or to suggest amendments, reach out to our Contact Centre:

- by email: contact@cyber.gc.ca
- by telephone, toll free: [1-833-CYBER-88](tel:1-833-CYBER-88) ([1-833-292-3788](tel:1-833-292-3788))

Effective date

This publication takes effect on March 31, 2026

Revision history

Revision	Amendments	Date
1	First release.	March 31, 2026

D97-3/10-033-2026E-PDF
ISBN 978-0-660-76132-9

Overview

To ensure a common baseline approach to risk management with the United States (US), the controls and assurance activities described in this publication align with [National Institute of Standards and Technology \(NIST\) Special Publication \(SP\) 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations](#). This enables us to adopt standards such as the US Committee on National Security Systems (CNSS) overlays on Canadian national security systems. This publication is an adapted version of NIST SP 800-53, reflecting Canadian unique business and legislative requirements. Sections 1 and 2 highlight the main differences between both publications.

This publication is part of a series of guidelines published by the Cyber Centre, under “Cyber security and privacy risk management: A lifecycle approach.” It contains definitions of assurance activities and controls for systems and organizations that practitioners can use as a foundation for selecting, tailoring and allocating controls and assurance activities to manage cyber security and privacy risks. Implementing a comprehensive set of security and privacy controls and assurance activities can help organizations achieve their business activities.

This publication has been created as a tool to assist security and privacy practitioners in their efforts to protect systems in compliance with applicable legislation, policies, directives and standards.

Organizational cyber security and privacy risk management activities (ITSP.10.036) and System lifecycle cyber security and privacy risk management activities (ITSP.10.037) provide guidance on how to use this catalogue to adequately select, tailor and implement controls and assurance activities at the organizational and system level, respectively.

Revision changes

The following items describe the main changes in the Cyber security and privacy risk management: A lifecycle approach series:

- Addition of privacy elements: due to permutations in the relationship between cyber security and privacy program objectives and risk management, there is a need for close collaboration between those programs
- Scope of the audience: now addressing critical infrastructures in addition to Government of Canada (GC)

Specifically, in ITSP.10.033, changes are as follows:

- Alignment with NIST SP 800-53 Rev. 5 (formerly Rev. 4)
- Addition of privacy and privacy-related controls and assurance activities
- Addition of new families:
 - PM: Program Management
 - PT: Personal Information and Transparency
 - SR: Supply Chain Risk Management
- If applicable, the discussion section is divided into a general discussion and a GC discussion. GC discussion is specifically directed to a GC audience as it addresses requirements derived from laws, policies, directives, and standards that GC departments and agencies need to comply with
- All Canadian-specific security and privacy controls, activities or enhancements that previously started at 100 now start at 400 (e.g., SA-400, IA-04(400)). This change was made to avoid collision with NIST enhancements as some of them were getting close to 100
- We refer to assurance-related “controls” as activities, rather than controls

Acknowledgments

The Cyber Centre wishes to acknowledge and thank Dr. Ron Ross and Victoria Pillitteri from the Computer Security Division at NIST for allowing the Cyber Security Guidance (CSG) team to use the [NIST 800-53 Rev 5](#) control catalogue and modify it to the Canadian context.

We also want to acknowledge the continuous support provided by the Security Management and Governance Privacy Assessment (SMGPA) team at Shared Services Canada, especially for their significant contributions on the privacy aspects which have been instrumental in the completion of this project.

Furthermore, we would like to thank those who contributed to this project in various capacities: Treasury Board of Canada Secretariat and various Cyber Centre teams.

Table of contents

1. Introduction	17
Purpose	18
Scope and applicability.....	18
Audience.....	18
Publication taxonomy	19
Publication organization	19
2. Concepts and structure.....	21
Requirements, controls, and activities	21
Controls	21
Assurance activities.....	21
Controls and assurance activities, structure, and organization	21
Implementation approaches	26
Security and privacy controls and assurance activities.....	27
Robustness	27
3. The controls and assurance activities	29
Family: Access control	30
AC-01 Access control policy and procedures	30
AC-02 Account management.....	31
AC-03 Access enforcement.....	35
AC-04 Information flow enforcement.....	40
AC-05 Separation of duties	48
AC-06 Least privilege.....	48
AC-07 Unsuccessful logon attempts.....	51
AC-08 System use notification	52
AC-09 Previous logon notification	53
AC-10 Concurrent session control	54
AC-11 Device lock	55
AC-12 Session termination.....	55
AC-13 Supervision and review – access control.....	56
AC-14 Permitted actions without identification or authentication.....	56
AC-15 Automated marking	57
AC-16 Security and privacy attributes	57
AC-17 Remote access.....	60

AC-18 Wireless access	63
AC-19 Access control for mobile devices	64
AC-20 Use of external systems	66
AC-21 Information sharing	68
AC-22 Publicly accessible content.....	69
AC-23 Data mining protection	70
AC-24 Access control decisions.....	70
AC-25 Reference monitor	71
Family: Awareness and training.....	73
AT-01 Awareness and training policy and procedures	73
AT-02 Literacy training and awareness	74
AT-03 Role-based training.....	76
AT-04 Training records	78
AT-05 Contacts with security groups and associations	78
AT-06 Training feedback.....	78
Family: Audit and accountability.....	80
AU-01 Audit and accountability policy and procedures	80
AU-02 Event logging	81
AU-03 Content of audit records	82
AU-04 Audit log storage capacity	83
AU-05 Response to audit logging process failures	84
AU-06 Audit record review, analysis, and reporting.....	85
AU-07 Audit record reduction and report generation.....	88
AU-08 Time stamps	89
AU-09 Protection of audit information	89
AU-10 Non-repudiation	91
AU-11 Audit record retention.....	93
AU-12 Audit record generation	93
AU-13 Monitoring for information disclosure	95
AU-14 Session audit	96
AU-15 Alternate audit logging capability	97
AU-16 Cross-organizational audit logging	97
Family: Assessment, authorization, and monitoring	99
CA-01 Assessment, authorization and monitoring policy and procedures.....	99
CA-02 Control assessments.....	100

CA-03 Information exchange.....	103
CA-04 Security certification	105
CA-05 Plan of action and milestones.....	105
CA-06 Authorization	106
CA-07 Continuous monitoring	107
CA-08 Penetration testing.....	109
CA-09 Internal system connections	111
Family: Configuration management.....	113
CM-01 Configuration management policy and procedures.....	113
CM-02 Baseline configuration	114
CM-03 Configuration change control	115
CM-04 Impact analyses	118
CM-05 Access restrictions for change.....	119
CM-06 Configuration Settings	120
CM-07 Least functionality	122
CM-08 System component inventory	125
CM-09 Configuration management plan.....	127
CM-10 Software use restrictions	128
CM-11 User-installed software	129
CM-12 Information location	130
CM-13 Data action mapping.....	131
CM-14 Signed components	131
Family: Contingency planning	132
CP-01 Contingency planning policy and procedures	132
CP-02 Contingency plan.....	133
CP-03 Contingency training.....	136
CP-04 Contingency plan testing	137
CP-05 Contingency plan update	138
CP-06 Alternate storage site	138
CP-07 Alternate processing site.....	139
CP-08 Telecommunications services.....	141
CP-09 System backup.....	143
CP-10 System recovery and reconstitution.....	145
CP-11 Alternate communications protocols.....	146
CP-12 Safe mode.....	146

CP-13 Alternative security mechanisms.....	147
Family: Identification and authentication	148
IA-01 Identification and authentication policy and procedures	148
IA-02 Identification and authentication (organizational users)	149
IA-03 Device identification and authentication	152
IA-04 Identifier management.....	153
IA-05 Authenticator management.....	156
IA-06 Authentication feedback	161
IA-07 Cryptographic module authentication	161
IA-08 Identification and authentication (non-organizational users)	161
IA-09 Service identification and authentication	163
IA-10 Adaptive authentication	164
IA-11 Re-authentication	164
IA-12 Identity proofing	164
IA-13 Identity providers and authorization servers.....	166
Family: Incident response	169
IR-01 Incident response policy and procedures	169
IR-02 Incident response training.....	170
IR-03 Incident response testing	171
IR-04 Incident handling	172
IR-05 Incident monitoring.....	178
IR-06 Incident reporting	178
IR-07 Incident response assistance	179
IR-08 Incident response plan.....	180
IR-09 Information spillage response	182
IR-10 Integrated information security analysis team.....	183
Family: Maintenance	184
MA-01 Maintenance policy and procedures	184
MA-02 Controlled maintenance	185
MA-03 Maintenance tools	186
MA-04 Non-local maintenance	187
MA-05 Maintenance personnel.....	189
MA-06 Timely maintenance.....	191
MA-07 Field maintenance	192
Family: Media protection.....	193

MP-01 Media protection policy and procedures	193
MP-02 Media access	194
MP-03 Media marking.....	194
MP-04 Media storage	195
MP-05 Media transport	196
MP-06 Media sanitization	197
MP-07 Media use	199
MP-08 Media downgrading	200
Family: Physical and environmental protection	202
PE-01 Physical and environmental protection policy and procedures	202
PE-02 Physical access authorizations	203
PE-03 Physical access control	204
PE-04 Access control for transmission.....	207
PE-05 Access control for output devices	207
PE-06 Monitoring physical access.....	208
PE-07 Visitor control.....	209
PE-08 Visitor access records	210
PE-09 Power equipment and cabling	211
PE-10 Emergency shutoff.....	211
PE-11 Emergency power	212
PE-12 Emergency lighting	212
PE-13 Fire protection	213
PE-14 Environmental controls	214
PE-15 Water damage protection.....	215
PE-16 Delivery and removal.....	215
PE-17 Alternate work site.....	215
PE-18 Location of system components.....	216
PE-19 Information leakage.....	216
PE-20 Asset monitoring and tracking.....	217
PE-21 Electromagnetic pulse protection	217
PE-22 Component marking.....	218
PE-23 Facility location	218
PE-400 Remote and telework environments	218
PE-401 Security operations centre.....	220
Family: Planning	222

PL-01 Planning policy and procedures	222
PL-02 System security and privacy plans	223
PL-03 System security plan update.....	224
PL-04 Rules of behaviour	225
PL-05 Privacy impact assessment.....	226
PL-06 Security-related activity planning	226
PL-07 Concept of operations.....	226
PL-08 Security and privacy architecture	226
PL-09 Central management.....	228
PL-10 Baseline selection.....	229
PL-11 Baseline tailoring	230
Family: Program management.....	231
PM-01 Information security program plan.....	231
PM-02 Information security program leadership role	232
PM-03 Information security and privacy resources	232
PM-04 Plan of action and milestones process	233
PM-05 System and program inventory	233
PM-06 Measures of performance	234
PM-07 Enterprise architecture.....	234
PM-08 Critical infrastructure plan.....	235
PM-09 Risk management strategy	236
PM-10 Authorization process	236
PM-11 Mission and business process definition	237
PM-12 Insider threat program	238
PM-13 Security and privacy workforce.....	238
PM-14 Testing, training, and monitoring	239
PM-15 Security and privacy groups and associations	239
PM-16 Threat awareness program.....	240
PM-17 Protecting controlled information on outsourced external systems	240
PM-18 Privacy program plan	241
PM-19 Privacy program leadership role	242
PM-20 Communication of key privacy services	243
PM-21 Maintain a record of disclosures	244
PM-22 Personal information quality management.....	244
PM-23 Data governance committee.....	246

PM-24 Data integrity board	246
PM-25 Minimization of personal information used in testing, training, and research	247
PM-26 Complaint management	248
PM-27 Privacy reporting	249
PM-28 Risk framing	249
PM-29 Risk management program leadership roles.....	250
PM-30 Supply chain risk management strategy	250
PM-31 Continuous monitoring strategy	251
PM-32 Purposing.....	252
Family: Personnel security	253
PS-01 Personnel security policy and procedures	253
PS-02 Position security analysis	254
PS-03 Personnel screening	254
PS-04 Personnel termination.....	255
PS-05 Personnel transfer	257
PS-06 Access agreements	258
PS-07 External personnel security	259
PS-08 Personnel sanctions	260
PS-09 Position descriptions	260
Family: Personal information handling and transparency	261
PT-01 Personal information handling and transparency policy and procedures.....	261
PT-02 Authority to collect and use personal information	262
PT-03 Personal information handling uses and disclosures	263
PT-04 Consent	264
PT-05 Privacy notice.....	266
PT-06 Personal information banks	268
PT-07 Particularly sensitive personal information	269
PT-08 Data matching requirements	271
Family: Risk assessment.....	272
RA-01 Risk assessment policy and procedures	272
RA-02 Security categorization	273
RA-03 Risk assessment	274
RA-04 Risk assessment update	276
RA-05 Vulnerability monitoring and scanning	276
RA-06 Technical surveillance countermeasures survey.....	280

RA-07 Risk response.....	280
RA-08 Privacy impact assessments.....	280
RA-09 Criticality analysis	281
RA-10 Threat hunting.....	282
Family: System and services acquisition	284
SA-01 System and services acquisition policy and procedures	284
SA-02 Allocation of resources.....	285
SA-03 System development lifecycle	285
SA-04 Acquisition process	287
SA-05 System documentation	292
SA-06 Software usage restrictions	293
SA-07 User-installed software	293
SA-08 Security and privacy engineering principles.....	293
SA-09 External system services	307
SA-10 Developer configuration management	310
SA-11 Developer testing and evaluation.....	312
SA-12 Supply chain protection	316
SA-13 Trustworthiness	317
SA-14 Criticality analysis	317
SA-15 Development process, standards, and tools.....	317
SA-16 Developer-provided training	320
SA-17 Developer security and privacy architecture and design.....	321
SA-18 Tamper resistance and detection	325
SA-19 Component authenticity.....	325
SA-20 Customized development of critical components.....	325
SA-21 Developer screening	326
SA-22 Unsupported system components	326
SA-23 Specialization.....	327
SA-400 Sovereignty and jurisdiction	328
Family: System and communications protection	332
SC-01 System and communications protection policy and procedures	332
SC-02 Separation of system and user functionality	333
SC-03 Security function isolation.....	333
SC-04 Information in shared system resources	335
SC-05 Denial-of-service protection	335

SC-06 Resource availability	337
SC-07 Boundary protection	337
SC-08 Transmission confidentiality and integrity	345
SC-09 Transmission confidentiality	346
SC-10 Network disconnect	346
SC-11 Trusted path	347
SC-12 Cryptographic key establishment and management	347
SC-13 Cryptographic protection	349
SC-14 Public access protections	350
SC-15 Collaborative computing devices and platforms	350
SC-16 Transmission of security and privacy attributes	351
SC-17 Public key infrastructure certificates	352
SC-18 Mobile code	352
SC-19 Voice over Internet protocol	353
SC-20 Secure name/address resolution service (authoritative source)	354
SC-21 Secure name/address resolution service (recursive or caching resolver)	355
SC-22 Architecture and provisioning for name/address resolution service	355
SC-23 Session authenticity	356
SC-24 Fail in known state	357
SC-25 Thin nodes	357
SC-26 Decoys	357
SC-27 Platform-independent applications	358
SC-28 Protection of information at rest	358
SC-29 Heterogeneity	359
SC-30 Concealment and misdirection	359
SC-31 Covert channel analysis	361
SC-32 System partitioning	362
SC-33 Transmission preparation integrity	362
SC-34 Non-modifiable executable programs	362
SC-35 External malicious code identification	363
SC-36 Distributed processing and storage	364
SC-37 Out-of-band channels	364
SC-38 Operations security	365
SC-39 Process isolation	365
SC-40 Wireless link protection	366

SC-41 Port and input/output device access	367
SC-42 Sensor capability and data	368
SC-43 Usage restrictions	369
SC-44 Detonation chambers.....	370
SC-45 System time synchronization	370
SC-46 Cross-domain policy enforcement	371
SC-47 Alternate communications paths.....	372
SC-48 Sensor relocation	372
SC-49 Hardware-enforced separation and policy enforcement.....	373
SC-50 Software-enforced separation and policy enforcement.....	373
SC-51 Hardware-based protection	373
SC-400 Entity source authentication.....	373
SC-401 Unclassified telecommunications in secure facilities	374
Family: System and information integrity	376
SI-01 System and information integrity policy and procedures	376
SI-02 Flaw remediation	377
SI-03 Malicious code protection	379
SI-04 System monitoring.....	381
SI-05 Security alerts, advisories, and directives.....	388
SI-06 Security and privacy function verification.....	388
SI-07 Software, firmware, and information integrity.....	389
SI-08 Spam protection	393
SI-09 Information input restrictions	393
SI-10 Information input validation	393
SI-11 Error handling	395
SI-12 Information management and retention	396
SI-13 Predictable failure prevention.....	397
SI-14 Non-persistence	398
SI-15 Information output filtering	399
SI-16 Memory protection.....	400
SI-17 Fail-safe procedures	400
SI-18 Personal information quality operations	400
SI-19 De-identification	402
SI-20 Tainting.....	405
SI-21 Information refresh.....	406

SI-22 Information diversity	406
SI-23 Information fragmentation	406
SI-400 Dedicated administration workstation.....	407
Family: Supply chain risk management	409
SR-01 Supply chain risk management policy and procedures	409
SR-02 Supply chain risk management plan.....	410
SR-03 Supply chain controls and processes	411
SR-04 Provenance	413
SR-05 Acquisition strategies, tools, and methods.....	415
SR-06 Supplier assessments and reviews	416
SR-07 Supply chain operations security	417
SR-08 Notification agreements.....	417
SR-09 Tamper resistance and detection	418
SR-10 Inspection of systems or components	418
SR-11 Component authenticity	419
SR-12 Component disposal	419
Works Cited	420

List of figures

Figure 1: Control or activity structure.....	23

1. Introduction

A **security control**, also known as a safeguard, is a legal, administrative, operational or technical element of a system. They protect the confidentiality, integrity or availability of a business activity or asset and the information it relies on to satisfy security requirements and mitigate cyber security risk. A privacy control is a legal, administrative, operational or technical element of a system implemented at the organizational or system level to mitigate privacy risks and to ensure compliance with applicable privacy requirements.

An **assurance activity**¹ is a collection of tasks that increases the confidence that a security or privacy control is appropriately designed and implemented and is operating as intended. Assurance activities include tasks that aim to ensure that all security and privacy controls in a system's design, implementation and operations are able to satisfy the business needs for security.

Security and privacy activities and controls are selected to satisfy security and privacy requirements levied on a system or organization. Security and privacy requirements are derived from applicable laws, Orders in Council, directives, regulations, policies, standard, and business needs to ensure the confidentiality, integrity and availability of information handled, stored or transmitted, and to manage risks to individual privacy.

The selection, allocation, design and implementation of security and privacy activities and controls are important tasks that have significant implications for the operations and assets of organizations, as well as for the welfare of individuals and of Canada. Organizations should answer the following key questions when addressing information security and privacy activities and controls:

- What security and privacy activities and controls are needed to satisfy security and privacy requirements and to adequately manage mission or business risks or risks to individuals?
- Have the selected activities and controls been implemented or is there a plan in place to do so?
- What is the required level of assurance (i.e., grounds for confidence) that the selected controls, as designed and implemented, are effective?²

The cyber security and privacy risk management activities described in Organizational cyber security and privacy risk management activities (ITSP.10.036) provide the context to adequately answer the above questions.

The Cyber Centre recommends that organizations use the security and privacy controls and assurance activities in this publication to satisfy their cyber security and privacy requirements. The activities and controls catalogue can be viewed as a toolbox containing a collection of safeguards, countermeasures, techniques and processes to respond to security and privacy risks. The activities and controls are employed as part of a well-defined risk management process that supports organizational cyber security and privacy programs. In turn, those cyber security and privacy programs lay the foundation for the success of the mission and business functions of the organization.

It is important that responsible officials or executives understand the cyber security and privacy risks that could adversely affect organizational operations and assets, individuals, other organizations and Canada. They must also understand the current status of their cyber security and privacy programs and the activities and controls planned or in place to protect information, information systems, and organizations to make informed judgments and investments that respond to identified risks in an acceptable manner. The objective is to manage these risks by selecting and implementing security and privacy assurance activities and controls.

¹ In the document, activity is meant as assurance activity.

² Levels of assurance are addressed in System lifecycle cyber security and privacy risk management activities (ITSP.10.037).

Purpose

This publication is part of a series of guidelines published by the Canadian Centre for Cyber Security (the Cyber Centre), under “Cyber security and privacy risk management: A lifecycle approach.” It contains definitions of assurance activities and controls for systems and organizations that practitioners can use as a foundation for selecting, tailoring and allocating activities and controls to manage cyber security and privacy risks. Implementing a comprehensive set of security and privacy activities and controls can help organizations achieve their business activities.

The security and privacy activities and controls catalogue:

- supports organizations in identifying the activities and controls needed to manage cyber security and privacy risks, and to satisfy their cyber security and privacy requirements
- provides a set of security and privacy activities and controls to meet current organizational protection needs, while also adapting to evolving technical and business requirements and threat actor tradecraft
- facilitates a consistent and repeatable approach for specifying and tailoring assurance activities and controls
- creates a foundation for developing assessment methods and procedures to determine the effectiveness of security and privacy controls
- provides a series of assurance activities used to specify security assurance levels (SALs) in System lifecycle cyber security and privacy risk management activities (ITSP.10.037)
- improves communication among organizations and stakeholders by providing a common lexicon that supports discussion of cyber security and privacy risk management

In the GC context, this catalogue enables appropriate officials and executives to protect GC information systems and manage cyber security and privacy risks. This publication, along with others in the series, facilitates compliance to GC legislation and Treasury Board of Canada Secretariat (TBS) policies, directives and standards related to the protection of information systems and personal information.

Scope and applicability

The Security and privacy controls and assurance activities catalogue (ITSP.10.033) can assist cyber security and privacy practitioners during the definition and implementation of organizational cyber security and privacy functions, and during the information system implementation process when selecting security controls for specific information systems. The catalogue can also serve as the basis for developing organizational and domain-specific security and privacy activities and controls profiles.

The activities and controls are independent of the process employed to select those controls and assurance activities. The selection process can be part of an organizational risk management process, a systems engineering process or any other suitable framework addressing cyber security and privacy risk. Organizational cyber security and privacy risk management activities (ITSP.10.036) and System lifecycle cyber security and privacy risk management activities (ITSP.10.037) are recommended processes to adequately select, tailor and implement controls and assurance activities at the organizational and system level, respectively.

In the GC context, this publication provides security and privacy controls and assurance activities that are suitable for departments and agencies engaged in business activities ranging from very low to very high sensitivity and criticality, in Unclassified, Protected and Classified domains.

Audience

This publication is intended to serve a diverse audience, including:

- individuals with system-development responsibilities, including mission or business owners, program managers, system engineers, system security engineers, privacy practitioners, hardware and software developers, system integrators and acquisition or procurement officials or executives
- individuals with logistical or disposition-related responsibilities, including program managers, procurement officials or executives, system integrators and property managers
- individuals with security and privacy implementation and operations responsibilities, including mission or business owners, system owners, information custodians, system administrators, continuity planners and system security or privacy officers
- individuals with security and privacy assessment and monitoring responsibilities, including auditors, system evaluators, control assessors, independent verifiers and validators and analysts
- commercial entities, including industry partners, that produce component products and systems, create security and privacy technologies, or provide services or capabilities that support cyber security or privacy

In the GC, this publication is intended for the audience above, as well as for individuals who support departmental cyber security and privacy risk management activities, such as:

- individuals with system, information security, privacy, or risk management and oversight responsibilities, including authorizing officials, chief information officers (CIOs), chief security officers (CSOs), senior officials in the department's security governance, designated officials for cyber security and appropriate privacy officials or executives
- individuals who participate in the definition, design, development, installation and operation of information systems; more specifically, authorizers, project managers, cyber security architects, cyber security engineers, cyber security assessors and members of cyber security operations groups

Publication taxonomy

This publication is part of a series of guidelines, under "Cyber security and privacy risk management: A lifecycle approach." The documents in the series are as follows:

- Overview, Cyber security and privacy risk management: A lifecycle approach (ITSP.10.035)
- Organizational cyber security and privacy risk management activities (ITSP.10.036)
- System lifecycle cyber security and privacy risk management activities (ITSP.10.037)
- Security and privacy controls and assurance activities catalogue (ITSP.10.033)
- Suggested organizational security and privacy control and activity profile – Medium impact (ITSP.10.033-01)
- Assessment of security and privacy controls and assurance activities (ITSP.10.033-02)

Publication organization

The remainder of this publication is organized as follows:

- [Section 2 Concepts and structure](#) addresses the fundamental concepts associated with controls and assurance activities, including the structure of activities and controls, how they are organized in the catalogue, implementation approaches, the relationship between controls and activities and robustness
- [Section 3 The controls and assurance activities](#) provides a catalogue of assurance activities and controls, including a discussion section to explain the purpose of each assurance activity and control and to provide useful information regarding implementation and assessment. Where applicable, the discussion is divided into a general discussion and a GC discussion. GC discussion is specifically directed at a GC audience as it addresses requirements derived from laws, policies, directives and standards that departments and agencies need to comply with. A list of related

activities and controls is provided to show the relationships and dependencies among them, and the section also contains a list of references to supporting publications that may be helpful to organizations

- The references, glossary of terms, and list of abbreviations provide additional information on the use of assurance activities and controls

2. Concepts and structure

This section presents the fundamental concepts associated with security and privacy controls and assurance activities, including the relationship between requirements, controls, and activities, as well as their structure, implementation approaches for systems and organizations, the relationship between security and privacy controls and activities, the importance of the robustness concept and the effects of the controls and activities on achieving a robust and secure solution.

Requirements, controls, and activities

Security and privacy requirements generally arise from obligations imposed on organizations. Indeed, organizations need to comply with applicable laws, regulations, and generally accepted industry standards. Controls are a standardized way of expressing security and privacy requirements for organizations and systems.

The term “requirement” can also be used in a broader sense to refer to an expression of stakeholders’ business needs for security and privacy for a particular system or organization. These business needs for security and privacy and the corresponding security and privacy requirements can be derived from many sources (e.g., laws, Orders in Council, regulations, policies, directives, standards, mission or business needs or risk assessments) and will drive the selection of appropriate controls and activities.

In this document, the term “requirement” includes both legal and policy requirements, as well as an expression of the broader set of stakeholder business needs for security and privacy that may be derived from other sources.

All these requirements, when applied to a system, help determine the necessary characteristics of the system, encompassing cyber security, privacy and assurance.

Controls

Controls are a description of safeguards and protection capabilities appropriate for achieving the particular cyber security and privacy objectives of the organization, as well as for reflecting the business needs for security and privacy of organizational stakeholders. They are selected, allocated, designed and implemented by the organization to satisfy the system requirements. Controls can include administrative, legal, policy, operational, technical and physical aspects.

In some cases, the selection and implementation of a control may necessitate additional specification by the organization in the form of derived requirements or instantiated control parameter values. The derived requirements and control parameter values may be necessary to provide the appropriate level of implementation detail for particular controls within the system development lifecycle.

Assurance activities

Assurance activities are a description of tasks, such as engineering tasks, documentation content requirements, and assessment tasks, to be completed as part of a project that increases the confidence that controls are appropriately implemented. Pre-selected sets of security and privacy assurance requirements are grouped into security assurance levels (SALs), that provide an increasing level of rigour in the creation of assurance evidence. See System lifecycle cyber security and privacy risk management activities (ITSP.10.037) for further discussion on assurance levels.

Controls and assurance activities, structure, and organization

Security and privacy controls and assurance activities described in this publication have a well-defined organization and structure. They are organized into 20 families to make it easier to select and specify security and privacy controls and activities. Each family contains controls and activities that are related to the specific topic of the family. A 2 character

identifier uniquely identifies each family (e.g., PS for personnel security). Controls and activities may involve aspects of policy, oversight, supervision, manual processes, and automated mechanisms that are implemented by systems or actions by individuals.

The following lists the security and privacy controls and assurance activities families and their associated identifiers:

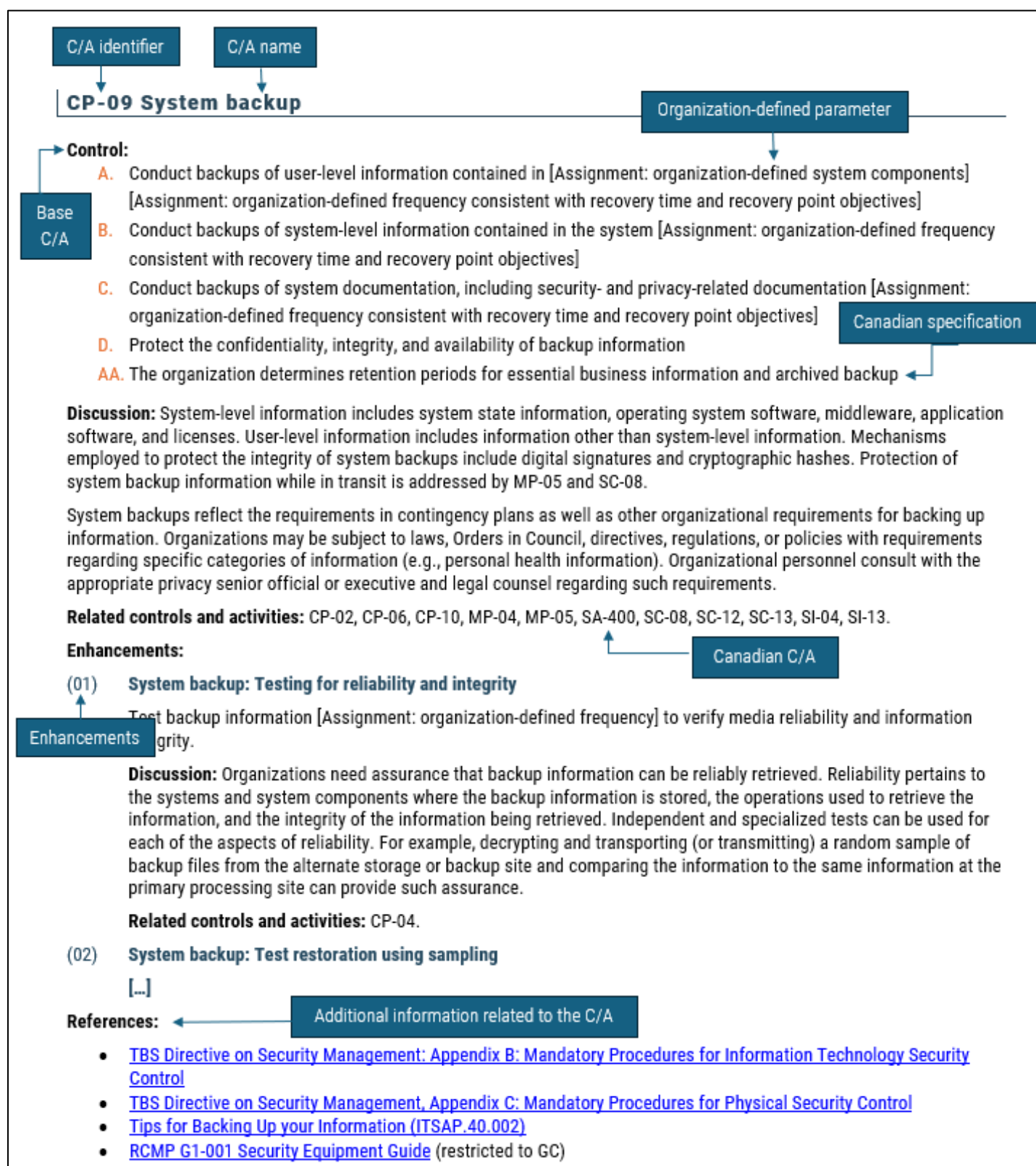
- AC: Access control
- AT: Awareness and training
- AU: Audit and accountability
- CA: Assessment, authorization, and monitoring
- CM: Configuration management
- CP: Contingency planning
- IA: Identification and authentication
- IR: Incident response
- MA: Maintenance
- MP: Media protection
- PE: Physical and environmental protection
- PL: Planning
- PM: Program management
- PS: Personnel security
- PT: Personal information handling and transparency
- RA: Risk assessment
- SA: System and services acquisition
- SC: System and communications protection
- SI: System and information integrity
- SR: Supply chain risk management

Families contain base controls or activities and enhancements. Enhancements are directly related to their base controls or activities. Enhancements either add functionality or specificity to a base control or activity or increase the strength of a base control or rigour of the activity. Enhancements are used in systems and operational environments that require greater protection than what is provided by the base control or activity. The selection of enhancements always requires the selection of the base control or activity.

The families are arranged in alphabetical order, while the controls and activities and their enhancements within each family are in numerical order. The order of the families, controls and activities, and enhancements does not imply any logical progression, level of prioritization or importance, or order in which they are to be implemented. Rather, it reflects the order in which they were included in the catalogue. Control and activity designations are not reused when one is withdrawn. Security and privacy controls and activities have the following sections: base control or activity, discussion, GC discussion when applicable, related controls and activities, enhancements and references.

All security and privacy controls, activities or enhancements starting at 400 (e.g., SA-400, IA-04(400)) are Canada-specific controls and activities. Figure 1 illustrates the structure of a typical control or activity.

Figure 1: Control or activity structure



The **control or activity** (C/A) section provides a description of the security or privacy control or activity to be implemented, through one or more concise statements of the specific security or privacy capability needed to protect an aspect of the system. They are achieved by the actions, whether automated or non-automated, carried out by information systems and

organizations. Each statement in the control or activity section is assigned a separate alphabetic designator (A., B., etc.) and must be complied with to implement the security or privacy control or activity. All statements starting at AA (e.g., CP-09 AA.) are Canada-specific. Organizations have the flexibility to implement the controls or activities selected in whatever manner satisfies organizational mission or business needs consistent with law, regulation, and policy.

The optional **discussion** section provides additional information to facilitate the implementation of a security or privacy control or activity, including any other associated controls and activities. The discussion section does not contain any statements that organizations must comply with to implement the control or activity. Organizations can use the information as needed when developing, tailoring, implementing, assessing, or monitoring controls or activities. Additionally, if applicable, the discussion is divided into a general discussion and a **GC discussion**. GC discussion is specifically directed to a GC audience as it addresses requirements derived from laws, policies, directives, and standards that GC departments and agencies need to comply with.

The **related controls and activities** section provides a list of controls and activities from the catalogue that impact or support the implementation of a particular control, activity, or enhancement; address a related security or privacy capability; or are referenced in the discussion section. Enhancements are inherently related to their base control or activity. Thus, related controls and activities that are referenced in the base control or activity are not repeated in the enhancements. There may be related controls and activities that are only associated with the specific enhancement and therefore do not appear in the base-related controls and activities.

The optional **enhancements** section defines, through concise statements, additional security or privacy capabilities used to increase the strength of a control or the rigour of an activity. Each enhancement is assigned a separate numeric designator ((01), (02), etc.). All enhancements starting at 400 (e.g., AC-17(400)) are Canada-specific. The enhancements are numbered sequentially within each control or activity so that they can be easily identified when selected to supplement the base control or activity. Each enhancement has a short subheading to indicate the intended function or capability it provides. In the CP-09 example above, if an enhancement is selected, the control designation becomes CP-09(01). The numerical designation of an enhancement is used solely for identification purposes; it is not indicative of the strength of the enhancement, level of protection, degree of importance, or any hierarchical relationship among the enhancements. Enhancements are not intended to be selected separately; if one is selected, then the corresponding base control or activity is also selected and implemented.

The **references** section includes a list of applicable laws, policies, directives, standards, guidelines, publications, and other useful references that are relevant to a specific control, activity, or enhancement. The purpose of this section is to provide additional information or context that the reader may find useful in selecting and implementing the control or activity. A reference can be broad or narrow in scope depending on the nature of the control or activity (e.g., GC guidelines on authentication versus a technical security configuration standard).

For some controls and activities, additional flexibility is provided by allowing organizations to define specific values for designated parameters. Flexibility is achieved as part of a tailoring process using **assignment** and **selection** operations embedded within the controls and activities and enclosed in brackets. The assignment and selection operations give organizations the capability to customize controls and activities based on organizational security and privacy requirements. In contrast to assignment operations, which allow complete flexibility in the designation of parameter values, selection operations narrow the range of potential values by providing a specific list of items for organizations to choose from.

These parameters may be derived from many sources, including laws, Orders in Council, policies, directives, regulations, jurisprudence, standards, guidance, and mission or business needs. Organizational risk assessments and risk tolerance are also important factors in determining the values for parameters. Once specified by the organization, the values for the assignment and selection operations become a part of the control or activity. Organization-defined parameters (ODPs) used in the base control or activity also apply to the enhancements associated with those. The implementation of the control or activity is assessed for effectiveness against the completed control or activity statement. When present in a control or activity statement, the square brackets indicate that there is an ODP that needs to be inserted by the reader for an organization to tailor the control to their context.

In addition to assignment and selection operations embedded in a control or activity, additional flexibility can be achieved through **iteration** and **refinement** actions. Iteration allows organizations to use a control or activity multiple times with different assignment and selection values, perhaps applying it in different situations or when implementing multiple policies. For example, an organization may have multiple systems implementing a control or activity, but with different parameters established to address different risks for each system and operation environment. Refinement is the process of providing additional implementation detail to a control or activity. Refinement can also be used to narrow the scope of a control or activity in conjunction with iteration to cover all applicable scopes (e.g., applying different authentication mechanisms to different system interfaces). Combining assignment and selection operations with iteration and refinement actions when applied to controls and activities provides the needed flexibility to allow organizations to satisfy a broad base of security and privacy requirements at the organization, mission and business process, and system levels of implementation.

The security and privacy controls in the catalogue are expected to change over time, as they are withdrawn, revised, and added. Controls, activities, and enhancements will not be renumbered each time security and privacy plans are withdrawn; this maintains stability in security and privacy plans and automated tools supporting the implementation. Notations of controls, activities and enhancements that have been withdrawn will be maintained in the catalogue for historical purposes.

Implementation approaches

There are 3 approaches to implementing the controls and activities in Section 3: a common (inheritable) implementation approach, a system-specific implementation approach, and a hybrid implementation approach. The implementation approaches define the scope of applicability for the control or activity, its shared nature or inheritability, and the responsibility for control or activity development, implementation, assessment, and authorization. Each implementation approach has a specific objective and focus that helps organizations select the appropriate controls and activities, implement them in an effective manner, and satisfy security and privacy requirements. A specific implementation approach may achieve cost benefits by leveraging security and privacy capabilities across multiple systems and operational environments.

A common control or activity is deployed as a shared service to the organization. Implementing common controls or activities results in a capability that is inheritable by multiple systems or programs. A control or activity is deemed inheritable when the system or program receives protection from its implementation, but the control or activity is developed, implemented, assessed, authorized, and monitored by an internal or external entity other than the entity responsible for the system or program. The security and privacy capabilities provided by common controls and activities can be inherited from many sources, including mission or business lines, organizations, enclaves, operational environments, sites, or other systems or programs. However, implementing common controls and activities can introduce the risk of a single point of failure.

Many of the controls and activities needed to protect organizational information systems—including many physical and environmental protection controls, personnel security controls, and incident response controls—are inheritable and, therefore, are good candidates for common control status. Common controls and activities can also be technology-based, such as identification and authentication, boundary protection, audit and accountability, and access control. The cost of development, implementation, assessment, authorization, and monitoring can be amortized across multiple systems, organizational elements, and programs using the common control and activity implementation approach.

System-specific controls and activities are the primary responsibility of the system owner and the authorizing official for a given system. Implementing system-specific controls and activities can introduce risk if the implementations are not interoperable with common controls and activities. Organizations can implement a control or activity as a hybrid if one part of the control or activity is common (inheritable) and the other part is system specific. For example, an organization may implement control CP-02 using a predefined template for the contingency plan for all organizational information systems with individual system owners tailoring the plan for system-specific uses, where appropriate.

The division of a hybrid control or activity into its common (inheritable) and system-specific parts may vary by organization, depending on the types of information technologies employed, the approach used by the organization to manage its controls and activities, and the assignment of responsibilities. When a control or activity is implemented as a hybrid, the common

control or activity provider is responsible for ensuring the implementation, assessment, and monitoring of the common part of the hybrid control or activity. The system owner is responsible for ensuring the implementation, assessment, and monitoring of the system-specific part of the hybrid control or activity. Implementing controls and activities as hybrid controls can introduce risk if the responsibility for the implementation and ongoing management of the common and system-specific parts of the controls and activities is unclear.

Context is important when determining which implementation approach (i.e., common, hybrid, or system-specific) is most appropriate. The implementation approach cannot be determined to be common, hybrid, or system-specific simply based on the language of the control or activity. Identifying the implementation approach can result in significant savings to organizations in implementation and assessment costs, and a more consistent application of the controls and activities throughout the organization. Typically, identifying the implementation approach is straightforward. However, the implementation itself requires significant planning and coordination.

It is better to plan for the implementation approach of a control or activity (i.e., common, hybrid, or system-specific) early in the system development lifecycle and to coordinate with the entities providing the control. In other words, this is part of doing enterprise security architecture. Similarly, if a control or activity is to be inheritable, coordination with the inheriting entity is required to ensure that the control or activity meets the inheriting entity's needs. This is especially important given the nature of control or activity parameters.

An inheriting entity cannot assume that controls or activities are the same and mitigate the appropriate risk to the system just because the identifiers (e.g., AC-01) are the same. It is essential to examine the parameters (e.g., assignment or selection operations) when determining if a common control or activity is adequate to mitigate system-specific risks.

Security and privacy controls and assurance activities

The selection and implementation of security and privacy controls and activities reflect the objectives of cyber security and privacy programs and how those programs manage their respective risks. Depending on the circumstances, these objectives and risks can be independent or overlapping.

Due to permutations in the relationship between cyber security and privacy program objectives and risk management, there is a need for close collaboration between programs to select and implement the appropriate controls and activities for information systems that handle personal information. Organizations should consider how to promote and institutionalize collaboration between the 2 programs to ensure that the objectives of both disciplines are met and that risks are appropriately managed.

GC cyber security programs are responsible for protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction (i.e., unauthorized activity or system behaviour) to provide confidentiality, integrity, and availability. Those programs are also responsible for managing security risk and for ensuring compliance with applicable security requirements. GC privacy programs are responsible for managing risks to individuals associated with the creation, collection, correction, modification, use, retention, disclosure, or disposal (collectively referred to as "handling") of personal information, and for ensuring compliance with applicable privacy requirements. When a system handles personal information, the cyber security program and the privacy program have shared responsibility for managing the security risks for the personal information in the system. Due to this overlap in responsibilities, the controls and activities that organizations select to manage these security risks will generally be the same regardless of their designation (security or privacy) in control and activity baselines or program or system plans.

For further information on the subject, refer to Organizational cyber security and privacy risk management activities (ITSP.10.036).

Robustness

Robustness is a characterization of the security strength and assurance of a security control. The security **strength** is related to the control's potential ability to protect the confidentiality, integrity, or availability of systems. The security

assurance of a control is related to confidence that the control is designed and implemented correctly and is operating as intended. Together, these 2 aspects define the requirements that must be met in the implementation of a control to satisfy its security objective.

For example, a security control that is conceptually strong (e.g., an encryption algorithm using the Advanced Encryption Standard (AES)) but comes with no assurance (e.g., there is no evidence to show that the algorithm is coded correctly) will have a lower effective robustness than a similar control that has higher assurance (e.g., the software has been validated).

Security controls that protect more sensitive or critical systems or that are exposed to more significant threats will generally require stronger security solutions, and more assurance in their implementation. Therefore, they will also require higher levels of robustness. The robustness model defines a hierarchy of robustness levels that are based on expected injury levels and the capabilities or magnitude of the threats. A thorough discussion on robustness is presented in System lifecycle cyber security and privacy risk management activities (ITSP.10.037).

3. The controls and assurance activities

This section provides the security and privacy controls and activities descriptions.

Organization-defined parameters (ODPs) used in the base control or activity also apply to the enhancements associated with those. The implementation of the control or activity is assessed for effectiveness against the completed control or activity statement. When present in a control or activity statement, the square brackets indicate that there is an ODP that needs to be inserted by the reader in order for an organization to tailor the control to their context. For example, the following enhancement statement “Support the management of system accounts using [Assignment: organization-defined automated mechanisms]” indicates the ODP within the square brackets. The reader must determine the variable that fits the statement best, based on their own circumstances and requirements.

Family: Access control

The controls and activities in the Access control (AC) family support the ability to permit or deny user access to resources within the system.

AC-01 Access control policy and procedures

Activity:

- A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]
 - 1. [Selection (1 or more): Organization-level; Mission/business process-level; System-level] access control policy that
 - a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
 - b. is consistent with applicable laws, Orders in Council, jurisprudence, directives, regulations, policies, standards, and guidelines
 - 2. procedures to facilitate the implementation of the access control policy and the associated access controls
- B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures
- C. Review and update the current access control
 - 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]
 - 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]

Discussion: Access control policies and procedures address the controls in the AC family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy functions collaborate on the development of access control policy and procedures. In general, security and privacy framework policies and procedures at the organization level are preferable and may prevent the need for mission- or system-specific policies and procedures. The access control policies can be included as part of the general security and privacy framework or be represented by multiple policies reflecting the complex nature of organizations.

Procedures can be established for security and privacy, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Privacy procedures should not be ad hoc in nature.

Events that may precipitate an update to access control policy and procedures include assessment or audit findings, security incidents or breaches, legislative changes, jurisprudence, Orders in Council, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related controls and activities: IA-01, PM-09, PM-24, PS-08, SI-02, SI-12.

Enhancements: None.

References:

- [TBS Directive on Security Management, Appendix E: Mandatory Procedures for Information Management Security Control](#)
- [An introduction to the cyber threat environment](#)
- [TBS Guide to Integrated Risk Management](#)

AC-02 Account management

Control:

- A. Define and document the types of accounts allowed and specifically prohibited for use within the system
- B. Assign account managers and data custodians
- C. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership
- D. Specify
 - 1. authorized users of the system
 - 2. group and role membership
 - 3. access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account
- E. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts
- F. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria]
- G. Monitor the use of accounts
- H. Notify account managers and [Assignment: organization-defined personnel or roles] within
 - 1. [Assignment: organization-defined time period] when accounts are no longer required or are dormant
 - 2. [Assignment: organization-defined time period] when users are terminated or transferred
 - 3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual
- I. Authorize access to the system based on
 - 1. a valid access authorization
 - 2. intended system usage
 - 3. [Assignment: organization-defined attributes (as required)]
- J. Periodically review accounts for compliance with account management requirements [Assignment: organization-defined frequency]
- K. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group
- L. Align account management processes with personnel termination and transfer processes

Discussion: Examples of system account types include individual, shared, group, system, guest, anonymous, emergency, developer, temporary, and service. Identification of authorized system users and the specification of access privileges reflect the requirements in other controls related to security and privacy. Users requiring administrative privileges on system accounts receive additional scrutiny by organizational personnel responsible for approving such accounts and privileged access, including system owner, mission, or business owner, senior official in the department's security governance, data custodian, or appropriate privacy senior official or executive. Types of accounts that organizations may wish to prohibit due to increased risk include shared, group, emergency, anonymous, temporary, and guest accounts.

Where access involves personal information, security and privacy officials collaborate with the data custodian to establish the specific conditions for group and role membership; identify authorized users, group and role membership, and access authorizations for each account; and create, adjust, or remove system accounts in accordance with organizational policies. Policies can include such information as account expiration dates or other factors that trigger the disabling of accounts.

Organizations may choose to define access privileges or other attributes by account, type of account, or a combination of the 2. Examples of other attributes required for authorizing access include restrictions on time of day, day of week, and point of origin. In defining other system account attributes, organizations consider system-related requirements and mission/business requirements. Failure to consider these factors could affect system availability.

Temporary and emergency accounts are intended for short-term use. Organizations establish temporary accounts as part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts, including local logon accounts used for special tasks or when network resources are unavailable (may also be known as accounts of last resort). Such accounts remain available and are not subject to automatic disabling or removal dates.

Conditions for disabling or deactivating accounts include when shared/group, emergency, or temporary accounts are no longer required and when individuals are transferred or terminated. Changing shared/group authenticators when members leave the group is intended to ensure that former group members do not retain access to the shared or group account. Some types of system accounts may require specialized training.

Related controls and activities: AC-03, AC-05, AC-06, AC-17, AC-18, AC-20, AC-24, AU-02, AU-12, CM-05, IA-02, IA-04, IA-05, IA-08, MA-03, MA-05, PE-02, PL-04, PS-02, PS-04, PS-05, PS-07, PT-02, PT-03, SC-07, SC-12, SC-13, SC-37.

Enhancements:

(01) Account management: Automated system account management

Support the management of system accounts using [Assignment: organization-defined automated mechanisms].

Discussion: Automated system account management includes using automated mechanisms to

- create, enable, modify, disable, and remove accounts
- notify account managers when an account is created, enabled, modified, disabled, or removed, or when users are terminated or transferred
- monitor system account usage; and report atypical system account usage

Automated mechanisms can include internal system functions and email, telephonic, and text messaging notifications.

Related controls and activities: None.

(02) Account management: Automated temporary and emergency accounts management

Automatically [Selection (1): remove; disable] temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].

Discussion: Management of temporary and emergency accounts includes the removal or disabling of such accounts automatically after a predefined time period rather than at the convenience of the system administrator. Automatic removal or disabling of accounts provides a more consistent implementation.

Related controls and activities: None.

(03) Account management: Disable accounts

Disable accounts within [Assignment: organization-defined time period] when the accounts

- a. have expired
- b. are no longer associated with a user or individual
- c. are in violation of organizational policy
- d. have been inactive for [Assignment: organization-defined time period]

Discussion: Disabling expired, inactive, or otherwise anomalous accounts supports the concepts of least privilege and least functionality which reduce the attack surface of the system.

Related controls and activities: None.

(04) **Account management: Automated audit actions**

Automatically audit account creation, modification, enabling, disabling, and removal actions.

Discussion: Account management audit records are defined in accordance with AU-02 and reviewed, analyzed, and reported in accordance with AU-06.

Related controls and activities: AU-02, AU-06.

(05) **Account management: Inactivity logout**

Require that users log out when [Assignment: organization-defined time period of expected inactivity or description of when to log out].

Discussion: Inactivity logout is behaviour- or policy-based and requires users to take physical action to log out when they are expecting inactivity longer than the defined period. Automatic enforcement of inactivity logout is addressed by AC-11.

Related controls and activities: AC-11.

(06) **Account management: Dynamic privilege management**

Implement [Assignment: organization-defined dynamic privilege management capabilities].

Discussion: In contrast to access control approaches that employ static accounts and predefined user privileges, dynamic access control approaches rely on runtime access control decisions facilitated by dynamic privilege management, such as attribute-based access control (ABAC).

While user identities remain relatively constant over time, user privileges typically change more frequently based on ongoing mission or business requirements and the operational needs of organizations. An example of dynamic privilege management is the immediate revocation of privileges from users as opposed to requiring that users terminate and restart their sessions to reflect changes in privileges.

Dynamic privilege management can also include mechanisms that change user privileges based on dynamic rules as opposed to editing specific user profiles. Examples include automatic adjustments of user privileges if they are operating out of their normal work times, if their job function or assignment changes, or if systems are under duress or in emergency situations. Dynamic privilege management includes the effects of privilege changes, for example, when there are changes to encryption keys used for communications.

Related controls and activities: AC-16.

(07) **Account management: Privileged user accounts**

- a. Establish and administer privileged user accounts in accordance with [Selection (1): a role-based access scheme; an attribute-based access scheme]
- b. Monitor privileged role or attribute assignments
- c. Monitor changes to roles or attributes

- d. Revoke access when privileged role or attribute assignments are no longer appropriate

Discussion: Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. Privileged roles include key management, account management, database administration, system and network administration, and web administration. A role-based access scheme organizes permitted system access and privileges into roles. In contrast, an attribute-based access scheme specifies allowed system access and privileges based on attributes.

Related controls and activities: None.

(08) **Account management: Dynamic account management**

Create, activate, manage, and deactivate [Assignment: organization-defined system accounts] dynamically.

Discussion: Approaches for dynamically creating, activating, managing, and deactivating system accounts rely on automatically provisioning the accounts at runtime for entities that were previously unknown. Organizations plan for the dynamic management, creation, activation, and deactivation of system accounts by establishing trust relationships, business rules, and mechanisms with appropriate authorities to validate related authorizations and privileges.

Related controls and activities: AC-16.

(09) **Account management: Restrictions on use of shared and group accounts**

Only permit the use of shared and group accounts that meet [Assignment: organization-defined conditions for establishing shared and group accounts].

Discussion: Before permitting the use of shared or group accounts, organizations consider the increased risk due to the lack of accountability with such accounts.

Related controls and activities: None.

(10) **Account management: Shared and group account credential change**

Withdrawn: Incorporated into AC-02.

(11) **Account management: Usage conditions**

Enforce [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined system accounts].

Discussion: Specifying and enforcing usage conditions helps to enforce the principle of least privilege, increase user accountability, and enable effective account monitoring. Account monitoring includes alerts generated if the account is used in violation of organizational parameters. Organizations can describe specific conditions or circumstances under which system accounts can be used, such as by restricting usage to certain days of the week, time of day, or specific durations of time.

Related controls and activities: None.

(12) **Account management: Account monitoring for atypical usage**

- a. Monitor system accounts for [Assignment: organization-defined atypical usage]
- b. Report atypical usage of system accounts to [Assignment: organization-defined personnel or roles]

Discussion: Atypical usage includes accessing systems at certain times of the day or from locations that are not consistent with the normal usage patterns of individuals. Monitoring for atypical usage may reveal rogue behaviour by individuals or an attack in progress. Account monitoring may inadvertently create privacy risks since data collected to identify atypical usage may reveal previously unknown information about the behaviour of individuals. Organizations assess and document privacy risks from monitoring accounts for atypical usage in their privacy impact assessment (PIA) and make determinations that are in alignment with their privacy program plan.

Related controls and activities: AU-06, AU-07, CA-07, IR-08, SI-04.

(13) **Account management: Disable accounts for high-risk individuals**

Disable accounts of individuals within [Assignment: organization-defined time period] of discovery of [Assignment: organization-defined significant risks].

Discussion: Users who pose a significant security and/or privacy risk include individuals for whom reliable evidence indicates either the intention to use authorized access to systems to cause harm or through whom adversaries will cause harm. Such harm includes adverse impacts to organizational operations, organizational assets, individuals, other organizations, or Canada. Close coordination among system administrators, legal staff, human resource managers, and authorizing officials is essential when disabling system accounts for high-risk individuals.

Related controls and activities: AU-06, SI-04.

References:

- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [Managing and controlling administrative privileges \(ITSAP.10.094\)](#)
- [How to protect your organization from insider threats \(ITSAP.10.003\)](#)

AC-03 Access enforcement

Control: Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

Discussion: Access control policies control or document access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (i.e., devices, files, records, domains) in organizational systems. In addition to documenting and enforcing authorized access at the system level and recognizing that systems can host many applications and services in support of mission and business functions, access enforcement mechanisms can also be employed at the application and service level to provide increased information security and privacy. In contrast to logical access controls that are implemented within the system, physical access controls are addressed by the controls in the Physical and Environmental Protection (PE) family.

Related controls and activities: AC-02, AC-04, AC-05, AC-06, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AC-24, AC-25, AT-02, AT-03, AU-09, CA-09, CM-05, CM-11, IA-02, IA-05, IA-06, IA-07, IA-11, IA-13, MA-03, MA-04, MA-05, MP-04, PM-02, PS-03, PT-02, PT-03, SA-17, SC-02, SC-03, SC-04, SC-12, SC-13, SC-28, SC-31, SC-34, SI-04, SI-08.

Enhancements:

(01) **Access enforcement: Restricted access to privileged functions**

Withdrawn: Incorporated into AC-06.

(02) **Access enforcement: Dual authorization**

Enforce dual authorization for [Assignment: organization-defined privileged commands and/or other organization-defined actions].

Discussion: Dual authorization, also known as two-person control, reduces risk related to insider threats. Dual authorization mechanisms require the approval of 2 authorized individuals to execute. To reduce the risk of collusion, organizations consider rotating dual authorization duties. Organizations consider the risk associated with implementing dual authorization mechanisms when immediate responses are necessary to ensure public and environmental safety.

Related controls and activities: CP-09, MP-06.

(03) Access enforcement: Mandatory access control

Enforce [Assignment: organization-defined mandatory access control policy] over the set of covered subjects and objects specified in the policy, and where the policy:

- a. is uniformly enforced across the covered subjects and objects within the system
- b. specifies that a subject that has been granted access to information is constrained from doing any of the following
 - 1) passing the information to unauthorized subjects or objects
 - 2) granting its privileges to other subjects
 - 3) changing one or more security attributes (specified by the policy) on subjects, objects, the system, or system components
 - 4) choosing the security attributes and attribute values (specified by the policy) to be associated with newly created or modified objects
 - 5) changing the rules governing access control
- c. specifies that [Assignment: organization-defined subjects] may explicitly be granted [Assignment: organization-defined privileges] such that they are not limited by any defined subset (or all) of the above constraints

Discussion: Mandatory access control is a type of nondiscretionary access control. Mandatory access control policies constrain what actions subjects can take with information obtained from objects for which they have already been granted access. This prevents the subjects from passing the information to unauthorized subjects and objects. Mandatory access control policies constrain actions that subjects can take with respect to the propagation of access control privileges; that is, a subject with a privilege cannot pass that privilege to other subjects. The policy is uniformly enforced over all subjects and objects to which the system has control. Otherwise, the access control policy can be circumvented. This enforcement is provided by an implementation that meets the reference monitor concept as described in AC-25. The policy is bounded by the system (i.e., once the information is passed outside of the control of the system, additional means may be required to ensure that the constraints on the information remain in effect).

The trusted subjects described above are granted privileges consistent with the concept of least privilege (see AC-06). Trusted subjects are only given the minimum privileges necessary for satisfying organizational mission/business needs relative to the above policy. The control is most applicable when there is a mandate that establishes a policy regarding access to protected information or classified information and some users of the system are not authorized access to all such information resident in the system.

Mandatory access control can operate in conjunction with discretionary access control as described in AC-03(04). A subject constrained in its operation by mandatory access control policies can still operate under the less rigorous constraints of AC-03(04), but mandatory access control policies take precedence over the less rigorous constraints of AC-03(04). For example, while a mandatory access control policy imposes a constraint that prevents a subject from passing information to another subject operating at a different impact or classification level, AC-03(04) permits the subject to pass the information to any other subject with the same impact or classification level as the subject. Examples of mandatory access control policies include the Bell-LaPadula policy to protect confidentiality of information and the Biba policy to protect the integrity of information.

Related controls and activities: SC-07.

(04) Access enforcement: Discretionary access control

Enforce [Assignment: organization-defined discretionary access control policy] over the set of covered subjects and objects specified in the policy, and where the policy specifies that a subject that has been granted access to information can do one or more of the following:

- a. pass the information to any other subjects or objects
- b. grant its privileges to other subjects
- c. change security attributes on subjects, objects, the system, or the system's components
- d. choose the security attributes to be associated with newly created or revised objects
- e. change the rules governing access control

Discussion: When discretionary access control policies are implemented, subjects are not constrained regarding what actions they can take with operational information for which they have already been granted access. However, there are restrictions for use or disclosure of personal information. Notice of uses is provided to the individual at the point of collection and the only permitted uses of the information are communicated in the Privacy Notice Statement and are restricted by uses detailed in ss. 8(2) of the *Privacy Act*.

For operational records, subjects that have been granted access to information are not prevented from passing the information to other subjects or objects (i.e., subjects have the discretion to pass). Discretionary access control can operate in conjunction with mandatory access control as described in AC-03(03) and AC-03(15). A subject that is constrained in its operation by mandatory access control policies can still operate under the less rigorous constraints of discretionary access control. Therefore, while AC-03(03) imposes constraints that prevent a subject from passing information to another subject operating at a different impact or classification level, AC-03(04) permits the subject to pass the information to any subject at the same impact or classification level.

The policy is bounded by the system. Once the information is passed outside of system control, additional means may be required to ensure that the constraints remain in effect. While traditional definitions of discretionary access control require identity-based access control, that limitation is not required for this particular use of discretionary access control.

Related controls and activities: None.

(05) **Access enforcement: Security-relevant information**

Prevent access to [Assignment: organization-defined security-relevant information] except during secure, non-operable system states.

Discussion: Security-relevant information is information within systems that can potentially impact the operation of security functions or the provision of security services in a manner that could result in failure to enforce system security and privacy policies or maintain the separation of code and data. Security-relevant information includes access control lists, filtering rules for routers or firewalls, configuration parameters for security services, and cryptographic key management information. Secure, non-operable system states include the times in which systems are not performing mission or business-related processing, such as when the system is offline for maintenance, boot-up, troubleshooting, or shut down.

Related controls and activities: CM-06, SC-39.

(06) **Access enforcement: Protection of user and system information**

Withdrawn: Incorporated into MP-04 and SC-28.

(07) **Access enforcement: Role-based access control**

Enforce a role-based access control policy over defined subjects and objects and control access based upon [Assignment: organization-defined roles and users authorized to assume such roles].

Discussion: Role-based access control (RBAC) is an access control policy that enforces access to objects and system functions based on the defined role (i.e., job function) of the subject. Organizations can create specific roles based on job functions and the authorizations (i.e., privileges) to perform needed operations on the systems associated with the organization-defined roles. When users are assigned to specific roles, they inherit the authorizations or privileges defined for those roles. RBAC simplifies privilege administration for organizations because privileges are not assigned directly to every user (which can be many individuals) but are instead acquired through role assignments. RBAC can also increase privacy and security risk if individuals assigned to a role are given access to information beyond what they need to support organizational missions or business functions. RBAC can be implemented as a mandatory or discretionary form of access control. For organizations implementing RBAC with mandatory access controls, the requirements in AC-03(03) define the scope of the subjects and objects covered by the policy.

Related controls and activities: None.

(08) **Access enforcement: Revocation of access authorizations**

Enforce the revocation of access authorizations resulting from changes to the security attributes of subjects and objects based on [Assignment: organization-defined rules governing the timing of revocations of access authorizations].

Discussion: Revocation of access rules may differ based on the types of access revoked. For example, if a subject (i.e., user or process acting on behalf of a user) is removed from a group, access may not be revoked until the next time the object is opened or the next time the subject attempts to access the object. Revocation based on changes to security labels may take effect immediately. Organizations provide alternative approaches on how to make revocations immediate if systems cannot provide such capability and immediate revocation is necessary.

Related controls and activities: None.

(09) **Access enforcement: Controlled release**

Release information outside of the system only if:

- a. the receiving [Assignment: organization-defined system or system component] provides [Assignment: organization-defined controls]
- b. [Assignment: organization-defined controls] are used to validate the appropriateness of the information designated for release

Discussion: Organizations can only directly protect information when it resides within the system. Additional controls may be needed to ensure that organizational information is adequately protected once it is transmitted outside of the system. In situations where the system is unable to determine the adequacy of the protections provided by external entities, as a mitigation measure, organizations procedurally determine whether the external systems are providing adequate controls.

The means used to determine the adequacy of controls provided by external systems include conducting periodic assessments (inspections/tests), establishing agreements between the organization and its counterpart organizations, or some other process. The means used by external entities to protect the information received need not be the same as those used by the organization, but the means employed must be sufficient to provide consistent adjudication of the security and privacy policy to protect the information and individuals' privacy.

Controlled release of information requires systems to implement technical or procedural means to validate the information prior to releasing it to external systems. For example, if the system passes information to a system controlled by another organization, technical means are employed to validate that the security and privacy attributes associated with the exported information are appropriate for the receiving system. Alternatively, if the system passes information to a printer in organization-controlled space, procedural means can be employed to ensure that only authorized individuals gain access to the printer.

Related controls and activities: CA-03, PT-07, PT-08, SA-09, SC-16.

(10) Access enforcement: Audited override of access control mechanisms

Employ an audited override of automated access control mechanisms under [Assignment: organization-defined conditions] by [Assignment: organization-defined roles].

Discussion: In certain situations, such as when there is a threat to human life or an event that threatens the organization's ability to carry out critical missions or business functions, an override capability for access control mechanisms may be needed. Override conditions are defined by organizations and used only in those limited circumstances. Audit events are defined in AU-02. Audit records are generated in AU-12.

Related controls and activities: AU-02, AU-06, AU-10, AU-12, AU-14.

(11) Access enforcement: Restrict access to specific information types

Restrict access to data repositories containing [Assignment: organization-defined information types].

Discussion: Restricting access to specific information is intended to provide flexibility regarding access control of specific information types within a system. For example, role-based access could be employed to allow access to only a specific type of personal information within a database rather than allowing access to the database in its entirety. Other examples include restricting access to cryptographic keys, authentication information, and selected system information.

Related controls and activities: CM-08, CM-12, CM-13, PM-05.

(12) Access enforcement: Assert and enforce application access

- a. Require applications to assert, as part of the installation process, the access needed to the following system applications and functions: [Assignment: organization-defined system applications and functions]
- b. Provide an enforcement mechanism to prevent unauthorized access
- c. Approve access changes after initial installation of the application

Discussion: Asserting and enforcing application access is intended to address applications that need to access existing system applications and functions, including user contacts, global positioning systems, cameras, keyboards, microphones, networks, phones, or other files.

Related controls and activities: CM-07.

(13) Access enforcement: Attribute-based access control

Enforce ABAC policy over defined subjects and objects and control access based upon [Assignment: organization-defined attributes to assume access permissions].

Discussion: ABAC is an access control policy that restricts system access to authorized users based on specified organizational attributes (e.g., job function, identity), action attributes (e.g., read, write, delete), environmental attributes (e.g., time of day, location), and resource attributes (e.g., classification of a document). Organizations can create rules based on attributes and the authorizations (i.e., privileges) to perform needed operations on the systems associated with organization-defined attributes and rules.

When users are assigned to attributes defined in ABAC policies or rules, they can be provisioned to a system with the appropriate privileges or dynamically granted access to a protected resource. ABAC can be implemented as either a mandatory or discretionary form of access control. When implemented with mandatory access controls, the requirements in AC-03(03) define the scope of the subjects and objects covered by the policy.

Related controls and activities: None.

(14) Access enforcement: Individual access

Provide [Assignment: organization-defined mechanisms] to enable individuals to have access to the following elements of their personal information: [Assignment: organization-defined elements].

Discussion: Individual access allows individuals to access and potentially correct inaccuracies related to their personal information held within organizational records, regardless of format. Access helps individuals to develop an understanding about how their personal information is being collected, used, or disclosed by government organizations. It can also help individuals ensure that their personal information used to make administrative decisions is accurate. Access mechanisms can include request forms and application interfaces.

GC discussion: For federal departments and agencies, the *Privacy Act* processes can be located in the government publication, [Sources of Federal Government and Employee Information](#), and on departmental websites. Access to certain types of records may not be appropriate or may require certain levels of authentication assurance. Organizational personnel may consult with the appropriate privacy senior official or executive and legal counsel to determine appropriate mechanisms and access rights or limitations.

Related controls and activities: IA-08, PM-22, PM-20, PM-21, PT-06.

(15) **Access enforcement: Discretionary and mandatory access control**

- a. Enforce [Assignment: organization-defined mandatory access control policy] over the set of covered subjects and objects specified in the policy
- b. Enforce [Assignment: organization-defined discretionary access control policy] over the set of covered subjects and objects specified in the policy

Discussion: Simultaneously implementing a mandatory access control policy and a discretionary access control policy can provide additional protection against the unauthorized execution of code by users or by processes acting on behalf of users. This helps prevent a single compromised user or process from compromising the entire system.

Related controls and activities: SC-02, SC-03, AC-04.

References:

- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [Top 10 IT security actions: No. 3 managing and controlling administrative privileges \(ITSM.10.094\)](#)
- [Managing and controlling administrative privileges \(ITSAP.10.094\)](#)
- [How to protect your organization from insider threats \(ITSAP.10.003\)](#)
- [Privacy Act](#)
- [Government of Canada, Info Source: Sources of Federal Government and Employee Information](#)

AC-04 Information flow enforcement

Control: Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [Assignment: organization-defined information flow control policies].

Discussion: Information flow control regulates where information can travel within a system and between systems (in contrast to who is allowed to access the information) and without regard to subsequent accesses to that information. Flow control restrictions include blocking external traffic that claims to be from within the organization, keeping export-controlled information from being transmitted in the clear to the Internet, restricting web requests that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between organizations may require an agreement specifying how the information flow is enforced (see CA-03).

Transferring information between systems in different security or privacy domains with different security or privacy policies introduces the risk that such transfers violate one or more domain security or privacy policies. In such situations, information custodians/stewards provide guidance at designated policy enforcement points between connected systems.

Organizations consider mandating specific architectural solutions to enforce specific security and privacy policies. Enforcement includes prohibiting information transfers between connected systems (i.e., allowing access only), verifying write permissions before accepting information from another security or privacy domain or connected system, employing hardware mechanisms to enforce one-way information flows, and implementing trustworthy regrading mechanisms to reassign security or privacy attributes and labels.

Custodians for personal information holdings should ensure that the minimal required personal information is shared between one system and another and, where possible, that the sharing of personal information is documented in an agreement.

Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations within systems and between connected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices that employ rule sets or establish configuration settings that restrict system services, provide a packet-filtering capability based on header information, or provide a message-filtering capability based on message content.

Organizations also consider the robustness of filtering and/or inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Control enhancements 3 through 32 primarily address cross-domain solution needs that focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, such as high-assurance guards. Such capabilities are generally unavailable in commercial off-the-shelf products (COTS). Information flow enforcement also applies to control plane traffic (e.g., routing and domain name system (DNS)).

Related controls and activities: AC-03, AC-06, AC-16, AC-17, AC-19, AC-21, AU-10, CA-03, CA-09, CM-07, PL-09, PM-24, SA-17, SC-04, SC-07, SC-16, SC-31.

Enhancements:

(01) **Information flow enforcement: Object security and privacy attributes**

Use [Assignment: organization-defined security and privacy attributes] associated with [Assignment: organization-defined information, source, and destination objects] to enforce [Assignment: organization-defined information flow control policies] as a basis for flow control decisions.

Discussion: Information flow enforcement mechanisms compare security and privacy attributes associated with information (i.e., data content and structure) and source and destination objects and respond appropriately when the enforcement mechanisms encounter information flows not explicitly allowed by information flow policies. For example, an information object labelled Secret would be allowed to flow to a destination object labelled Secret, but an information object labelled Top Secret would not be allowed to flow to a destination object labelled Secret.

A dataset of personal information may be tagged with restrictions against combining with other types of datasets and, thus, would not be allowed to flow to the restricted dataset. Security and privacy attributes can also include source and destination addresses employed in traffic filter firewalls. Flow enforcement using explicit security or privacy attributes can be used, for example, to control the release of certain types of information.

Related controls and activities: None.

(02) **Information flow enforcement: Processing domains**

Use protected processing domains to enforce [Assignment: organization-defined information flow control policies] as a basis for flow control decisions.

Discussion: Protected processing domains within systems are processing spaces that have controlled interactions with other processing spaces, enabling control of information flows between these spaces and to/from information objects. A protected processing domain can be provided, for example, by implementing domain and type enforcement. In domain and type enforcement, system processes are assigned to domains, information is identified

by types, and information flows are controlled based on allowed information accesses (i.e., determined by domain and type), allowed signalling among domains, and allowed process transitions to other domains.

Related controls and activities: SC-39.

(03) **Information flow enforcement: Dynamic information flow control**

Enforce [Assignment: organization-defined information flow control policies].

Discussion: Organizational policies regarding dynamic information flow control include allowing or disallowing information flows based on changing conditions or mission or operational considerations. Changing conditions include changes in risk tolerance due to changes in the immediacy of mission or business needs, changes in the threat environment, and detection of potentially harmful or adverse events.

Related controls and activities: SI-04.

(04) **Information flow enforcement: Flow control of encrypted information**

Prevent encrypted information from bypassing [Assignment: organization-defined information flow control mechanisms] by [Selection (1 or more): decrypting the information; blocking the flow of the encrypted information; terminating communications sessions attempting to pass encrypted information; [Assignment: organization-defined procedure or method]].

Discussion: Flow control mechanisms include content checking, security policy filters, and data type identifiers. The term “encryption” is extended to cover encoded data not recognized by filtering mechanisms.

Related controls and activities: SI-04.

(05) **Information flow enforcement: Embedded data types**

Enforce [Assignment: organization-defined limitations] on embedding data types within other data types.

Discussion: Embedding data types within other data types may result in reduced flow control effectiveness. Data type embedding includes inserting files as objects within other files and using compressed or archived data types that may include multiple embedded data types. Limitations on data type embedding consider the levels of embedding and prohibit levels of data type embedding that are beyond the capability of the inspection tools.

Related controls and activities: None.

(06) **Information flow enforcement: Metadata**

Enforce information flow control based on [Assignment: organization-defined metadata].

Discussion: Metadata is information that describes the characteristics of data. Metadata can include structural metadata describing data structures or descriptive metadata describing data content. Metadata can also infer personal characteristics about an individual. Enforcement of allowed information flows based on metadata enables simpler and more effective flow control.

Organizations consider the trustworthiness of metadata regarding data accuracy (i.e., knowledge that the metadata values are correct with respect to the data), data integrity (i.e., protecting against unauthorized changes to metadata tags), and the binding of metadata to the data payload (i.e., employing sufficiently strong binding techniques with appropriate assurance).

Related controls and activities: AC-16, SI-07.

(07) **Information flow enforcement: One-way flow mechanisms**

Enforce one-way information flows through hardware-based flow control mechanisms.

Discussion: One-way flow mechanisms may also be referred to as a unidirectional network, unidirectional security gateway, or data diode. One-way flow mechanisms can be used to prevent data from being exported from a higher

impact or classified domain or system while permitting data from a lower impact or unclassified domain or system to be imported.

Related controls and activities: None.

(08) Information flow enforcement: Security and privacy policy filters

- a. Enforce information flow control using [Assignment: organization-defined security or privacy policy filters] as a basis for flow control decisions for [Assignment: organization-defined information flows].
- b. [Selection (1 or more): Block; Strip; Modify; Quarantine] data after a filter processing failure in accordance with [Assignment: organization-defined security or privacy policy].

Discussion: Organization-defined security or privacy policy filters can address data structures and content. For example, security or privacy policy filters for data structures can check for maximum file lengths, maximum field sizes, and data/file types (for structured and unstructured data). Security or privacy policy filters for data content can check for specific words, enumerated values or data value ranges, and hidden content. These filters can be used to improve the accuracy of data used for decision-making purposes; for example, phone numbers should include 10 digits. Organizations can implement more than one security or privacy policy filter to meet information flow control objectives.

Structured data permits the interpretation of data content by applications. Unstructured data refers to digital information without a data structure or with a data structure that does not facilitate the development of rule sets to address the impact or classification level of the information conveyed by the data or the flow enforcement decisions.

Unstructured data consists of bitmap objects that are inherently non-language-based (i.e., image, video, or audio files) and textual objects that are based on written or printed languages.

Related controls and activities: None.

(09) Information flow enforcement: Human reviews

Enforce the use of human reviews for [Assignment: organization-defined information flows] under the following conditions: [Assignment: organization-defined conditions].

Discussion: Organizations define security or privacy policy filters for all situations where automated flow control decisions are possible. When a fully automated flow control decision is not possible, then a human review may be employed in lieu of or as a complement to automated security or privacy policy filtering. Human reviews may also be employed as deemed necessary by organizations.

Related controls and activities: None.

(10) Information flow enforcement: Enable and disable security or privacy policy filters

Provide the capability for privileged administrators to enable and disable [Assignment: organization-defined security or privacy policy filters] under the following conditions: [Assignment: organization-defined conditions].

Discussion: For example, as allowed by the system authorization, administrators can enable security or privacy policy filters to accommodate approved data types. Administrators also have the capability to select the filters that are executed on a specific data flow based on the type of data that is being transferred, the source and destination security domains, and other security or privacy relevant features, as needed.

Related controls and activities: None.

(11) Information flow enforcement: Configuration of security or privacy policy filters

Provide the capability for privileged administrators to configure [Assignment: organization-defined security or privacy policy filters] to support different security or privacy policies.

Discussion: Documentation contains detailed information for configuring security or privacy policy filters. For example, administrators can configure security or privacy policy filters to include the list of inappropriate words that security or privacy policy mechanisms check in accordance with the definitions provided by organizations.

Related controls and activities: None.

(12) **Information flow enforcement: Data type identifiers**

When transferring information between different security domains, use [Assignment: organization-defined data type identifiers] to validate data essential for information flow decisions.

Discussion: Data type identifiers include file names, file types, file signatures or tokens, and multiple internal file signatures or tokens. Systems only allow transfer of data that is compliant with data type format specifications. Identification and validation of data types is based on defined specifications associated with each allowed data format. The file name and number alone are not used for data type identification. Content is validated syntactically and semantically against its specification to ensure that it is the proper data type. This can improve the integrity of data, particularly personal information, that is transmitted between systems.

Related controls and activities: None.

(13) **Information flow enforcement: Decomposition into policy-relevant subcomponents**

When transferring information between different security domains, decompose information into [Assignment: organization-defined policy-relevant subcomponents] for submission to policy enforcement mechanisms.

Discussion: Decomposing information into policy-relevant subcomponents prior to information transfer facilitates policy decisions on source, destination, certificates, classification, attachments, and other security- or privacy-related component differentiators. Policy enforcement mechanisms apply filtering, inspection, and/or sanitization rules to the policy-relevant subcomponents of information to facilitate flow enforcement prior to transferring such information to different security domains.

Related controls and activities: None.

(14) **Information flow enforcement: Security or privacy policy filter constraints**

When transferring information between different security domains, implement [Assignment: organization-defined security or privacy policy filters] requiring fully enumerated formats that restrict data structure and content.

Discussion: Data structure and content restrictions reduce the range of potential malicious or unsanctioned content in cross-domain transactions. Security or privacy policy filters that restrict data structures include restricting file sizes and field lengths. Limiting size and field length to open-ended data fields can reduce the risk of over collection of personal information. Data content policy filters include encoding formats for character sets, restricting character data fields to only contain alphanumeric characters, prohibiting special characters, and validating schema structures.

Related controls and activities: None.

(15) **Information flow enforcement: Detection of unsanctioned information**

When transferring information between different security domains, examine the information for the presence of [Assignment: organization-defined unsanctioned information] and prohibit the transfer of such information in accordance with the [Assignment: organization-defined security or privacy policy].

Discussion: Unsanctioned information includes malicious code, information that is inappropriate for release from the source network, or executable code that could disrupt or harm the services or systems on the destination network. Limiting the collection of specific unsanctioned information can reduce the risk of collection of inappropriate personal information.

Related controls and activities: SI-03.

(16) Information flow enforcement: Information transfers on interconnected systems

Withdrawn: Incorporated into AC-04.

(17) Information flow enforcement: Domain authentication

Uniquely identify and authenticate source and destination points by [Selection (1 or more): organization; system; application; service; individual] for information transfer.

Discussion: Attribution is a critical component of a security and privacy concept of operations. The ability to identify source and destination points for information flowing within systems allows the forensic reconstruction of events and encourages policy compliance by attributing policy violations to specific organizations or individuals. Successful domain authentication requires that system labels distinguish among systems, organizations, and individuals involved in preparing, sending, receiving, or disseminating information. Attribution also allows organizations to better maintain the lineage of personal information processing as it flows through systems and can facilitate consent tracking, as well as correction, deletion, or access requests from individuals.

Related controls and activities: IA-02, IA-03, IA-09.

(18) Information flow enforcement: Security attribute binding

Withdrawn: Incorporated into AC-16.

(19) Information flow enforcement: Validation of metadata

When transferring information between different security domains, implement [Assignment: organization-defined security or privacy policy filters] on metadata.

Discussion: All information (including metadata and the data to which the metadata applies) is subject to filtering and inspection. Some organizations distinguish between metadata and data payloads (i.e., only the data to which the metadata is bound). Other organizations do not make such distinctions and consider metadata and the data to which the metadata applies to be part of the payload.

Related controls and activities: None.

(20) Information flow enforcement: Approved solutions

Employ [Assignment: organization-defined solutions in approved configurations] to control the flow of [Assignment: organization-defined information] across security domains.

Discussion: Organizations define approved solutions and configurations in cross-domain policies and guidance in accordance with the types of information flows across classification boundaries.

GC discussion: The Cyber Centre provides recommendations on certified cross-domain solution (CDS) products and design patterns. Contact the Cyber Centre at contact@cyber.gc.ca for more information.

Related controls and activities: None.

(21) Information flow enforcement: Physical or logical separation of information flows

Separate information flows logically or physically using [Assignment: organization-defined mechanisms and/or techniques] to accomplish [Assignment: organization-defined required separations by types of information].

Discussion: Enforcing the separation of information flows associated with defined types of data can enhance protection by ensuring that information is not commingled while in transit and by enabling flow control by transmission paths that are not otherwise achievable. Types of separable information include inbound and outbound communications traffic, service requests and responses, and information of differing security impact or classification levels.

Related controls and activities: SC-32.

(22) Information flow enforcement: Access only

Provide access from a single device to computing platforms, applications, or data residing in multiple different security domains, while preventing information flow between the different security domains.

Discussion: The system provides a capability for users to access each connected security domain without providing any mechanisms to allow users to transfer data or information between the different security domains. An example of an access-only solution is a terminal that provides a user access to information with different security classifications while assuredly keeping the information separate.

Related controls and activities: SI-400.

(23) **Information flow enforcement: Modify non-releasable information**

When transferring information between different security domains, modify non-releasable information by implementing [Assignment: organization-defined modification action].

Discussion: Modifying or de-identifying non-releasable information can help prevent a data spill or attack when information is transferred across security domains. Modification actions include masking, permutation, alteration such as scrambling of data removal, or redaction.

Related controls and activities: None.

(24) **Information flow enforcement: Internal normalized format**

When transferring information between different security domains, parse incoming data into an internal normalized format and regenerate the data to be consistent with its intended specification.

Discussion: Converting data into normalized forms is one of most of effective mechanisms to stop malicious attacks and large classes of data exfiltration.

Related controls and activities: None.

(25) **Information flow enforcement: Data sanitization**

When transferring information between different security domains, sanitize data to minimize [Selection (1 or more): delivery of malicious content, command and control of malicious code, malicious code augmentation, and steganography encoded data; spillage of sensitive information] in accordance with [Assignment: organization-defined policy].

Discussion: Data sanitization is the process of irreversibly removing or destroying data stored on a memory device (e.g., hard drives, flash memory/solid state drives, mobile devices, CDs, DVDs, and Blu-rays) or in hard copy form.

Related controls and activities: MP-06.

(26) **Information flow enforcement: Audit filtering actions**

When transferring information between different security domains, record and audit content filtering actions and results for the information being filtered.

Discussion: Content filtering is the process of inspecting information as it traverses a CDS and determines if the information meets a predefined policy. Content filtering actions and the results of filtering actions are recorded for individual messages to ensure that the correct filter actions were applied. Content filter reports are used to assist in troubleshooting actions by, for example, determining why message content was modified and/or why it failed the filtering process. Audit events are defined in AU-02. Audit records are generated in AU-12.

Related controls and activities: AU-02, AU-03, AU-12.

(27) **Information flow enforcement: Redundant/independent filtering mechanisms**

When transferring information between different security domains, implement content filtering solutions that provide redundant and independent filtering mechanisms for each data type.

Discussion: Content filtering is the process of inspecting information as it traverses a CDS and determines if the information meets a predefined policy. Redundant and independent content filtering eliminates a single point of failure filtering system. Independence is defined as the implementation of a content filter that uses a different code base and supporting libraries (e.g., 2 JPEG filters using different vendors' JPEG libraries) and multiple, independent system processes.

Related controls and activities: None.

(28) **Information flow enforcement: Linear filter pipelines**

When transferring information between different security domains, implement a linear content filter pipeline that is enforced with discretionary and mandatory access controls.

Discussion: Content filtering is the process of inspecting information as it traverses a CDS and determines if the information meets a predefined policy. The use of linear content filter pipelines ensures that filter processes are non-bypassable and always invoked. In general, the use of parallel filtering architectures for content filtering of a single data type introduces bypass and non-invocation issues.

Related controls and activities: None.

(29) **Information flow enforcement: Filter orchestration engines**

When transferring information between different security domains, employ content filter orchestration engines to ensure that:

- a. content filtering mechanisms successfully complete execution without errors
- b. content filtering actions occur in the correct order and comply with [Assignment: organization-defined policy]

Discussion: Content filtering is the process of inspecting information as it traverses a CDS and determines if the information meets a predefined security policy. An orchestration engine coordinates the sequencing of activities (manual and automated) in a content filtering process. Errors are defined as either anomalous actions or unexpected termination of the content filter process. This is not the same as a filter failing content due to non-compliance with policy. Content filter reports are a commonly used mechanism to ensure that expected filtering actions are completed successfully.

Related controls and activities: None.

(30) **Information flow enforcement: Filter mechanisms using multiple processes**

When transferring information between different security domains, implement content filtering mechanisms using multiple processes.

Discussion: The use of multiple processes to implement content filtering mechanisms reduces the likelihood of a single point of failure.

Related controls and activities: None.

(31) **Information flow enforcement: Failed content transfer prevention**

When transferring information between different security domains, prevent the transfer of failed content to the receiving domain.

Discussion: Content that failed filtering checks can corrupt the system if transferred to the receiving domain.

Related controls and activities: None.

(32) **Information flow enforcement: Process requirements for information transfer**

When transferring information between different security domains, the process that transfers information between filter pipelines:

- a. does not filter message content
- b. validates filtering metadata
- c. ensures the content associated with the filtering metadata has successfully completed filtering
- d. transfers the content to the destination filter pipeline

Discussion: The processes transferring information between filter pipelines have minimum complexity and functionality to provide assurance that the processes operate correctly.

Related controls and activities: None.

References:

- [Baseline security requirements for network security zones \(ITSP.80.022\)](#)
- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [Cross domain security primer \(ITSB-120\)](#)
- [Security considerations for the use of removable media devices for Protected C and Classified Information \(ITSB-112\)](#)
- [IT media sanitization \(ITSP.40.006\)](#)
- [TBS Directive on Service and Digital, Appendix L: Standard for Managing Metadata](#)
- [TBS Directive on Service and Digital, Appendix J: Standard on Systems that Manage Information and Data](#)

AC-05 Separation of duties

Control:

- A. Identify and document [Assignment: organization-defined duties of individuals requiring separation]
- B. Define system access authorizations to support separation of duties

Discussion: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes dividing mission or business functions and support functions among different individuals or roles, conducting system support functions with different individuals, and ensuring that security personnel who administer access control functions do not also administer audit functions.

Because separation of duty violations can span systems and application domains, organizations consider the entirety of systems and system components when developing policy on separation of duties. Separation of duties is enforced through the account management activities in AC-02, access control mechanisms in AC-03, and identity management activities in IA-02, IA-04, and IA-12.

Related controls and activities: AC-02, AC-03, AC-06, AU-09, CM-05, CM-11, CP-09, IA-02, IA-04, IA-05, IA-12, MA-03, MA-05, PS-02, SA-08, SA-17.

Enhancements: None.

References: None.

AC-06 Least privilege

Control: Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

Discussion: Organizations employ least privilege for specific duties and systems. The principle of least privilege is also applied to system processes, ensuring that the processes have access to systems and operate at privilege levels no higher than necessary to accomplish organizational missions or business functions. Organizations consider the creation of

additional processes, roles, and accounts as necessary to achieve least privilege. Organizations apply least privilege to the development, implementation, and operation of organizational systems.

Related controls and activities: AC-02, AC-03, AC-05, AC-16, CM-05, CM-11, PL-02, PM-12, SA-08, SA-15, SA-17, SC-38.

Enhancements:

(01) Least privilege: Authorize access to security functions

Authorize access for [Assignment: organization-defined individuals or roles] to:

- a. [Assignment: organization-defined security functions (deployed in hardware, software, and firmware)]
- b. [Assignment: organization-defined security-relevant information]

Discussion: Security functions include establishing system accounts, configuring access authorizations (i.e., permissions, privileges), configuring settings for events to be audited, and establishing intrusion detection parameters.

Security-relevant information includes filtering rules for routers or firewalls, configuration parameters for security services, cryptographic key management information, and access control lists.

Authorized personnel include security administrators, system administrators, system security officers, system programmers, and other privileged users.

Related controls and activities: AC-17, AC-18, AC-19, AU-09, PE-02.

(02) Least privilege: Non-privileged access to non-security functions

Require that users of system accounts (or roles) with access to [Assignment: organization-defined security functions or security-relevant information] use non-privileged accounts or roles, when accessing non-security functions.

Discussion: Requiring the use of non-privileged accounts when accessing non-security functions limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies, such as role-based access control, and where a change of role provides the same degree of assurance in the change of access authorizations for the user and the processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account.

Related controls and activities: AC-17, AC-18, AC-19, PL-04.

(03) Least privilege: Network access to privileged commands

Authorize network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs] and document the rationale for such access in the security plan for the system.

Discussion: Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device).

Related controls and activities: AC-17, AC-18, AC-19.

(04) Least privilege: Separate processing domains

Provide separate processing domains to enable finer-grained allocation of user privileges.

Discussion: Providing separate processing domains for finer-grained allocation of user privileges includes using virtualization techniques to permit additional user privileges within a virtual machine while restricting privileges to other virtual machines or to the underlying physical machine, implementing separate physical domains, and employing hardware or software domain separation mechanisms.

Related controls and activities: AC-04, SC-02, SC-03, SC-30, SC-32, SC-39.

(05) Least privilege: Privileged accounts

Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].

Discussion: Privileged accounts, including super user accounts, are typically described as the system administrator for various types of COTS operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from accessing privileged information or privileged functions. Organizations may differentiate in the application of restricting privileged accounts between allowed privileges for local accounts and for domain accounts provided that they retain the ability to control system configurations for key parameters and as otherwise necessary to sufficiently mitigate risk.

Related controls and activities: IA-02, MA-03, MA-04.

(06) Least privilege: Privileged access by non-organizational users

Prohibit privileged access to the system by non-organizational users.

Discussion: An organizational user is an employee, or an individual considered by the organization to have the equivalent status of an employee. Organizational users include contractors, guest researchers, or individuals detailed from other organizations. Policies and procedures for granting equivalent status of employees to individuals include a need-to-know, citizenship, and the relationship to the organization.

Related controls and activities: AC-18, AC-19, IA-02, IA-08.

(07) Least privilege: Review of user privileges

- a. Review [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles or classes of users] to validate the need for such privileges
- b. Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs

Discussion: The need for certain assigned user privileges may change over time to reflect changes in organizational mission and business functions, environments of operation, technologies, or threats. A periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions.

Related controls and activities: CA-07.

(08) Least privilege: Privilege levels for code execution

Prevent the following software from executing at higher privilege levels than users executing the software: [Assignment: organization-defined software].

Discussion: In certain situations, software applications or programs need to execute with elevated privileges to perform required functions. However, depending on the software functionality and configuration, if the privileges required for execution are at a higher level than the privileges assigned to organizational users invoking such applications or programs, those users may indirectly be provided with greater privileges than assigned.

Related controls and activities: None.

(09) Least privilege: Log use of privileged functions

Log the execution of privileged functions.

Discussion: The misuse of privileged functions, either intentionally or unintentionally by authorized users or by unauthorized external entities that have compromised system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Logging and analyzing the use of privileged functions is one way to detect such misuse and help mitigate the risk from insider threats and the advanced persistent threat (APT).

Related controls and activities: AU-02, AU-03, AU-12.

(10) Least privilege: Prohibit non-privileged users from executing privileged functions

Prevent non-privileged users from executing privileged functions.

Discussion: Privileged functions include disabling, circumventing, or altering implemented security or privacy controls, establishing system accounts, performing system integrity checks, and administering cryptographic key management activities. Non-privileged users are individuals who do not possess appropriate authorizations.

Privileged functions that require protection from non-privileged users include circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms. Preventing non-privileged users from executing privileged functions is enforced by AC-03.

Related controls and activities: None.

References: None.

AC-07 Unsuccessful logon attempts

Control:

- A. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]
- B. Automatically [Selection (1 or more): lock the account or node for an [Assignment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt per [Assignment: organization-defined delay algorithm]; notify system administrator; take other [Assignment: organization-defined action]] when the maximum number of unsuccessful attempts is exceeded

Discussion: The need to limit unsuccessful logon attempts and take subsequent action when the maximum number of attempts is exceeded applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by systems are usually temporary and automatically release after a predetermined, organization-defined time period.

If a delay algorithm is selected, organizations may employ different algorithms for different components of the system based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at the operating system and the application levels.

Organization-defined actions that may be taken when the number of allowed consecutive invalid logon attempts is exceeded include prompting the user to answer a secret question in addition to the username and password, invoking a lockdown mode with limited user capabilities (instead of full lockout), allowing users to only logon from specified Internet Protocol (IP) addresses, requiring a CAPTCHA to prevent automated attacks, or applying user profiles such as location, time of day, IP address, device, or Media Access Control (MAC) address.

If automatic system lockout or execution of a delay algorithm is not implemented in support of the availability objective, organizations consider a combination of other actions to help prevent brute force attacks. In addition to the above, organizations can prompt users to respond to a secret question before the number of allowed unsuccessful logon attempts is exceeded. Automatically unlocking an account after a specified period of time is generally not permitted. However, exceptions may be required based on operational mission or need.

Related controls and activities: AC-02, AC-09, AU-02, AU-06, IA-05.

Enhancements:

(01) Unsuccessful logon attempts: Automatic account lock

Withdrawn: Incorporated into AC-07.

(02) Unsuccessful logon attempts: Purge or wipe mobile device

Purge or wipe information from [Assignment: organization-defined mobile devices] based on [Assignment: organization-defined purging or wiping requirements and techniques] after [Assignment: organization-defined number] consecutive, unsuccessful device logon attempts.

Discussion: A mobile device is a computing device that has a small form factor such that it can be carried by a single individual; is designed to operate without a physical connection; possesses local, non-removable or removable data storage; and includes a self-contained power source.

Purging or wiping the device applies only to mobile devices for which the organization-defined number of unsuccessful logons occurs. The logon is to the mobile device, not to any one account on the device. Successful logons to accounts on mobile devices reset the unsuccessful logon count to zero. Purging or wiping may be unnecessary if the information on the device is protected with sufficiently strong encryption mechanisms.

Related controls and activities: AC-19, MP-05, MP-06.

(03) Unsuccessful logon attempts: Biometric attempt limiting

Limit the number of unsuccessful biometric logon attempts to [Assignment: organization-defined number].

Discussion: Biometrics are probabilistic in nature. The ability to successfully authenticate can be impacted by many factors, including matching performance and presentation attack detection mechanisms. Organizations select the appropriate number of attempts for users based on organizationally defined factors.

Related controls and activities: IA-03.

(04) Unsuccessful logon attempts: Use of alternate authentication factor

- a. Allow the use of [Assignment: organization-defined authentication factors] that are different from the primary authentication factors after the number of organization-defined consecutive invalid logon attempts have been exceeded
- b. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts through use of the alternative factors by a user during a [Assignment: organization-defined time period]

Discussion: The use of alternate authentication factors supports the objective of availability and allows a user who has inadvertently been locked out to use additional authentication factors to bypass the lockout.

Related controls and activities: IA-03.

References: [User authentication guidance for information technology systems \(ITSP.30.031\)](#)

AC-08 System use notification

Control:

- A. Display [Assignment: organization-defined system use notification message or banner] to users before granting access to the system that provides privacy and security notices consistent with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines and state that
 1. users are accessing a GC system
 2. system usage may be monitored, recorded, and subject to audit
 3. unauthorized use of the system is prohibited and subject to criminal and civil penalties
 4. the relevant personal information bank (PIB) reference, if applicable
 5. legal authority for the collection of personal information
 6. any legal or administrative consequences for refusing to provide the personal information
 7. the rights of access to, correction and protection of personal information

8. how the information will be used
 9. the right to file a complaint to the Privacy Commissioner of Canada regarding the institution's handling of the individual's personal information
- B.** Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system
- C.** For publicly accessible systems
1. display system use information [Assignment: organization-defined conditions], before granting further access to the publicly accessible system
 2. display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities
 3. include a description of the authorized uses of the system

Discussion: System use notifications can be implemented using messages or warning banners displayed before individuals log in to systems. System use notifications are used only for access via logon interfaces with human users. Notifications are not required when human interfaces do not exist. Based on a risk assessment, organizations consider whether or not a secondary system use notification is needed to access applications or other system resources after the initial network logon. Organizations consider system use notification messages or banners displayed in multiple languages based on organizational needs and the demographics of system users.

This control legally enables additional security controls such as monitoring, auditing, identifier management, acceptable use enforcement, anomalous behaviour detection, and tainting/watermarking.

GC discussion: Organizations consult with the privacy office for input regarding privacy messaging and the TBS or organizational equivalent for legal review and approval of warning banner content. System use notifications may be privacy notice statements (PNS) for systems users.

Related controls and activities: AC-04, AC-14, AC-25, AU-01, AU-16, CA-01, CA-07, CM-13, IA-04, PL-04, PT-02, PT-03, PT-04, PT-05, PT-06, RA-08, SI-04, SI-12, SI-18, SI-19, SI-20, SI-21, SR-03, SR-05.

Enhancements: None.

References:

- [TBS Policy on Service and Digital](#)
- [TBS Directive on Service and Digital](#)
- [TBS Directive on Service and Digital, Appendix C: Mandatory Procedures for Privacy and Monitoring of Network and Device Use Information Notices](#)

AC-09 Previous logon notification

Control: Notify the user, upon successful logon to the system, of the date and time of the last logon.

Discussion: Previous logon notification is applicable to system access via human user interfaces and access to systems that occurs in other types of architectures. Information about the last successful logon allows the user to recognize if the date and time provided is not consistent with the user's last access.

Related controls and activities: AC-07, PL-04.

Enhancements:

(01) Previous logon notification: Unsuccessful logons

Notify the user, upon successful logon, of the number of unsuccessful logon attempts since the last successful logon.

Discussion: Information about the number of unsuccessful logon attempts since the last successful logon allows the user to recognize if the number of unsuccessful logon attempts is consistent with the user's actual logon attempts.

Related controls and activities: None.

(02) **Previous logon notification: Successful and unsuccessful logons**

Notify the user, upon successful logon, of the number of [Selection (1): successful logons; unsuccessful logon attempts; both] during [Assignment: organization-defined time period].

Discussion: Information about the number of successful and unsuccessful logon attempts within a specified time period allows the user to recognize if the number and type of logon attempts are consistent with the user's actual logon attempts.

Related controls and activities: None.

(03) **Previous logon notification: Notification of account changes**

Notify the user, upon successful logon, of changes to [Assignment: organization-defined security-related characteristics or parameters of the user's account] during [Assignment: organization-defined time period].

Discussion: Information about changes to security-related account characteristics within a specified time period allows users to recognize if changes were made without their knowledge.

Related controls and activities: None.

(04) **Previous logon notification: Additional logon information**

Notify the user, upon successful logon, of the following additional information: [Assignment: organization-defined additional information].

Discussion: Organizations can specify additional information to be provided to users upon logon, including the location of the last logon. User location is defined as information that can be determined by systems, such as IP addresses from which network logons occurred, notifications of local logons, or device identifiers.

Related controls and activities: None.

References: None.

AC-10 Concurrent session control

Control: Limit the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined number].

Discussion: Organizations may define the maximum number of concurrent sessions for system accounts globally, by account type, by account, or any combination thereof. For example, organizations may limit the number of concurrent sessions for system administrators or other individuals working in particularly sensitive domains or mission-critical applications. Concurrent session control addresses concurrent sessions for system accounts. It does not, however, address concurrent sessions by single users via multiple system accounts.

Related controls and activities: SC-23.

Enhancements: None.

References: None.

AC-11 Device lock

Control:

- A. Prevent further access to the system by [Selection (1 or more): initiating a device lock after [Assignment: organization-defined tie period] of inactivity; requiring the user to initiate a device lock before leaving the system unattended]
- B. Retain the device lock until the user re-establishes access using established identification and authentication procedures

Discussion: Device locks are temporary actions taken to prevent logical access to organizational systems when users stop work and move away from the immediate vicinity of those systems but do not want to log out because of the temporary nature of their absences. Device locks can be implemented at the operating system level or at the application level.

A proximity lock may be used to initiate the device lock (e.g., via a Bluetooth-enabled device or dongle). User-initiated device locking is behaviour or policy-based and, as such, requires users to take physical action to initiate the device lock. Device locks are not an acceptable substitute for logging out of systems, such as when organizations require users to log out at the end of workdays.

Related controls and activities: AC-02, AC-07, IA-11, PL-04.

Enhancements:

(01) Device lock: Pattern-hiding displays

Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

Discussion: The pattern-hiding display can include static or dynamic images, such as patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen with the caveat that protected information is not displayed.

Related controls and activities: None.

References: None.

AC-12 Session termination

Control: Automatically terminate a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect].

Discussion: Session termination addresses the termination of user-initiated logical sessions (in contrast to SC-10, which addresses the termination of network connections associated with communications sessions (i.e., network disconnect)). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational system. Such user sessions can be terminated without terminating network sessions.

Session termination ends all processes associated with a user's logical session except for those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events that require automatic termination of the session include organization-defined periods of user inactivity, targeted responses to certain types of incidents, or time-of-day restrictions on system use.

Related controls and activities: MA-04, SC-10, SC-23.

Enhancements:

(01) Session termination: User-initiated logouts

Provide a logout capability for user-initiated communications sessions whenever authentication is used to gain access to [Assignment: organization-defined information resources].

Discussion: Information resources to which users gain access via authentication include local workstations, databases, and password-protected websites or web-based services.

Related controls and activities: None.

(02) **Session termination: Termination message**

Display an explicit logout message to users indicating the termination of authenticated communications sessions.

Discussion: Logout messages for web access can be displayed after authenticated sessions have been terminated. However, for certain types of sessions, including file transfer protocol (FTP) sessions, systems typically send logout messages as final messages prior to terminating sessions.

Related controls and activities: None.

(03) **Session termination: Timeout warning message**

Display an explicit message to users indicating that the session will end in [Assignment: organization-defined time until end of session].

Discussion: To increase usability, notify users of pending session termination and prompt users to continue the session. The pending session termination time period is based on the parameters defined in the AC-12 base control.

Related controls and activities: None.

References: None.

AC-13 Supervision and review – access control

Withdrawn: Incorporated into AC-02 and AU-06.

AC-14 Permitted actions without identification or authentication

Control:

- A. Identify [Assignment: organization-defined user actions] that can be performed on the system without identification or authentication consistent with organizational mission and business functions
- B. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication

Discussion: Specific user actions may be permitted without identification or authentication if organizations determine that identification and authentication are not required for the specified user actions. Organizations may allow a limited number of user actions without identification or authentication, including when individuals access public websites or other publicly accessible federal systems, when individuals use mobile phones to receive calls, or when facsimiles are received.

Organizations identify actions that normally require identification or authentication but may, under certain circumstances, allow identification or authentication mechanisms to be bypassed. Such bypasses may occur, for example, via a software-readable physical switch that commands bypass of the logon functionality and is protected from accidental or unmonitored use.

Permitting actions without identification or authentication does not apply to situations where identification and authentication have already occurred and are not repeated but rather to situations where identification and authentication have not yet occurred. Organizations may decide that there are no user actions that can be performed on organizational systems without identification and authentication, and therefore, the value for the assignment operation can be none.

Related controls and activities: AC-08, IA-02, PL-02.

Enhancements:**(01) Permitted actions without identification or authentication: Necessary uses**

Withdrawn: Incorporated into AC-14.

References: None.**AC-15 Automated marking**

Withdrawn: Incorporated into MP-03.

AC-16 Security and privacy attributes

Control:

- A. Provide the means to associate [Assignment: organization-defined types of security and privacy attributes] with [Assignment: organization-defined security and privacy attribute values] for information in storage, in process, and/or in transmission
- B. Ensure that the attribute associations are made and retained with the information
- C. Establish the following permitted security and privacy attributes from the attributes defined in AC-16A for [Assignment: organization-defined systems]: [Assignment: organization-defined security and privacy attributes]
- D. Determine the following permitted attribute values or ranges for each of the established attributes: [Assignment: organization-defined attribute values or ranges for established attributes]
- E. Audit changes to attributes
- F. Review [Assignment: organization-defined security and privacy attributes] for applicability [Assignment: organization-defined frequency]

Discussion: Information is represented internally within systems using abstractions known as data structures. Internal data structures can represent different types of entities, both active and passive. Active entities, also known as subjects, are typically associated with individuals, devices, or processes acting on behalf of individuals. Passive entities, also known as objects, are typically associated with data structures, such as records, buffers, tables, files, inter-process pipes, and communications ports. Security attributes, a form of metadata, are abstractions that represent the basic properties or characteristics of active and passive entities with respect to safeguarding information. Privacy attributes, which may be used independently or in conjunction with security attributes, represent the basic properties or characteristics of active or passive entities with respect to the management of personal information. Attributes can be either explicitly or implicitly associated with the information contained in organizational systems or system components.

Attributes may be associated with active entities (i.e., subjects) that have the potential to send or receive information, cause information to flow among objects, or change the system state. These attributes may also be associated with passive entities (i.e., objects) that contain or receive information. The association of attributes to subjects and objects by a system is referred to as binding and is inclusive of setting the attribute value and the attribute type.

Attributes, when bound to data or information, permit the enforcement of security and privacy policies for access control and information flow control, including data retention limits, permitted uses of personal information, and identification of personal information within data objects. Such enforcement occurs through organizational processes or system functions or mechanisms. The binding techniques implemented by systems affect the strength of attribute binding to information. Binding strength and the assurance associated with binding techniques play important parts in the trust that organizations have in the information flow enforcement process. The binding techniques affect the number and degree of additional reviews required by organizations. The content or assigned values of attributes can directly affect the ability of individuals to access organizational information.

Organizations can define the types of attributes needed for systems to support missions or business functions. There are many values that can be assigned to a security attribute. By specifying the permitted attribute ranges and values, organizations ensure that attribute values are meaningful and relevant. Labelling refers to the association of attributes with the subjects and objects represented by the internal data structures within systems. This facilitates system-based enforcement of information security and privacy policies. Labels include classification of information in accordance with legal and compliance requirements (e.g., Top Secret, Secret, Confidential, Protected), information impact level; high value asset information, access authorizations, nationality; data lifecycle protection (i.e., encryption and data expiration), personal information processing permissions, including individual consent to personal information processing, and contractor affiliation.

A related term to labeling is marking. Marking refers to the association of attributes with objects in a human-readable form and displayed on system media. Marking enables manual, procedural, or process-based enforcement of information security and privacy policies. Security and privacy labels may have the same value as media markings (e.g., Top Secret, Secret, Confidential). See MP-03 (Media Marking).

Related controls and activities: AC-03, AC-04, AC-06, AC-21, AC-25, AU-02, AU-10, MP-03, PE-22, PT-02, PT-03, PT-04, SC-11, SC-16, SI-12, SI-18, SA-400.

Enhancements:

(01) Security and privacy attributes: Dynamic attribute association

Dynamically associate security and privacy attributes with [Assignment: organization-defined subjects and objects] in accordance with the following security and privacy policies as information is created and combined: [Assignment: organization-defined security and privacy policies].

Discussion: Dynamic association of attributes is appropriate whenever the security or privacy characteristics of information change over time. Attributes may change due to information aggregation issues (i.e., characteristics of individual data elements are different from the combined elements), changes in individual access authorizations (i.e., privileges), changes in the security category of information, or changes in security or privacy policies. Attributes may also change situationally.

Related controls and activities: None.

(02) Security and privacy attributes: Attribute value changes by authorized individuals

Provide authorized individuals (or processes acting on behalf of individuals) the capability to define or change the value of associated security and privacy attributes.

Discussion: The content or assigned values of attributes can directly affect the ability of individuals to access organizational information. Therefore, it is important for systems to be able to limit the ability to create or modify attributes to authorized individuals.

Related controls and activities: None.

(03) Security and privacy attributes: Maintenance of attribute associations by system

Maintain the association and integrity of [Assignment: organization-defined security and privacy attributes] to [Assignment: organization-defined subjects and objects].

Discussion: Maintaining the association and integrity of security and privacy attributes to subjects and objects with sufficient assurance helps to ensure that the attribute associations can be used as the basis of automated policy actions. The integrity of specific items, such as security configuration files, may be maintained through the use of an integrity monitoring mechanism that detects anomalies and changes that deviate from known good baselines. Automated policy actions include retention date expirations, access control decisions, information flow control decisions, and information disclosure decisions.

Related controls and activities: None.

(04) Security and privacy attributes: Association of attributes by authorized individuals

Provide the capability to associate [Assignment: organization-defined security and privacy attributes] with [Assignment: organization-defined subjects and objects] by authorized individuals (or processes acting on behalf of individuals).

Discussion: Systems, in general, provide the capability for privileged users to assign security and privacy attributes to system-defined subjects (e.g., users) and objects (e.g., directories, files, and ports). Some systems provide additional capability for general users to assign security and privacy attributes to additional objects (e.g., files, emails).

The association of attributes by authorized individuals is described in the design documentation. The support provided by systems can include prompting users to select security and privacy attributes to be associated with information objects, employing automated mechanisms to categorize information with attributes based on defined policies, or ensuring that the combination of the security or privacy attributes selected is valid. Organizations consider the creation, deletion, or modification of attributes when defining auditable events.

Related controls and activities: None.

(05) **Security and privacy attributes: Attribute displays on objects to be output**

Display security and privacy attributes in human-readable form on each object that the system transmits to output devices to identify [Assignment: organization-defined special dissemination, handling, or distribution instructions] using [Assignment: organization-defined human-readable, standard naming conventions].

Discussion: System outputs include printed pages, screens, or equivalent items. System output devices include printers, notebook computers, video displays, smart phones, and tablets. To mitigate the risk of unauthorized exposure of information (e.g., shoulder surfing), the outputs display full attribute values when unmasked by the subscriber.

Related controls and activities: None.

(06) **Security and privacy attributes: Maintenance of attribute association**

Require personnel to associate and maintain the association of [Assignment: organization-defined security and privacy attributes] with [Assignment: organization-defined subjects and objects] in accordance with [Assignment: organization-defined security and privacy policies].

Discussion: Maintaining attribute association requires individual users (as opposed to the system) to maintain associations of defined security and privacy attributes with subjects and objects.

Related controls and activities: None.

(07) **Security and privacy attributes: Consistent attribute interpretation**

Provide a consistent interpretation of security and privacy attributes transmitted between distributed system components.

Discussion: To enforce security and privacy policies across multiple system components in distributed systems, organizations provide a consistent interpretation of security and privacy attributes employed in access enforcement and flow enforcement decisions. Organizations can establish agreements and processes to help ensure that distributed system components implement attributes with consistent interpretations in automated access enforcement and flow enforcement actions.

Related controls and activities: None.

(08) **Security and privacy attributes: Association techniques and technologies**

Implement [Assignment: organization-defined techniques and technologies] in associating security and privacy attributes to information.

Discussion: The association of security and privacy attributes to information within systems is important for conducting automated access enforcement and flow enforcement actions. The association of such attributes to information (i.e., binding) can be accomplished with technologies and techniques that provide different levels of assurance. For example, systems can cryptographically bind attributes to information using digital signatures that support cryptographic keys protected by hardware devices (sometimes known as hardware roots of trust).

Related controls and activities: SC-12, SC-13.

(09) **Security and privacy attributes: Attribute reassignment – regrading mechanisms**

Change security and privacy attributes associated with information only via regrading mechanisms validated using [Assignment: organization-defined techniques or procedures].

Discussion: A regrading mechanism is a trusted process authorized to re-classify and re-label data in accordance with a defined policy exception. Validated regrading mechanisms are used by organizations to provide the requisite levels of assurance for attribute reassignment activities. The validation is facilitated by ensuring that regrading mechanisms are single purpose and of limited function. Since security and privacy attribute changes can directly affect policy enforcement actions, implementing trustworthy regrading mechanisms is necessary to help ensure that such mechanisms perform in a consistent and correct mode of operation.

Related controls and activities: None.

(10) **Security and privacy attributes: Attribute configuration by authorized individuals**

Provide authorized individuals the capability to define or change the type and value of security and privacy attributes available for association with subjects and objects.

Discussion: The content or assigned values of security and privacy attributes can directly affect the ability of individuals to access organizational information. Thus, it is important for systems to be able to limit the ability to create or modify the type and value of attributes available for association with subjects and objects to authorized individuals only.

Related controls and activities: None.

References:

- [TBS Policy on Government Security](#)
- [TBS Directive on Security Management, Appendix J: Standard on Security Categorization](#)
- [Managing and controlling administrative privileges \(ITSAP.10.094\)](#)
- [Top 10 IT security actions: No. 3 managing and controlling administrative privileges \(ITSM.10.094\)](#)
- [NIST Federal Information Processing Standards \(FIPS\) 140-3 Security Requirements for Cryptographic Modules](#)
- [NIST FIPS 186-5 Digital Signature Standard \(DSS\)](#)

AC-17 Remote access

Control:

- A. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed
- B. Authorize each type of remote access to the system prior to allowing such connections

Discussion: Remote access is access to organizational systems (or processes acting on behalf of users) that communicate through external networks such as the Internet. Types of remote access include dial-up, broadband, and wireless. Organizations use encrypted virtual private networks (VPNs) to enhance confidentiality and integrity for remote connections. The use of encrypted VPNs provides sufficient assurance to the organization that it can effectively treat such connections

as internal networks if the cryptographic mechanisms used are implemented in accordance with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines.

Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. VPNs with encrypted tunnels can also affect the ability to adequately monitor network communications traffic for malicious code. Remote access controls apply to systems other than public web servers or systems designed for public access. Authorization of each remote access type addresses authorization prior to allowing remote access without specifying the specific formats for such authorization. While organizations may use information exchange and system connection security agreements to manage remote access connections to other systems, such agreements are addressed as part of CA-03. Enforcing access restrictions for remote access is addressed via AC-03.

GC discussion: The organization ensures that all employees working off-site safeguard information as per the minimum requirements in accordance with the TBS Directive on Security Management, Appendix C: Mandatory Procedures for Physical Security Control.

Related controls and activities: AC-02, AC-03, AC-04, AC-18, AC-19, AC-20, CA-03, CM-10, IA-02, IA-03, IA-08, MA-04, PE-17, PE-400, PL-02, PL-04, SC-10, SC-12, SC-13, SI-04.

Enhancements:

(01) Remote access: Monitoring and control

Employ automated mechanisms to monitor and control remote access methods.

Discussion: Monitoring and control of remote access methods allows organizations to detect attacks and help ensure compliance with remote access policies by auditing the connection activities of remote users on a variety of system components, including servers, notebook computers, workstations, smart phones, and tablets. Audit logging for remote access is enforced by AU-02. Audit events are defined in AU-02A.

Related controls and activities: AU-02, AU-06, AU-12, AU-14.

(02) Remote access: Protection of confidentiality and integrity using encryption

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

Discussion: VPNs can be used to protect the confidentiality and integrity of remote access sessions. Transport Layer Security (TLS) is an example of a cryptographic protocol that provides end-to-end communications security over networks and is used for Internet communications and online transactions.

Related controls and activities: SC-08, SC-12, SC-13.

(03) Remote access: Managed access control points

Route remote accesses through authorized and managed network access control points.

Discussion: Organizations consider a managed access control points solution for external network connections since limiting the number of access control points for remote access reduces attack surfaces.

GC discussion: GC departments and agencies consider the secure remote access infrastructure provided by Shared Services Canada for external network connections.

Related controls and activities: SC-07.

(04) Remote access: Privileged commands and access

- a. Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides trustworthy evidence and for the following needs: [Assignment: organization-defined needs]
- b. Document the rationale for remote access in the security plan for the system

Discussion: Remote access to systems represents a significant potential vulnerability that can be exploited by adversaries. As such, restricting the execution of privileged commands and access to security-relevant information via remote access reduces the exposure of the organization and the susceptibility to threats by adversaries to the remote access capability.

Related controls and activities: AC-06, SC-12, SC-13.

(05) **Remote access: Monitoring for unauthorized connections**

Withdrawn: Incorporated into SI-04.

(06) **Remote access: Protection of mechanism information**

Protect information about remote access mechanisms from unauthorized use and disclosure.

Discussion: Remote access to organizational information by non-organizational entities can increase the risk of unauthorized use and disclosure about remote access mechanisms. The organization considers including remote access requirements in the information exchange agreements with other organizations, as applicable. Remote access requirements can also be included in rules of behaviour (see PL-04) and access agreements (see PS-06).

Related controls and activities: AT-02, AT-03, PS-06.

(07) **Remote access: Additional protection for security function access**

Withdrawn: Incorporated into AC-03(10).

(08) **Remote access: Disable nonsecure network protocols**

Withdrawn: Incorporated into CM-07.

(09) **Remote access: Disconnect or disable access**

Provide the capability to disconnect or disable remote access to the system within [Assignment: organization-defined time period].

Discussion: The speed of system disconnect or disablement varies based on the criticality of missions or business functions and the need to eliminate immediate or future remote access to systems.

Related controls and activities: None.

(10) **Remote access: Authenticate remote commands**

Implement [Assignment: organization-defined mechanisms] to authenticate [Assignment: organization-defined remote commands].

Discussion: Authenticating remote commands protects against unauthorized commands and the replay of authorized commands. The ability to authenticate remote commands is important for remote systems for which loss, malfunction, misdirection, or exploitation would have immediate or serious consequences, such as injury, death, property damage, loss of high-value assets, failure of mission or business functions, or compromise of classified or protected information. Authentication mechanisms for remote commands ensure that systems accept and execute commands in the order intended, execute only authorized commands, and reject unauthorized commands. Cryptographic mechanisms can be used, for example, to authenticate remote commands.

Related controls and activities: SC-12, SC-13, SC-23.

(400) **Remote access: Privileged accounts remote access**

Remote access to privileged accounts is done from dedicated management consoles only.

Discussion: Remote access to privileged accounts is performed on dedicated management consoles governed entirely by the system's security policies and used exclusively for this purpose (e.g., Internet access not allowed). In the context of this control, remote access means anything not local to the host.

Related controls and activities: SI-400.

References:

- [TBS Directive on Security Management, Appendix C: Mandatory Procedures for Physical Security Control](#)
- [TBS Directive on Security Management, Appendix E: Mandatory Procedures for Information Management Security Control](#)

AC-18 Wireless access

Control:

- Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access
- Authorize each type of wireless access to the system prior to allowing such connections

Discussion: Wireless technologies include microwave, packet radio (ultra-high frequency or very high frequency), 802.11x, and Bluetooth. Wireless networks use authentication protocols that provide authenticator protection and mutual authentication.

Related controls and activities: AC-02, AC-03, AC-17, AC-19, CA-09, CM-07, IA-02, IA-03, IA-08, PL-04, SC-40, SC-43, SI-04.

Enhancements:

(01) **Wireless access: Authentication and encryption**

Protect wireless access to the system using authentication of [Selection (1 or more): users; devices] and encryption.

Discussion: Wireless networking capabilities represent a significant potential vulnerability that can be exploited by adversaries. To protect systems with wireless access points, strong authentication of users and devices along with strong encryption can reduce susceptibility to threats by adversaries involving wireless technologies.

Related controls and activities: SC-08, SC-12, SC-13.

(02) **Wireless access: Monitoring unauthorized connections**

Withdrawn: Incorporated into SI-04.

(03) **Wireless access: Disable wireless networking**

Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.

Discussion: Wireless networking capabilities that are embedded within system components represent a significant potential vulnerability that can be exploited by adversaries. Disabling wireless capabilities when not needed for essential organizational missions or functions can reduce susceptibility to threats by adversaries involving wireless technologies.

Related controls and activities: None.

(04) **Wireless access: Restrict configurations by users**

Identify and explicitly authorize users allowed to independently configure wireless networking capabilities.

Discussion: Organizational authorizations to allow selected users to configure wireless networking capabilities are enforced, in part, by the access enforcement mechanisms employed within organizational systems.

Related controls and activities: SC-07, SC-15.

(05) **Wireless access: Antennas and transmission power levels**

Select radio antennas and calibrate transmission power levels to reduce the probability that signals from wireless access points can be received outside of organization-controlled boundaries.

Discussion: Actions that may be taken to limit unauthorized use of wireless communications outside of organization-controlled boundaries include reducing the power of wireless transmissions so that the transmissions are less likely to emit a signal that can be captured outside of the physical perimeters of the organization, employing measures such as emissions security to control wireless emanations, and using directional or beamforming antennas that reduce the likelihood that unintended receivers will be able to intercept signals. Prior to taking such mitigating actions, organizations can conduct periodic wireless surveys to understand the radio frequency profile of organizational systems as well as other systems that may be operating in the area.

Related controls and activities: PE-19.

References:

- [Security requirements for wireless local area networks \(ITSG-41\)](#)
- [Guidance on securely configuring network protocols \(ITSP.40.062\)](#)
- Criteria for the design, fabrication, supply, installation and acceptance testing of walk-in, radio-frequency-shielded enclosures (ITSG-02) (available upon request from the Cyber Centre's Contact Centre by email at contact@cyber.gc.ca or by phone at 1-833-CYBER-88 (1-833-292-3788))

AC-19 Access control for mobile devices

Control:

- Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas
- Authorize the connection of mobile devices to organizational systems

Discussion: A mobile device is a computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection; possesses local, non-removable or removable data storage; and includes a self-contained power source. Mobile device functionality may also include voice communication capabilities, on-board sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones and tablets.

Mobile devices are typically associated with a single individual, with some information defined as personal. For example, mobile devices can triangulate access enabling identification of the individual's geolocation. In addition, some work-issued mobile devices enable personal profiles. Government departments should establish policies and procedures to document the custody and control of personal transactions completed in the personal profile, on work-issued mobile devices.

The processing, storage, and transmission capability of the mobile device may be comparable to or merely a subset of notebook/desktop systems, depending on the nature and intended purpose of the device. Protection and control of mobile devices is behaviour or policy-based and requires users to take physical action to protect and control such devices when outside of controlled areas. Controlled areas are spaces for which organizations provide physical or procedural controls to meet the requirements established for protecting information and systems.

Due to the large variety of mobile devices with different characteristics and capabilities, organizational restrictions may vary for the different classes or types of such devices. Usage restrictions and specific implementation guidance for mobile devices include configuration management, device identification and authentication, implementation of mandatory protective software, scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware.

Usage restrictions and authorization to connect may vary among organizational systems. For example, the organization may authorize the connection of mobile devices to its network and impose a set of usage restrictions, while a system owner may

withhold authorization for mobile device connection to specific applications or impose additional usage restrictions before allowing mobile device connections to a system. Adequate security for mobile devices goes beyond the requirements specified in AC-19. Many safeguards for mobile devices are reflected in other controls. AC-20 addresses mobile devices that are not organization-controlled. AC-08 lists the notice requirements for collection of personal information associated with the use of government-issued work cell phones.

Related controls and activities: AC-03, AC-04, AC-07, AC-08, AC-11, AC-17, AC-18, AC-20, CA-09, CM-02, CM-06, IA-02, IA-03, MP-02, MP-04, MP-05, MP-07, PL-04, SC-07, SC-34, SC-43, SI-03, SI-04.

Enhancements:

(01) **Access control for mobile devices: Use of writeable and portable storage devices**

Withdrawn: Incorporated into MP-07.

(02) **Access control for mobile devices: Use of personally owned portable storage devices**

Withdrawn: Incorporated into MP-07.

(03) **Access control for mobile devices: Use of portable storage devices with no identifiable owner**

Withdrawn: Incorporated into MP-07.

(04) **Access control for mobile devices: Restrictions for classified information**

- a. Prohibit the use of unclassified mobile devices in facilities containing systems processing, storing, or transmitting classified information unless specifically permitted by the authorizing official
- b. Enforce the following restrictions on individuals permitted by the authorizing official to use unclassified mobile devices in facilities containing systems processing, storing, or transmitting classified information
 - 1) connection of unclassified mobile devices to classified systems is prohibited
 - 2) connection of unclassified mobile devices to unclassified systems requires approval from the authorizing official
 - 3) use of internal or external modems or wireless interfaces within the unclassified mobile devices is prohibited
 - 4) unclassified mobile devices and the information stored on those devices are subject to random reviews and inspections by [Assignment: organization-defined security officials], and if classified information is found, the incident handling policy is followed
- c. Restrict the connection of classified mobile devices to classified systems in accordance with [Assignment: organization-defined security policies]

Discussion: None.

Related controls and activities: CM-08, IR-04.

(05) **Access control for mobile devices: Full device or container-based encryption**

Employ [Selection: full-device encryption; container-based encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices].

Discussion: Container-based encryption provides a more fine-grained approach to data and information encryption on mobile devices, including encrypting selected data structures such as files, records, or fields.

Related controls and activities: SC-12, SC-13, SC-28.

(400) **Access control for mobile devices: Wireless devices**

Withdrawn: Moved to SC-42(400).

References:

- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [Security requirements for wireless local area networks \(ITSG-41\)](#)
- [Security Considerations for mobile device deployments \(ITSAP.70.002\)](#)
- Security configurations and best practices to protect your mobile device (ITSM.80.002)
- [Securing the enterprise for mobility \(ITSM.80.001\)](#)

AC-20 Use of external systems

Control:

- A. [Selection (1 or more): Establish [Assignment: organization-defined terms and conditions]; Identify [Assignment: organization-defined controls asserted to be implemented on external systems]], consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to
 1. access the system from external systems
 2. process, store, or transmit organization-controlled information using external systems
- B. Prohibit the use of [Assignment: organizationally-defined types of external systems]

Discussion: External systems are systems that are used by but are not part of organizational systems, and for which the organization has no direct control over the implementation of required controls or the assessment of control effectiveness. External systems include personally owned systems, components, or devices; privately owned computing and communications devices in commercial or public facilities; systems owned or controlled by non-federal organizations; systems managed by contractors; and federal information systems that are not owned by, operated by, or under the direct supervision or authority of the organization. External systems also include systems owned or operated by other components within the same organization and systems within the organization with different authorization boundaries. Organizations have the option to prohibit the use of any type of external system or prohibit the use of specified types of external systems (e.g., prohibit the use of any external system that is not organizationally owned or prohibit the use of personally owned systems).

For some external systems (i.e., systems operated by other organizations), the trust relationships that have been established between those organizations and the originating organization may be such that no explicit terms and conditions are required. Systems within these organizations may not be considered external. These situations occur when, for example, there are pre-existing information exchange agreements (either implicit or explicit) established between organizations or components or when such agreements are specified by applicable laws, Orders in Council, directives, regulations, policies, or standards.

Authorized individuals include organizational personnel, contractors, or other individuals with authorized access to organizational systems and over which organizations have the authority to impose specific rules of behaviour regarding system access. Restrictions that organizations impose on authorized individuals need not be uniform, as the restrictions may vary depending on trust relationships between organizations. Therefore, organizations may choose to impose different security restrictions on contractors than on provincial, territorial, or municipal governments.

External systems used to access public interfaces to organizational systems are outside the scope of AC-20. Organizations establish specific terms and conditions for the use of external systems in accordance with organizational security policies and procedures. At a minimum, terms and conditions address the specific types of applications that can be accessed on organizational systems from external systems and the highest security category of information that can be processed,

stored, or transmitted on external systems. If the terms and conditions with the owners of the external systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems.

Related controls and activities: AC-02, AC-03, AC-17, AC-19, CA-03, PL-02, PL-04, SA-09, SC-07.

Enhancements:

(01) Use of external systems: Limits on authorized use

Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after

- a. verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans
- b. retention of approved system connection or processing agreements with the organizational entity hosting the external system

Discussion: Limiting authorized use recognizes circumstances where individuals using external systems may need to access organizational systems. Organizations need assurance that the external systems contain the necessary controls so as to not compromise, damage, or otherwise harm organizational systems. Verification that the required controls have been implemented can be achieved by external, independent assessments, attestations, or other means, depending on the confidence level required by organizations.

Related controls and activities: CA-02.

(02) Use of external systems: Portable storage devices – restricted use

Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using [Assignment: organization-defined restrictions].

Discussion: Limits on the use of organization-controlled portable storage devices in external systems include restrictions on how the devices may be used and under what conditions the devices may be used.

Related controls and activities: MP-07, SC-41.

(03) Use of external systems: Non-organizationally owned systems – restricted use

Restrict the use of non-organizationally owned systems or system components to process, store, or transmit organizational information using [Assignment: organization-defined restrictions].

Discussion: Non-organizationally owned systems or system components include systems or system components owned by other organizations as well as personally owned devices. There are potential risks to using non-organizationally owned systems or components. In some cases, the risk is sufficiently high as to prohibit such use (see AC-20B.). In other cases, the use of such systems or system components may be allowed but restricted in some way.

Restrictions include requiring the implementation of approved controls prior to authorizing the connection of non-organizationally owned systems and components; limiting access to types of information, services, or applications; using virtualization techniques to limit processing and storage activities to servers or system components provisioned by the organization; and agreeing to the terms and conditions for usage. Organizations consult with the Office of the Privacy Commissioner (OPC) of Canada regarding legal issues associated with using personally owned devices, including requirements for conducting forensic analyses during investigations after an incident.

Related controls and activities: None.

(04) Use of external systems: Network accessible storage devices – prohibited use

Prohibit the use of [Assignment: organization-defined network accessible storage devices] in external systems.

Discussion: Network-accessible storage devices in external systems include online storage devices in public, hybrid, or community cloud-based systems.

Related controls and activities: None.

(05) **Use of external systems: Portable storage devices – prohibited use**

Prohibit the use of organization-controlled portable storage devices by authorized individuals on external systems.

Discussion: Limits on the use of organization-controlled portable storage devices in external systems include a complete prohibition of the use of such devices. Prohibiting such use is enforced using technical methods and/or nontechnical (i.e., process-based) methods.

Related controls and activities: MP-07, PL-04, PS-06, SC-41.

References:

- [End user device security for bring-your-own-device \(BYOD\) deployment models \(ITSM.70.003\)](#)
- [TBS Directive on Service and Digital, Appendix G: Standard on Enterprise Information Technology Service Common Configurations](#)
- [TBS Directive on Security Management, Appendix J: Standard on Security Categorization](#)

AC-21 Information sharing

Control:

- Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for [Assignment: organization-defined information sharing circumstances where user discretion is required]
- Employ [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing and collaboration decisions

Discussion: Information sharing applies to information that may be restricted in some manner based on some formal or administrative determination. Examples of such information include, contract-sensitive information, protected information, classified information related to special access programs or compartments, privileged information, proprietary information, and personal information. Security and privacy risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to these determinations.

Depending on the circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, security category, or special access program or compartment. Access restrictions may require non-disclosure agreements and access rights should be defined at the recipient organization based on permissible uses of the information and a demonstrated need-to-know. Information shared should be limited to the least amount of information required by the recipient organization. Information flow techniques and security attributes may be used to provide automated assistance to users making sharing and collaboration decisions.

Related controls and activities: AC-03, AC-04, AC-08, AC-16, PT-02, PT-07, RA-03, SC-15.

Enhancements:

(01) **Information sharing: Automated decision support**

Employ [Assignment: organization-defined automated mechanisms] to enforce information-sharing decisions by authorized users based on access authorizations of sharing partners and access restrictions on information to be shared.

Discussion: Automated mechanisms are used to enforce information sharing decisions.

Related controls and activities: None.

(02) **Information sharing: Information search and retrieval**

Implement information search and retrieval services that enforce [Assignment: organization-defined information sharing restrictions].

Discussion: Information search and retrieval services identify information system resources relevant to an information need.

Related controls and activities: None.

(400) **Information sharing: Information sharing agreement**

Ensure through written agreements the appropriate safeguarding of sensitive information shared with external public-sector entities and organizations.

Discussion: An agreement outlines the terms and conditions under which personal information is disclosed between parties and may or may not be legally binding. Ensure that the agreement documents the legislative authorities, permissible uses, and retention standards for the recipient organization.

Related controls and activities: PT-08.

(401) **Information sharing: Information sharing arrangement**

Ensure through written arrangements the appropriate safeguarding of sensitive information shared between and within federal institutions.

Discussion: None.

GC discussion: An arrangement outlines the terms and conditions under which personal information is disclosed between parties and is not legally binding. Ensure that the arrangement documents the legislative authorities, permissible uses, and retention standards for the recipient organization.

Related controls and activities: PT-08.

References:

- [TBS Directive on Security Management: Appendix F: Mandatory Procedures for Security in Contracts and Other Arrangements Control](#)
- [TBS Guidance on Preparing Information Sharing Agreements Involving Personal Information](#)
- [TBS Directive on Privacy Practices](#)

AC-22 Publicly accessible content

Control:

- A. Designate individuals authorized to make information publicly accessible
- B. Train authorized individuals to ensure that publicly accessible information does not contain non-public information
- C. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that non-public information is not included
- D. Review the content on the publicly accessible system for non-public information [Assignment: organization-defined frequency] and remove such information, if discovered

Discussion: In accordance with applicable laws, Orders in Council, directives, policies, regulations, standards, and guidelines, the public is not authorized to have access to non-public information, including personal information, information protected under the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* (PIPEDA), and proprietary information. Publicly accessible content addresses systems that are controlled by the organization and accessible to the public, typically without identification or authentication. Posting information on non-organizational systems (e.g., non-organizational public websites, forums, and social media) is covered by organizational policy. While organizations may have individuals who are responsible for developing and implementing policies about the information that

can be made publicly accessible, publicly accessible content addresses the management of the individuals who make such information publicly accessible.

Related controls and activities: AC-03, AT-02, AT-03, AU-13.

Enhancements: None.

References: None.

AC-23 Data mining protection

Control: Employ [Assignment: organization-defined data mining prevention and detection techniques] for [Assignment: organization-defined data storage objects] to detect and protect against unauthorized data mining.

Discussion: Data mining is an analytical process that attempts to find correlations or patterns in large datasets for the purpose of data or knowledge discovery, at times matching information about the individual across datasets (data matching). Data storage objects include database records and database fields. Sensitive information can be extracted from data mining operations. When information is personal information, it may lead to unanticipated revelations about individuals and give rise to privacy risks. Ahead of any data mining activity, these privacy risks need to be identified, addressed, and when appropriate, mitigated. Prior to performing data mining activities, organizations determine whether such activities are authorized in law.

Data mining prevention and detection techniques include limiting the number and frequency of database queries to increase the work factor needed to determine the contents of databases, limiting types of responses provided to database queries, applying differential privacy techniques or homomorphic encryption, and notifying personnel when atypical database queries or accesses occur. Notification of atypical queries or accesses to the appropriate personnel is essential as they may constitute a privacy or security breach. Data mining protection focuses on protecting information from data mining while such information resides in organizational data stores. In contrast, AU-13 focuses on monitoring for inappropriate releases of organizational information that may have been mined or otherwise obtained from data stores and is available as open-source information.

GC discussion: The creation of personal information is governed by the same restrictions designated in the *Privacy Act* related to the collection of personal information. Organizations may be subject to applicable laws, Orders in Council, directives, regulations, or policies that address data mining requirements. Organizational personnel consult with the appropriate privacy senior official or executive and legal counsel regarding such requirements.

Related controls and activities: PM-12, PT-02.

Enhancements: None.

References: None.

AC-24 Access control decisions

Control: [Selection (1 or more): Establish procedures; Implement mechanisms] to ensure [Assignment: organization-defined access control decisions] are applied to each access request prior to access enforcement.

Discussion: Access control decisions (also known as authorization decisions) occur when authorization information is applied to specific accesses. In contrast, access enforcement occurs when systems enforce access control decisions. While it is common to have access control decisions and access enforcement implemented by the same entity, it is not required, and it is not always an optimal implementation choice. For some architectures and distributed systems, different entities may make access control decisions and enforce access.

Related controls and activities: AC-02, AC-03.

Enhancements:

(01) Access control decisions: Transmit access authorization information

Transmit [Assignment: organization-defined access authorization information] using [Assignment: organization-defined controls] to [Assignment: organization-defined systems] that enforce access control decisions.

Discussion: Authorization processes and access control decisions may occur in separate parts of systems or in separate systems. In such instances, authorization information is transmitted securely (e.g., using cryptographic mechanisms) so that timely access control decisions can be enforced at the appropriate locations. To support the access control decisions, it may be necessary to transmit as part of the access authorization information supporting security and privacy attributes. This is because in distributed systems, there are various access control decisions that need to be made, and different entities make these decisions in a serial fashion, each requiring those attributes to make the decisions. Protecting access authorization information ensures that such information cannot be altered, spoofed, or compromised during transmission.

Related controls and activities: AU-10.

(02) Access control decisions: No user or process identity

Enforce access control decisions based on [Assignment: organization-defined security or privacy attributes] that do not include the identity of the user or process acting on behalf of the user.

Discussion: In certain situations, it is important that access control decisions can be made without information regarding the identity of the users issuing the requests. These are generally instances where preserving individual privacy is of paramount importance. In other situations, user identification information is not needed for access control decisions, and especially in the case of distributed systems, transmitting such information with the needed degree of assurance may be very expensive or difficult to accomplish. MAC, RBAC, ABAC, and label-based control policies, for example, might not include user identity as an attribute.

Related controls and activities: None.

References: None.

AC-25 Reference monitor

Control: Implement a reference monitor for [Assignment: organization-defined access control policies] that is tamper-proof, always invoked, and small enough to be subject to analysis and testing, the completeness of which can be assured.

Discussion: A reference monitor is a set of design requirements on a reference validation mechanism that, as a key component of an operating system, enforces an access control policy over all subjects and objects. A reference validation mechanism is always invoked, tamper-proof, and small enough to be subject to analysis and tests, the completeness of which can be assured (i.e., verifiable). Information is represented internally within systems using abstractions known as data structures. Internal data structures can represent different types of entities, both active and passive. Active entities, also known as subjects, are associated with individuals, devices, or processes acting on behalf of individuals. Passive entities, also known as objects, are associated with data structures, such as records, buffers, communications ports, tables, files, and inter-process pipes.

Reference monitors enforce access control policies that restrict access to objects based on the identity of subjects or groups to which the subjects belong. The system enforces the access control policy based on the rule set established by the policy. The tamper-proof property of the reference monitor prevents determined adversaries from compromising the functioning of the reference validation mechanism. The always invoked property prevents adversaries from bypassing the mechanism and violating the security policy. The smaller size helps to ensure completeness in the analysis and testing of the mechanism to detect any weaknesses or deficiencies (i.e., latent flaws) that would prevent the enforcement of the security policy.

Related controls and activities: AC-03, AC-08, AC-16, SA-08, SA-17, SC-03, SC-11, SC-39, SI-13.

Enhancements: None.

References: None.

Family: Awareness and training

The controls and activities in the Awareness and training (AT) family deal with the education of users with respect to the security of the system.

AT-01 Awareness and training policy and procedures

Activity:

- A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]
 1. [Selection (1 or more): Organization-level; Mission/business process-level; System-level] awareness and training policy that
 - a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
 - b. is consistent with applicable laws, jurisprudence, Orders in Council, directives, regulations, policies, standards, and guidelines
 2. procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls
- B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the awareness and training policy and procedures
- C. Review and update the current awareness and training
 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]
 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]

Discussion: Awareness and training policy and procedures address the controls in the AT family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of awareness and training policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may prevent the need for mission- or system-specific policies and procedures. The approach to awareness and training can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations.

Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.

Events that may precipitate an update to awareness and training policy and procedures include assessment or audit findings, security or privacy incidents or breaches, or changes in applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related controls and activities: PM-09, PS-08, SI-02, SI-12.

Enhancements: None.

References:

- [TBS Directive on Security Management, Appendix H: Mandatory Procedures for Security Awareness and Training Control](#)
- [TBS Policy on Privacy Protection](#)

- [TBS Directive on Privacy Practices](#)
- [TBS Directive on Personal Information Requests and Correction of Personal Information](#)
- [Top 10 IT security actions: #6 provide tailored cyber security training \(ITSM.10.093\)](#)

AT-02 Literacy training and awareness

Control:

- A. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors)
 1. as part of initial training for new users and [Assignment: organization-defined frequency] thereafter
 2. when required by system changes or following [Assignment: organization-defined events]
- B. Employ the following techniques to increase the security and privacy awareness of system users [Assignment: organization-defined awareness techniques]
- C. Update literacy training and awareness content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]
- D. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques

Discussion: Organizations provide basic and advanced levels of literacy training to system users, including measures to test the knowledge level of users. As needed, organizations may supplement the content of literacy training and awareness based on specific organizational requirements, the systems to which personnel have authorized access, and work environments (e.g., telework). The content includes an understanding of the need for security and privacy as well as actions by users to maintain security and protect personal information as well as to respond to suspected incidents. The content addresses the need for operations security and the handling of personal information.

Awareness techniques include displaying posters, offering supplies inscribed with security and privacy reminders, displaying logon screen messages, generating email advisories or notices from organizational officials, and conducting awareness events. Literacy training after the initial training described in AT-02A.1 is conducted at a minimum frequency consistent with directives, and policies. Subsequent literacy training may be satisfied by one or more short ad hoc sessions and include topical information on recent attack schemes, changes to organizational security and privacy policies, revised security and privacy expectations, or a subset of topics from the initial training.

Updating literacy training and awareness content on a regular basis helps to ensure that the content remains relevant. Events that may precipitate an update to literacy training and awareness content include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, jurisprudence, Orders in Council, directives, regulations, policies, standards, and guidelines.

GC discussion: Organizations provide privacy content that covers, at minimum, the items addressed in the Mandatory Procedures for Privacy Training of the TBS Directive on Personal Information Requests and Correction of Personal Information.

Related controls and activities: AC-03, AC-17, AC-22, AT-03, AT-04, CP-03, IA-04, IR-02, IR-07, IR-09, PL-04, PM-13, PM-21, PS-07, PT-02, SA-08, SA-16, SA-400.

Enhancements:

(01) Literacy training and awareness: Practical exercises

Provide practical exercises in literacy training that simulate events and incidents.

Discussion: Practical exercises include no-notice social engineering attempts to collect information, gain unauthorized access, or simulate the adverse impact of opening malicious email attachments or invoking, via spear phishing attacks, malicious web links.

Related controls and activities: CA-02, CA-07, CP-04, IR-03.

(02) **Literacy training and awareness: Insider threat**

Provide literacy training on recognizing and reporting potential indicators of insider threat.

Discussion: Potential indicators and possible precursors of insider threat can include behaviours such as inordinate, long-term job dissatisfaction; attempts to gain access to information not required for job performance; unexplained access to financial resources; bullying or harassment of fellow employees; workplace violence; and other serious violations of policies, procedures, directives, regulations, rules, or practices.

Literacy training includes how to communicate the concerns of employees and management regarding potential indicators of insider threat through channels established by the organization and in accordance with established policies and procedures. Organizations may consider tailoring insider threat awareness topics to the role. For example, training for managers may be focused on changes in the behaviour of team members, while training for employees may be focused on more general observations.

Related controls and activities: PM-12.

(03) **Literacy training and awareness: Social engineering and mining**

Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.

Discussion: Social engineering is an attempt to trick an individual into revealing information or taking an action that can be used to breach, compromise, or otherwise adversely impact a system. Social engineering includes phishing, pretexting, impersonation, baiting, quid pro quo, thread-jacking, social media exploitation, and tailgating. Social mining is an attempt to gather information about the organization that may be used to support future attacks. Literacy training includes information on how to communicate the concerns of employees and management regarding potential and actual instances of social engineering and data mining through organizational channels based on established policies and procedures.

Related controls and activities: None.

(04) **Literacy training and awareness: Suspicious communications and anomalous system behaviour**

Provide literacy training on recognizing suspicious communications and anomalous behaviour in organizational systems using [Assignment: organization-defined indicators of malicious code].

Discussion: A well-trained workforce provides another organizational control that can be employed as part of a defence-in-depth strategy to protect against malicious code coming into organizations via email or the web applications. Personnel are trained to look for indications of potentially suspicious email (e.g., receiving an unexpected email, receiving an email containing strange or poor grammar, or receiving an email from an unfamiliar sender that appears to be from a known sponsor or contractor). Personnel are also trained on how to respond to suspicious email or web communications. For this process to work effectively, personnel are trained and made aware of what constitutes suspicious communications.

Training personnel on how to recognize anomalous behaviours in systems can provide organizations with early warning for the presence of malicious code. Recognition of anomalous behaviour by organizational personnel can supplement malicious code detection and protection tools and systems employed by organizations.

Related controls and activities: None.

(05) **Literacy training and awareness: Advanced persistent threat**

Provide literacy training on the advanced persistent threat.

Discussion: An effective way to detect APTs and to preclude successful attacks is to provide specific literacy training for individuals. Threat literacy training includes educating individuals on the various ways that APTs can infiltrate the organization (e.g., through websites, emails, advertisement pop-ups, articles, and social engineering). Effective training includes techniques for recognizing suspicious emails, use of removable systems in non-secure settings, and the potential targeting of individuals at home.

Related controls and activities: None.

(06) **Literacy training and awareness: Cyber threat environment**

- a. Provide literacy training on the cyber threat environment
- b. Reflect current cyber threat information in system operations

Discussion: Since threats continue to change over time, threat literacy training by the organization is dynamic. Moreover, threat literacy training is not performed in isolation from the system operations that support organizational mission and business functions.

Related controls and activities: RA-03.

References:

- [TBS Directive on Security Management, Appendix H: Mandatory Procedures for Security Awareness and Training Control](#)
- [TBS Directive on Personal Information Requests and Correction of Personal Information, Appendix B: Mandatory Procedures for Privacy Training](#)
- [Top 10 IT security actions: #6 provide tailored cyber security training \(ITSM.10.093\)](#)
- [Offer tailored cyber security training to your employees \(ITSAP.10.093\)](#)
- [Introduction to the cyber threat environment](#)

AT-03 Role-based training

Control:

- A. Provide role-based security and privacy training to personnel with the following roles and responsibilities:
[Assignment: organization-defined roles and responsibilities]
 1. before authorizing access to the system, information, or performing assigned duties, and [Assignment: organization-defined frequency] thereafter
 2. when required by system changes
- B. Update role-based training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]
- C. Incorporate lessons learned from internal or external security incidents or breaches into role-based training.

Discussion: Organizations determine the content of training based on the assigned roles and responsibilities of individuals as well as the security and privacy requirements of organizations and the systems to which personnel have authorized access, including technical training specifically tailored for assigned duties.

Roles that may require role-based training include senior leaders or management officials (e.g., head of agency, chief executive officer, chief information officer, senior accountable official for risk management, senior official in the department's security governance, appropriate privacy senior official or executive), system owners; authorizing officials; system security officers; privacy officers; acquisition and procurement officials; enterprise architects; systems engineers; software developers; systems security engineers; privacy practitioners; system, network, and database administrators; auditors; personnel conducting configuration management activities; personnel performing verification and validation

activities; personnel with access to system-level software; control assessors; personnel with contingency planning and incident response duties; personnel with privacy management responsibilities; and personnel with access to personal information.

Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical controls. Role-based training also includes policies, procedures, tools, methods, and artifacts for the defined security and privacy roles. Organizations provide the training necessary for individuals to fulfill their responsibilities related to operations and supply chain risk management within the context of organizational security and privacy programs. Role-based training also applies to contractors who provide services to federal agencies.

Types of training include web-based and computer-based training, classroom-style training, and hands-on training (including micro-training). Updating role-based training on a regular basis helps to ensure that the content remains relevant and effective. Events that may precipitate an update to role-based training content include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines.

GC discussion: Ensure that employees of government institutions receive privacy training as outlined in Appendix B of the TBS Directive on Personal Information Requests and Correction of Personal Information.

Related controls and activities: AC-03, AC-17, AC-22, AT-02, AT-04, CP-03, IR-02, IR-04, IR-07, IR-09, PL-04, PM-13, PM-23, PS-07, PS-09, SA-03, SA-08, SA-11, SA-16, SR-05, SR-06, SR-11.

Enhancements:

(01) **Role-based training: Environmental controls**

Provide [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of environmental controls.

Discussion: Environmental controls include fire suppression and detection devices or systems, sprinkler systems, handheld fire extinguishers, fixed fire hoses, smoke detectors, temperature or humidity, heating, ventilation, air conditioning, and power within the facility.

Related controls and activities: PE-01, PE-11, PE-13, PE-14, PE-15.

(02) **Role-based training: Physical security controls**

Provide [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of physical security controls.

Discussion: Physical security controls include physical access control devices, physical intrusion and detection alarms, operating procedures for facility security guards, and monitoring or surveillance equipment.

Related controls and activities: PE-02, PE-03, PE-04.

(03) **Role-based training: Practical exercises**

Provide practical exercises in security and privacy training that reinforce training objectives.

Discussion: Practical exercises for security include training for software developers that addresses simulated attacks that exploit common software vulnerabilities or spear or whale phishing attacks targeted at senior leaders or executives. Practical exercises for privacy include modules with quizzes on identifying personal information, assessing permissible uses of the information and acceptable processes in handling the personal information in various scenarios or scenarios on conducting PIAs.

Related controls and activities: None.

(04) **Role-based training: Suspicious communications and anomalous system behaviour**

Withdrawn: Moved to AT-02(4).

(05) **Role-based training: Handling personal information**

Provide [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of personal information handling and transparency controls.

Discussion: Personal information handling and transparency controls include identifying the organization's authority to collect, use or disclose personal information as well as communicating the authority and handling practices to the individual.

GC discussion: Role-based training for GC departments and agencies addresses the applicable definitions, such as the types of information that may constitute personal information and the risks, considerations, and obligations associated with its handling. Such training also considers the authority to collect and use personal information documented in TBS and institution-specific privacy policies and notices, PIBs, privacy notice statements, PIAs, the *Privacy Act*, contracts, information sharing agreements and arrangements, memoranda of understanding, and/or other documentation. The training covers the responsibilities of employees for the management of personal information and management of privacy breaches. It also addresses the complaints process and review by the courts of GC institutions handling personal information.

Related controls and activities: PT-02, PT-03, PT-05, PT-06.

References:

- [TBS Policy on Government Security](#)
- [TBS Directive on Security Management, Appendix H: Mandatory Procedures for Security Awareness and Training Control](#)
- [TBS Directive on Personal Information Requests and Correction of Personal Information, Appendix B: Mandatory Procedures for Privacy Training](#)

AT-04 Training records

Control:

- Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training
- Retain individual training records for [Assignment: organization-defined time period]

Discussion: Documentation for specialized training may be maintained by individual supervisors at the discretion of the organization.

GC discussion: Library and Archives Canada provides guidance on records retention for GC departments and agencies.

Related controls and activities: AT-02, AT-03, CP-03, IR-02, PM-14, SI-12.

Enhancements: None.

References:

- [TBS Directive on Privacy Practices](#)
- [TBS Directive on Personal Information Requests and Correction of Personal Information](#)

AT-05 Contacts with security groups and associations

Withdrawn: Incorporated into PM-15.

AT-06 Training feedback

Control: Provide feedback on organizational training results to the following personnel [Assignment: organization-defined frequency]: [Assignment: organization-defined personnel].

Discussion: Training feedback includes awareness training results and role-based training results. Training results, especially failures of personnel in critical roles, can be indicative of a potentially serious problem. Therefore, it is important that senior managers are made aware of such situations so that they can take appropriate response actions. Training feedback supports the evaluation and update of organizational training described in AT-02B and AT-03B.

GC discussion: Collection of individual's personal opinions and views related to training is considered to be personal information; as such, notice should be provided to respondents participating in the feedback process.

Related controls and activities: None.

Enhancements: None.

References: [TBS Directive on Privacy Practices](#)

Family: Audit and accountability

The controls and activities in the Audit and accountability (AU) family support the ability to collect, analyze, and store audit records associated with user operations performed within the system.

AU-01 Audit and accountability policy and procedures

Activity:

- A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]
 1. [Selection (1 or more): Organization-level; Mission/business process-level; System-level] audit and accountability policy that
 - a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
 - b. is consistent with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines
 2. procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls
- B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the audit and accountability policy and procedures
- C. Review and update the current audit and accountability
 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]
 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]

Discussion: Audit and accountability policy and procedures address the controls in the AU family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of audit and accountability policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may remove the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations.

Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.

Events that may precipitate an update to audit and accountability policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure. Users whose activities are monitored by audit logs should be given notice of the activity.

Related controls and activities: AC-08, PM-09, PS-08, SI-02, SI-12.

Enhancements: None.

References:

- [TBS Policy on Government Security](#)

- [TBS Policy on Internal Audit](#)
- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- Directive for the Control of COMSEC Material in the Government of Canada (ITSD-03A) (upon request to the Cyber Centre)
- Directive for the Control of COMSEC Material in the Canadian Private Sector (ITSD-06A) (upon request to the Cyber Centre)
- [CSE-RCMP Harmonized Threat and Risk Assessment Methodology \(TRA-1\)](#)

AU-02 Event logging

Control:

- Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]
- Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged
- Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-02A.) along with the frequency of (or situation requiring) logging for each identified event type]
- Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents
- Review and update the event types selected for logging [Assignment: organization-defined frequency]

Discussion: An event is an observable occurrence in a system. The types of events that require logging are those events that are significant and relevant to the security of systems and the privacy of individuals. Event logging also supports specific monitoring and auditing needs. Event types include password changes, failed logons or failed accesses related to systems, security or privacy attribute changes, accessing or viewing personal information, administrative privilege usage, digital credential usage, data action changes, query parameters, or external credential usage. In determining the set of event types that require logging, organizations consider the monitoring and auditing appropriate for each of the controls to be implemented. For completeness, event logging includes all protocols that are operational and supported by the system.

To balance monitoring and auditing requirements with other system needs, event logging requires identifying the subset of event types that are logged at a given point in time. For example, organizations may determine that systems need the capability to log every file access successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance.

The types of events that organizations desire to be logged may change. Reviewing and updating the set of logged events is necessary to help ensure that the events remain relevant and continue to support the needs of the organization. Organizations should consider how the types of logging events can reveal information about individuals that may give rise to privacy risk and how best to mitigate such risks. For example, there is the potential to reveal personal information in the audit trail, especially if the logging event is based on patterns or time of usage.

Event logging requirements, including the need to log specific event types, may be referenced in other controls and control enhancements. These include AC-02(04), AC-03(10), AC-06(09), AC-17(01), CM-03F, CM-05(01), IA-03(03)b, MA-04(01), MP-04(02), PE-03, PM-21, PT-07, RA-08, SC-07(09), SC-07(15), SI-03(08), SI-04(22), SI-07(08), and SI-10(01). Organizations include event types that are required by applicable laws, Orders in Council, directives, policies, regulations, standards, and guidelines. Audit records can be generated at various levels, including at the packet level as information traverses the network. Selecting the appropriate level of event logging is an important part of a monitoring and auditing capability and can identify the root causes of problems. When defining event types, organizations consider the logging necessary to cover

related event types, such as the steps in distributed, transaction-based processes and the actions that occur in service-oriented architectures.

Related controls and activities: AC-02, AC-03, AC-06, AC-07, AC-08, AC-16, AC-17, AU-03, AU-04, AU-05, AU-06, AU-07, AU-11, AU-12, CM-03, CM-05, CM-06, CM-13, IA-03, MA-04, MP-04, PE-03, PM-21, PT-02, PT-07, RA-08, SA-08, SA-15, SC-07, SC-18, SI-02, SI-03, SI-04, SI-07, SI-10, SI-11.

Enhancements:

(01) **Event logging: Compilation of audit records from multiple sources**

Withdrawn: Incorporated into AU-12.

(02) **Event logging: Selection of audit events by component**

Withdrawn: Incorporated into AU-12.

(03) **Event logging: Reviews and updates**

Withdrawn: Incorporated into AU-02.

(04) **Event logging: Privileged functions**

Withdrawn: Incorporated into AC-06(09).

References:

- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [TBS Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice \(SPIN\)](#)
- [TBS Directive on Service and Digital, Appendix C: Mandatory Procedures for Privacy and Monitoring of Network and Device Use Information Notices](#)
- [TBS Policy on Privacy Protection](#)
- [TBS Directive on Privacy Practices](#)

AU-03 Content of audit records

Control: Ensure that audit records contain information that establishes the following:

- what type of event occurred
- when the event occurred
- where the event occurred
- source of the event
- outcome of the event
- identity of any individuals, subjects, objects or entities associated with the event

Discussion: Audit record content that may be necessary to support the auditing function includes event descriptions (item A), time stamps (item B), source and destination addresses (item C), user or process identifiers (items D and F), success or fail indications (item E), and file names involved (items A, C, E, and F).

Event outcomes include indicators of event success or failure and event-specific results, such as the system security and privacy posture after the event occurred. Organizations consider how audit records can reveal information about individuals that may give rise to privacy risks and how best to mitigate such risks. For example, there is the potential to reveal personal information in the audit trail, especially if the trail records inputs or is based on patterns or time of usage.

GC discussion: GC departments and agencies ensure that the content of audit records aligns with the Security Incidents and Privacy Breaches PIBs.

Related controls and activities: AU-02, AU-08, AU-12, AU-14, MA-04, PL-09, SA-08, SA-15, SI-07, SI-11.

Enhancements:

(01) **Content of audit records: Additional audit information**

Generate audit records containing the following additional information: [Assignment: organization-defined additional information].

Discussion: The ability to add information generated in audit records is dependent on system functionality to configure the audit record content. Organizations may consider additional information in audit records including, but not limited to, access control or flow control rules invoked and individual identities of group account users.

Organizations may also consider limiting additional audit record information to only information that is explicitly needed for audit requirements. This facilitates the use of audit trails and audit logs by not including information in audit records that could potentially be misleading, make it more difficult to locate information of interest, or increase the risk to individuals' privacy.

Related controls and activities: None.

(02) **Content of audit records: Centralized management of planned audit record content**

Withdrawn: Incorporated into PL-09.

(03) **Content of audit records: Limit personal information elements**

Limit personal information contained in audit records to the following elements identified in the PIA: [Assignment: organization-defined elements].

Discussion: Limiting personal information in audit records when such information is not needed for operational purposes helps reduce the level of privacy risk created by a system.

Related controls and activities: RA-03.

References:

- [TBS Directive on Service and Digital, Appendix C: Mandatory Procedures for Privacy and Monitoring of Network and Device Use Information Notices](#)
- [TBS Directive on Privacy Practices](#)
- [TBS Policy on Access to Information](#)
- [TBS Directive on Access to Information Requests](#)
- [TBS Directive on Personal Information Requests and Correction of Personal Information](#)
- [TBS Event Logging Guidance, Appendix A: Recommended Events to Log](#)

AU-04 Audit log storage capacity

Control: Allocate audit log storage capacity to accommodate [Assignment: organization-defined audit log retention requirements].

Discussion: Organizations consider the types of audit logging to be performed and the audit log processing requirements when allocating audit log storage capacity. Allocating sufficient audit log storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of audit logging capability.

Related controls and activities: AU-02, AU-05, AU-06, AU-07, AU-09, AU-11, AU-12, AU-14, SI-04.

Enhancements:

(01) **Audit log storage capacity: Transfer to alternate storage**

Transfer audit logs [Assignment: organization-defined frequency] to a different system, system component, or media other than the system or system component conducting the logging.

Discussion: Audit log transfer, also known as offloading, is a common process in systems with limited audit log storage capacity and thus supports availability of the audit logs. The initial audit log storage is only used in a transitory fashion until the system can communicate with the secondary or alternate system allocated to audit log storage, at which point the audit logs are transferred. Transferring audit logs to alternate storage is similar to AU-09(02) in that audit logs are transferred to a different entity. However, the purpose of selecting AU-09(02) is to protect the confidentiality and integrity of audit records. Organizations can select either control enhancement to obtain the benefit of increased audit log storage capacity and preserving the confidentiality, integrity, and availability of audit records and logs.

Related controls and activities: None.

References:

- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)

AU-05 Response to audit logging process failures

Control:

- Alert [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] in the event of an audit logging process failure
- Take the following additional actions: [Assignment: organization-defined additional actions]

Discussion: Audit logging process failures include software and hardware errors, failures in audit log capturing mechanisms, and reaching or exceeding audit log storage capacity. Organization-defined actions include overwriting oldest audit records, shutting down the system, and stopping the generation of audit records. Organizations may choose to define additional actions for audit logging process failures based on the type of failure, the location of the failure, the severity of the failure, or a combination of such factors.

When the audit logging process failure is related to storage, the response is carried out for the audit log storage repository (i.e., the distinct system component where the audit logs are stored), the system on which the audit logs reside, the total audit log storage capacity of the organization (i.e., all audit log storage repositories combined), or all three. Organizations may decide to take no additional actions after alerting designated roles or personnel.

Related controls and activities: AU-02, AU-04, AU-07, AU-09, AU-11, AU-12, AU-14, SI-04, SI-12.

Enhancements:

(01) Response to audit logging process failures: Storage capacity warning

Provide a warning to [Assignment: organization-defined personnel, roles, and/or locations] within [Assignment: organization-defined time period] when allocated audit log storage volume reaches [Assignment: organization-defined percentage] of repository maximum audit log storage capacity.

Discussion: Organizations may have multiple audit log storage repositories distributed across multiple system components with each repository having different storage volume capacities.

Related controls and activities: None.

(02) Response to audit logging process failures: Real-time alerts

Provide an alert within [Assignment: organization-defined real-time period] to [Assignment: organization-defined personnel, roles, and/or locations] when the following audit failure events occur: [Assignment: organization-defined audit logging failure events requiring real-time alerts].

Discussion: Alerts provide organizations with urgent messages. Real-time alerts provide these messages at information technology speed (i.e., the time from event detection to alert occurs in seconds or less).

Related controls and activities: None.

(03) **Response to audit logging process failures: Configurable traffic volume thresholds**

Enforce configurable network communications traffic volume thresholds reflecting limits on audit log storage capacity and [Selection (1): reject; delay] network traffic above those thresholds.

Discussion: Organizations have the capability to reject or delay the processing of network communications traffic if audit logging information about such traffic is determined to exceed the storage capacity of the system audit logging function. The rejection or delay response is triggered by the established organizational traffic volume thresholds that can be adjusted based on changes to audit log storage capacity.

Related controls and activities: None.

(04) **Response to audit logging process failures: Shutdown on failure**

Invoke a [Selection (1): full system shutdown; partial system shutdown; degraded operational mode with limited mission or business functionality available] in the event of [Assignment: organization-defined audit logging failures] unless an alternate audit logging capability exists.

Discussion: Organizations determine the types of audit logging failures that can trigger automatic system shutdowns or degraded operations. Because of the importance of ensuring mission and business continuity, organizations may determine that the nature of the audit logging failure is not so severe that it warrants a complete shutdown of the system supporting the core organizational mission and business functions. In those instances, partial system shutdowns or operating in a degraded mode with reduced capability may be viable alternative.

Related controls and activities: AU-15.

(05) **Response to audit logging process failures: Alternate audit logging capability**

Provide an alternate audit logging capability in the event of a failure in primary audit logging capability that implements [Assignment: organization-defined alternate audit logging functionality].

Discussion: Since an alternate audit logging capability may be a short-term protection solution employed until the failure in the primary audit logging capability is corrected, organizations may determine that the alternate audit logging capability need only provide a subset of the primary audit logging functionality that is impacted by the failure.

Related controls and activities: AU-09.

References: None.

AU-06 Audit record review, analysis, and reporting

Control:

- A. Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity] and the potential impact of the inappropriate or unusual activity
- B. Report findings to [Assignment: organization-defined personnel or roles]
- C. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information

Discussion: Audit record review, analysis, and reporting covers information security-related and privacy-related logging performed by organizations, including logging that results from the monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and

non-local maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at system interfaces, and use of mobile code or Voice over Internet Protocol (VoIP).

Findings can be reported to organizational entities that include the incident response team, help desk, and security or privacy offices. Where possible, personal information should be removed from audit logs if the personal information is not required for reporting processes. If organizations are prohibited from reviewing and analyzing audit records or unable to conduct such activities, the review or analysis may be carried out by other organizations granted such authority. The frequency, scope, and/or depth of the audit record review, analysis, and reporting may be adjusted to meet organizational needs based on new information received.

Related controls and activities: AC-02, AC-03, AC-05, AC-06, AC-07, AC-17, AU-07, AU-16, CA-02, CA-07, CM-02, CM-05, CM-06, CM-10, CM-11, IA-02, IA-03, IA-05, IA-08, IR-05, MA-04, MP-04, PE-03, PE-06, RA-05, SA-08, SC-07, SI-03, SI-04, SI-07.

Enhancements:

(01) Audit record review, analysis, and reporting: Automated process integration

Integrate audit record review, analysis, and reporting processes using [Assignment: organization-defined automated mechanisms].

Discussion: Organizational processes that benefit from integrated audit record review, analysis, and reporting include incident response, continuous monitoring, contingency planning, investigation and response to suspicious activities, and Office of the Auditor General audits.

Related controls and activities: PM-07.

(02) Audit record review, analysis, and reporting: Automated security alerts

Withdrawn: Incorporated into SI-04.

(03) Audit record review, analysis, and reporting: Correlate audit record repositories

Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

Discussion: Organization-wide situational awareness includes awareness across all three levels of risk management (i.e., organizational level, mission/business process level, and information system level) and supports cross-organization awareness.

Related controls and activities: AU-12, IR-04.

(04) Audit record review, analysis, and reporting: Central review and analysis

Provide and implement the capability to centrally review and analyze audit records from multiple components within the system.

Discussion: Automated mechanisms for centralized reviews and analyses include Security Information and Event Management (SIEM) products.

Related controls and activities: AU-02, AU-12.

(05) Audit record review, analysis, and reporting: Integrated analysis of audit records

Integrate analysis of audit records with analysis of [Selection (1 or more): vulnerability scanning information; performance data; system monitoring information; [Assignment: organization-defined data/information collected from other sources]] to further enhance the ability to identify inappropriate or unusual activity.

Discussion: Integrated analysis of audit records does not require vulnerability scanning, the generation of performance data, or system monitoring. Rather, integrated analysis requires that the analysis of information generated by scanning, monitoring, or other data collection activities is integrated with the analysis of audit record information. SIEM tools can facilitate audit record aggregation or consolidation from multiple system components as well as audit record correlation and analysis.

The use of standardized audit record analysis scripts developed by organizations (with localized script adjustments, as necessary) provides more cost-effective approaches for analyzing audit record information collected. The correlation of audit record information with vulnerability scanning information is important in determining the veracity of vulnerability scans of the system and in correlating attack detection events with scanning results.

Correlation with performance data can uncover denial-of-service attacks or other types of attacks that result in the unauthorized use of resources. Correlation with system monitoring information can assist in uncovering attacks and in better relating audit information to operational situations.

Related controls and activities: AU-12, IR-04.

(06) **Audit record review, analysis, and reporting: Correlation with physical monitoring**

Correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

Discussion: The correlation of physical audit record information and the audit records from systems may assist organizations in identifying suspicious behaviour or supporting evidence of such behaviour. For example, the correlation of an individual's identity for logical access to certain systems with the additional physical security information that the individual was present at the facility when the logical access occurred may be useful in investigations.

Related controls and activities: None.

(07) **Audit record review, analysis, and reporting: Permitted actions**

Specify the permitted actions for each [Selection (1 or more): system process; role; user] associated with the review, analysis, and reporting of audit record information.

Discussion: Organizations specify permitted actions for system processes, roles, and users associated with the review, analysis, and reporting of audit records through system account management activities. Specifying permitted actions on audit record information is a way to enforce the principle of least privilege. Permitted actions are enforced by the system and include read, write, execute, append, and delete.

Related controls and activities: None.

(08) **Audit record review, analysis, and reporting: Full text analysis of privileged commands**

Perform a full text analysis of logged privileged commands in a physically distinct component or subsystem of the system, or other system that is dedicated to that analysis.

Discussion: Full text analysis of privileged commands requires a distinct environment for the analysis of audit record information related to privileged users without compromising such information on the system where the users have elevated privileges, including the capability to execute privileged commands. Full text analysis refers to analysis that considers the full text of privileged commands (i.e., commands and parameters) as opposed to analysis that considers only the name of the command. Full text analysis includes the use of pattern matching and heuristics.

Related controls and activities: AU-03, AU-09, AU-11, AU-12.

(09) **Audit record review, analysis, and reporting: Correlation with information from nontechnical sources**

Correlate information from nontechnical sources with audit record information to enhance organization-wide situational awareness.

Discussion: Nontechnical sources include records that document organizational policy violations related to harassment incidents and the improper use of information assets. Such information can lead to a directed analytical effort to detect potential malicious insider activity. Organizations limit access to information that is available from nontechnical sources due to its sensitive nature. Limited access minimizes the potential for inadvertent release of personal information to individuals who do not have a need to know. The correlation of information from

nontechnical sources with audit record information generally occurs only when individuals are suspected of being involved in an incident. Organizations obtain legal advice prior to initiating such actions.

GC discussion: The correlation of information from nontechnical sources with audit record information may be considered to be data matching, as defined in the TBS Policy on Privacy Protection.

Related controls and activities: PM-12.

(10) **Audit record review, analysis, and reporting: Audit level adjustment**

Withdrawn: Incorporated into AU-06.

References:

- [TBS Policy on Government Security](#)
- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [TBS Policy on Privacy Protection](#)

AU-07 Audit record reduction and report generation

Control: Provide and implement an audit record reduction and report generation capability that:

- A. supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents
- B. does not alter the original content or time ordering of audit records

Discussion: Audit record reduction is a process that manipulates collected audit log information and organizes it into a summary format that is more meaningful to analysts. Audit record reduction and report generation capabilities do not always emanate from the same system or from the same organizational entities that conduct audit logging activities. The audit record reduction capability includes modern data mining techniques with advanced data filters to identify anomalous behaviour in audit records. The report generation capability provided by the system can generate customizable reports. Time ordering of audit records can be an issue if the granularity of the time stamp in the record is insufficient.

Related controls and activities: AC-02, AU-02, AU-03, AU-04, AU-05, AU-06, AU-12, AU-16, CM-05, IA-05, IR-04, PM-12, SI-04.

Enhancements:

(01) **Audit record reduction and report generation: Automatic processing**

Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: [Assignment: organization-defined fields within audit records].

Discussion: Events of interest can be identified by the content of audit records, including system resources involved, information objects accessed, identities of individuals, event types, event locations, event dates and times, Internet Protocol addresses involved, or event success or failure. Organizations may define event criteria to any degree of granularity required, such as locations selectable by a general networking location or by specific system component. If personal information is captured on an audit log report and is not required for the resolution of the incident, the personal information should be removed from the report or masked appropriately before circulation of the audit record.

Related controls and activities: None.

(02) **Audit record reduction and report generation : Automatic sort and search**

Withdrawn: Incorporated into AU-07(01).

References: None.

AU-08 Time stamps

Control:

- A. Use internal system clocks to generate time stamps for audit records
- B. Record time stamps for audit records that meet [Assignment: organization-defined granularity of time measurement] and that use Coordinated Universal Time (UTC), have a fixed local time offset from UTC, or that include the local time offset as part of the time stamp

Discussion: Time stamps generated by the system include date and time. Time is commonly expressed in UTC or in local time with an offset from UTC. Granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks (e.g., clocks synchronizing within hundreds of milliseconds or tens of milliseconds). Organizations may define different time granularities for different system components. Time service can be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities.

Related controls and activities: AU-03, AU-12, AU-14, SC-45.

Enhancements:

(01) **Time stamps: Synchronized with authoritative time source**

Withdrawn: Moved to SC-45(01).

(02) **Time stamps: Secondary authoritative time source**

Withdrawn: Moved to SC-45(02).

References: None.

AU-09 Protection of audit information

Control:

- A. Protect audit information and audit logging tools from unauthorized access, modification, and deletion
- B. Alert [Assignment: organization-defined personnel or roles] upon detection of unauthorized access, modification, or deletion of audit information

Discussion: Audit information includes all information needed to successfully audit system activity, such as audit records, audit log settings, audit reports, and personal information. Audit logging tools are those programs and devices used to conduct system audit and logging activities. Protection of audit information focuses on technical protection and limits the ability to access and execute audit logging tools to authorized individuals. Physical protection of audit information is addressed by both media protection controls and physical and environmental protection controls.

Related controls and activities: AC-03, AC-06, AU-06, AU-11, AU-14, AU-15, MP-02, MP-04, PE-02, PE-03, PE-06, SA-08, SC-08, SI-04.

Enhancements:

(01) **Protection of audit information: Hardware write-once media**

Write audit trails to hardware-enforced, write-once media.

Discussion: Writing audit trails to hardware-enforced, write-once media applies to the initial generation of audit trails (i.e., the collection of audit records that represents the information to be used for detection, analysis, and reporting purposes) and to the backup of those audit trails. Writing audit trails to hardware-enforced, write-once media does not apply to the initial generation of audit records prior to being written to an audit trail. Write-once, read-many (WORM) media includes Compact Disc-Recordable (CD-R), Blu-ray Disc Recordable (BD-R), and Digital Versatile Disc-

Recordable (DVD-R). In contrast, the use of switchable write-protection media, such as tape cartridges, Universal Serial Bus (USB) drives, Compact Disc Re-Writeable (CD-RW), and Digital Versatile Disc-Read Write (DVD-RW) results in write-protected but not write-once media.

Related controls and activities: AU-04, AU-05.

(02) **Protection of audit information: Store on separate physical systems or components**

Store audit records [Assignment: organization-defined frequency] in a repository that is part of a physically different system or system component than the system or component being audited.

Discussion: Storing audit records in a repository separate from the audited system or system component helps to ensure that a compromise of the system being audited does not also result in a compromise of the audit records. Storing audit records on separate physical systems or components also preserves the confidentiality and integrity of audit records and facilitates the management of audit records as an organization-wide activity. Storing audit records on separate systems or components applies to initial generation as well as backup or long-term storage of audit records.

Related controls and activities: AU-04, AU-05.

(03) **Protection of audit information: Cryptographic protection**

Implement cryptographic mechanisms to protect the integrity of audit information and audit tools.

Discussion: Cryptographic mechanisms used for protecting the integrity of audit information include signed hash functions using asymmetric cryptography. This enables the distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

Related controls and activities: AU-10, SC-12, SC-13.

(04) **Protection of audit information: Access by subset of privileged users**

Authorize access to management of audit logging functionality to only [Assignment: organization-defined subset of privileged users or roles].

Discussion: Individuals or roles with privileged access to a system and who are also the subject of an audit by that system may affect the reliability of the audit information by inhibiting audit activities or modifying audit records. Requiring privileged access to be further defined between audit-related privileges and other privileges limits the number of users or roles with audit-related privileges.

Related controls and activities: AC-05.

(05) **Protection of audit information: Dual authorization**

Enforce dual authorization for [Selection (1 or more): movement; deletion] of [Assignment: organization-defined audit information].

Discussion: Organizations may choose different selection options for different types of audit information. Dual authorization mechanisms (also known as two-person control) require the approval of 2 authorized individuals to execute audit functions. To reduce the risk of collusion, organizations consider rotating dual authorization duties to other individuals. Organizations do not require dual authorization mechanisms when immediate responses are necessary to ensure public and environmental safety.

Related controls and activities: AC-03.

(06) **Protection of audit information: Read-only access**

Authorize read-only access to audit information to [Assignment: organization-defined subset of privileged users or roles].

Discussion: Restricting privileged user or role authorizations to read-only helps to limit the potential damage to organizations that could be initiated by such users or roles, such as deleting audit records to cover up malicious activity.

Related controls and activities: None.

(07) **Protection of audit information: Store on component with different operating system**

Store audit information on a component running a different operating system than the system or component being audited.

Discussion: Storing auditing information on a system component running a different operating system reduces the risk of a vulnerability specific to the system, resulting in a compromise of the audit records.

Related controls and activities: AU-04, AU-05, AU-11, SC-29.

References:

- [Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B information \(ITSP.40.111\)](#)
- [NIST FIPS 140-3 Security Requirements for Cryptographic Modules](#)
- [NIST FIPS 180-4 Secure Hash Standard \(SHS\)](#)
- [NIST FIPS 202 SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions](#)
- [Network security auditing \(ITSAP.80.086\)](#)

AU-10 Non-repudiation

Control: Provide irrefutable evidence that an individual (or process acting on behalf of an individual) has performed [Assignment: organization-defined actions to be covered by non-repudiation].

Discussion: Types of individual actions covered by non-repudiation include creating information, sending and receiving messages, and approving information. Non-repudiation protects against claims by authors of not having authored certain documents, senders of not having transmitted messages, receivers of not having received messages, and signatories of not having signed documents. Non-repudiation services can be used to determine if information originated from an individual or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request, or receiving specific information). Organizations obtain non-repudiation services by employing various techniques or mechanisms, including digital signatures and digital message receipts.

Related controls and activities: AU-09, PM-12, SA-08, SC-08, SC-12, SC-13, SC-16, SC-17, SC-23.

Enhancements:

(01) **Non-repudiation: Association of identities**

- a. Bind the identity of the information producer with the information to [Assignment: organization-defined strength of binding]
- b. Provide the means for authorized individuals to determine the identity of the producer of the information

Discussion: Binding identities to the information supports audit requirements that provide organizational personnel with the means to identify who produced specific information in the event of an information transfer. Organizations determine and approve the strength of attribute binding between the information producer and the information based on the security category of the information and other relevant risk factors.

Related controls and activities: AC-04, AC-16.

(02) **Non-repudiation: Validate binding of information producer identity**

- a. Validate the binding of the information producer identity to the information at [Assignment: organization-defined frequency]

- b. Perform [Assignment: organization-defined actions] in the event of a validation error

Discussion: Validating the binding of the information producer identity to the information prevents the modification of information between production and review. The validation of bindings can be achieved by, for example, using cryptographic checksums. Organizations determine if validations are in response to user requests or generated automatically.

Related controls and activities: AC-03, AC-04, AC-16.

(03) **Non-repudiation: Chain of custody**

Maintain reviewer or releaser credentials within the established chain of custody for information reviewed or released.

Discussion: Chain of custody is a process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each individual who handled the evidence, the date and time the evidence was collected or transferred, and the purpose for the transfer.

If the reviewer is a human or if the review function is automated but separate from the release or transfer function, the system associates the identity of the reviewer of the information to be released with the information and the information label. In the case of human reviews, maintaining the credentials of reviewers or releasers provides the organization with the means to identify who reviewed and released the information. In the case of automated reviews, it ensures that only approved review functions are used.

Related controls and activities: AC-04, AC-16.

(04) **Non-repudiation: Validate binding of information reviewer identity**

- a. Validate the binding of the information reviewer identity to the information at the transfer or release points prior to release or transfer between [Assignment: organization-defined security domains]
- b. Perform [Assignment: organization-defined actions] in the event of a validation error

Discussion: Validating the binding of the information reviewer identity to the information at transfer or release points prevents the unauthorized modification of information between review and the transfer or release. The validation of bindings can be achieved by using cryptographic checksums. Organizations determine if validations are in response to user requests or generated automatically.

Related controls and activities: AC-04, AC-16.

(05) **Non-repudiation: Digital signatures**

Withdrawn: Incorporated into SI-07.

References:

- [User authentication guidance for information technology systems \(ITSP.30.031\)](#)
- [Implementation guidance: email domain protection \(ITSP.40.065\)](#)
- [TBS Directive on Identity Management, Appendix A: Standard on Identity and Credential Assurance](#)
- [TBS Government of Canada Guidance on Using Electronic Signatures](#)
- [NIST FIPS 140-3 Security Requirements for Cryptographic Modules](#)
- [NIST FIPS 180-4 Secure Hash Standard \(SHS\)](#)
- [NIST FIPS 186-5 Digital Signature Standard \(DSS\)](#)
- [NIST FIPS 202 SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions](#)

AU-11 Audit record retention

Control: Retain audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

Discussion: Organizations retain audit records until it is determined that the records are no longer needed for administrative, legal, audit, or other operational purposes. Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action.

GC discussion: This includes the retention and availability of audit records relative to requests for GC information under the Access to Information Act, requests for personal information under the *Privacy Act*, subpoenas, and law enforcement actions. When audit records include personal information that is used for administrative decision such as an investigation, they must be retained in accordance with the Privacy Regulations. If audit records contain personal information that is not required for the audit process, that personal information should be removed or redacted prior to retention. If audit records rely on personal information and that information is used to make an administrative decision, the minimum retention standard is at least 2 years following the last time the personal information was used for an administrative purpose unless the individual consents to its disposal. Retention standards for personal information associated with this process should be reflected in the standard PIB for Internal Audit. Library and Archives Canada provides federal policy on records retention.

Related controls and activities: AU-02, AU-04, AU-05, AU-06, AU-09, AU-14, MP-06, RA-05, SI-12.

Enhancements:

(01) Audit record retention: Long-term retrieval capability

Employ [Assignment: organization-defined measures] to ensure that long-term audit records generated by the system can be retrieved.

Discussion: Organizations need to access and read audit records requiring long-term storage (on the order of years). Measures employed to help facilitate the retrieval of audit records include converting records to newer formats, retaining equipment capable of reading the records, and retaining the necessary documentation to help personnel understand how to interpret the records.

Related controls and activities: None.

References:

- [TBS Policy on Service and Digital](#)
- [TBS Directive on Service and Digital](#)
- [TBS Directive on Privacy Practices](#)
- [TBS Policy on Access to Information](#)
- [TBS Directive on Access to Information Requests](#)
- [TBS Directive on Personal Information Requests and Correction of Personal Information](#)

AU-12 Audit record generation

Control:

- A. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-02A on [Assignment: organization-defined system components]
- B. Allow [Assignment: organization-defined personnel or roles] to select the event types that are to be logged by specific components of the system
- C. Generate audit records for the event types defined in AU-02C that include the audit record content defined in AU-03

Discussion: Audit records can be generated from many different system components. The event types specified in AU-02D are the event types for which audit logs are to be generated and are a subset of all event types for which the system can generate audit records. If records generated for the audit process contain personal information that is not required for the audit process, that personal information should be removed or redacted.

Related controls and activities: AC-06, AC-17, AU-02, AU-03, AU-04, AU-05, AU-06, AU-07, AU-14, CM-05, MA-04, MP-04, PM-12, SA-08, SC-18, SI-03, SI-04, SI-07, SI-10.

Enhancements:

(01) Audit record generation: System-wide and time-correlated audit trail

Compile audit records from [Assignment: organization-defined system components] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail].

Discussion: Audit trails are time-correlated if the time stamps in the individual audit records can be reliably related to the time stamps in other audit records to achieve a time ordering of the records within organizational tolerances.

Related controls and activities: AU-08, SC-45.

(02) Audit record generation: Standardized formats

Produce a system-wide (logical or physical) audit trail composed of audit records in a standardized format.

Discussion: Audit records that follow common standards promote interoperability and information exchange between devices and systems. Promoting interoperability and information exchange facilitates the production of event information that can be readily analyzed and correlated. If logging mechanisms do not conform to standardized formats, systems may convert individual audit records into standardized formats when compiling system-wide audit trails.

Related controls and activities: None.

(03) Audit record generation: Changes by authorized individuals

Provide and implement the capability for [Assignment: organization-defined individuals or roles] to change the logging to be performed on [Assignment: organization-defined system components] based on [Assignment: organization-defined selectable event criteria] within [Assignment: organization-defined time thresholds].

Discussion: Permitting authorized individuals to make changes to system logging enables organizations to extend or limit logging as necessary to meet organizational requirements. Logging that is limited to conserve system resources may be extended (either temporarily or permanently) to address certain threat situations. In addition, logging may be limited to a specific set of event types to facilitate audit reduction, analysis, and reporting. Organizations can establish time thresholds in which logging actions are changed (e.g., near real-time, within minutes, or within hours).

Related controls and activities: AC-03.

(04) Audit record generation: Query parameter audits of personal information

Provide and implement the capability for auditing the parameters of user query events for data sets containing personal information.

Discussion: Query parameters are explicit criteria that an individual or automated system submits to a system to retrieve data. Auditing of query parameters for datasets that contain personal information augments the capability of an organization to track and understand the access, usage, or sharing of personal information by authorized personnel.

GC discussion: The use of personal information for the audit purpose is authorized without consent of the individual pursuant to 8(2)(h) of the *Privacy Act*.

Related controls and activities: None.

References:

- [TBS Directive on Privacy Practices](#)
- [TBS Policy on Privacy Protection](#)
- [Privacy Act](#)
- [Privacy Regulations SOR/83-508](#)
- [TBS Directive on Service and Digital, Appendix L: Standard for Managing Metadata](#)

AU-13 Monitoring for information disclosure

Control:

- A. Monitor [Assignment: organization-defined open-source information and/or information sites] [Assignment: organization-defined frequency] for evidence of unauthorized disclosure of organizational information
- B. If an information disclosure is discovered
 1. notify [Assignment: organization-defined personnel or roles]
 2. take the following additional actions: [Assignment: organization-defined additional actions]

Discussion: Unauthorized disclosure of information is a form of data leakage.

GC discussion: Federal departments and agencies may engage in proactive review of open-source information for the presence of classified information, related to national security. This process may reveal or require the collection of personal information and requires lawful authority. Where possible, personal identifiers should be redacted, removed, or masked and not stored in organization information holdings. Information may be obtained from Internet sites such as social networking sites, and code-sharing platforms and repositories.

Related controls and activities: AC-22, PE-03, PM-12, RA-05, SC-07, SI-20.

Enhancements:

(01) **Monitoring for information disclosure: Use of automated tools**

Monitor open-source information and information sites using [Assignment: organization-defined automated mechanisms].

Discussion: Automated mechanisms include commercial services that provide notifications and alerts to organizations and automated scripts to monitor new posts on websites.

GC discussion: Federal organizations should take care to ensure that these commercial organizations are compliant with jurisdictional privacy laws regarding the collection of personal information.

Related controls and activities: None.

(02) **Monitoring for information disclosure: Review of monitored sites**

Review the list of open-source information sites being monitored [Assignment: organization-defined frequency].

Discussion: Reviewing the current list of open-source information sites being monitored on a regular basis helps to ensure that the selected sites remain relevant. The review also provides the opportunity to add new open-source information sites with the potential to provide evidence of unauthorized disclosure of organizational information. The list of sites monitored can be guided and informed by threat intelligence of other credible sources of information.

Related controls and activities: None.

(03) **Monitoring for information disclosure: Unauthorized replication of information**

Employ discovery techniques, processes, and tools to determine if external entities are replicating organizational information in an unauthorized manner.

Discussion: The unauthorized use or replication of organizational information by external entities can cause adverse impacts on organizational operations and assets, including damage to reputation. Such activity can include the replication of an organizational website by an adversary or hostile threat actor who attempts to impersonate the web-hosting organization. Discovery tools, techniques, and processes used to determine if external entities are replicating organizational information in an unauthorized manner include scanning external websites, monitoring social media, and training staff to recognize the unauthorized use of organizational information.

Related controls and activities: None.

References:

- [TBS Privacy Implementation Notice 2023-03: Guidance pertaining to the collection, use, retention, and disclosure of personal information that is publicly available online](#)

AU-14 Session audit

Control:

- Provide and implement the capability for [Assignment: organization-defined users or roles] to [Selection (1 or more): record; view; hear; log] the content of a user session under [Assignment: organization-defined circumstances]
- Develop, integrate, and use session auditing activities in consultation with legal counsel and in accordance with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines

Discussion: Session audits can include monitoring keystrokes, tracking websites visited, and recording information and/or file transfers. Session audit capability is implemented in addition to event logging and may involve implementation of specialized session capture technology. Organizations consider how session auditing can reveal information about individuals that may give rise to privacy risk as well as how to mitigate those risks. Because session auditing can impact system and network performance, organizations activate the capability under well-defined situations (e.g., the organization is suspicious of a specific individual). Organizations consult with legal counsel and privacy officials to ensure that any legal, privacy, or Charter rights, including the use of personal information, are appropriately addressed.

GC discussion: Collecting personal information associated with session audits require lawful authority, in accordance with the *Privacy Act*.

Related controls and activities: AC-03, AC-08, AU-02, AU-03, AU-04, AU-05, AU-08, AU-09, AU-11, AU-12.

Enhancements:

(01) Session audit: System start-up

Initiate session audits automatically at system start-up.

Discussion: The automatic initiation of session audits at startup helps to ensure that the information being captured on selected individuals is complete and not subject to compromise through tampering by malicious threat actors.

Related controls and activities: None.

(02) Session audit: Capture and record content

Withdrawn: Incorporated into AU-14.

(03) Session audit: Remote viewing and listening

Provide and implement the capability for authorized users to remotely view and hear content related to an established user session in real time.

Discussion: None.

Related controls and activities: AC-17.

References:

- [TBS Directive on Service and Digital, Appendix C: Mandatory Procedures for Privacy and Monitoring of Network and Device Use Information Notices](#)
- [Privacy Act](#)

AU-15 Alternate audit logging capability

Withdrawn: Moved to AU-05(05).

AU-16 Cross-organizational audit logging

Control: Employ [Assignment: organization-defined methods] for coordinating [Assignment: organization-defined audit information] among external organizations when audit information is transmitted across organizational boundaries.

Discussion: When organizations use systems or services of external organizations, the audit logging capability necessitates a coordinated, cross-organization approach. For example, maintaining the identity of individuals who request specific services across organizational boundaries may often be difficult, and doing so may prove to have significant performance and privacy ramifications. Therefore, cross-organizational audit logging often simply captures the identity of individuals who issue requests at the initial system, and subsequent systems record that the requests originated from authorized individuals. Organizations should consider including processes for coordinating audit information requirements and protection of audit information in information exchange agreements.

GC discussion: Users whose activities are monitored by audit logs should be given notice of the activity. In addition, consideration should be given to documenting the cross-organizational information sharing in an Information Sharing Agreement or Information Sharing Arrangement.

Related controls and activities: AC-08, AC-21(400), AC-21(401), AU-03, AU-06, AU-07, CA-03, PT-07.

Enhancements:

(01) **Cross-organizational audit logging: Identity preservation**

Preserve the identity of individuals in cross-organizational audit trails.

Discussion: Identity preservation is applied when there is a need to be able to trace actions that are performed across organizational boundaries to a specific individual.

Related controls and activities: IA-02, IA-04, IA-05, IA-08.

(02) **Cross-organizational audit logging: Sharing of audit information**

Provide cross-organizational audit information to [Assignment: organization-defined organizations] based on [Assignment: organization-defined cross-organizational sharing agreements].

Discussion: Due to the distributed nature of the audit information, cross-organization sharing of audit information may be essential for effective analysis of the auditing being performed. For example, the audit records of one organization may not provide sufficient information to determine the appropriate or inappropriate use of organizational information resources by individuals in other organizations. In some instances, only individuals' home organizations have the appropriate knowledge to make such determinations, thus requiring the sharing of audit information among organizations.

Related controls and activities: IR-04, SI-04.

(03) **Cross-organizational audit logging: Disassociability**

Implement [Assignment: organization-defined measures] to disassociate individuals from audit information transmitted across organizational boundaries.

Discussion: Preserving identities in audit trails could have privacy ramifications, such as enabling the tracking and profiling of individuals, but may not be operationally necessary. These risks could be further amplified when transmitting information across organizational boundaries. Implementing privacy-enhancing cryptographic techniques can disassociate individuals from audit information and reduce privacy risk while maintaining accountability.

Related controls and activities: None.

References: None.

Family: Assessment, authorization, and monitoring

The controls and activities in the Assessment, authorization, and monitoring (CA) family deal with the security and privacy assessment, authorization, and monitoring of the system.

CA-01 Assessment, authorization and monitoring policy and procedures

Activity:

- A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]
 - 1. [Selection (1 or more): Organization-level; Mission/business process-level; System-level] assessment, authorization, and monitoring policy that
 - a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
 - b. is consistent with applicable laws, Orders in Council, directives, regulations, jurisprudence, policies, standards, and guidelines
 - 2. procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls
- B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures
- C. Review and update the current assessment, authorization, and monitoring
 - 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]
 - 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]

Discussion: Assessment, authorization, and monitoring policy and procedures address the controls in the CA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy practitioners collaborate on the development of assessment, authorization, and monitoring policy and procedures.

In general, security and privacy policies and procedures at the organization level are preferable and may remove the need for mission- or system-specific policies and procedures. Policy can be included as part of the general security and privacy framework or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.

Events that may precipitate an update to assessment, authorization, and monitoring policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, Orders in Council, directives, regulations, jurisprudence, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

GC discussion: Organizations can rely on the TBS Directive on Privacy Practices, Appendix C: Standard on Privacy Impact Assessment (PIA) or develop their own organization-specific obligations for assessment. At a minimum, organizational-level assessment policies should meet the TBS requirements. In accordance with the directive, PIAs must be initiated when personal information is used for or is intended to be used as part of a decision-making process that directly affects the individual; upon substantial modifications to existing programs or activities where personal information is used or intended to be used for an administrative purpose; and when contracting out or transferring a program or activities to another level of

government or the private sector results in substantial modifications to the program or activities. Users whose activities are monitored by audit logs should be given notice of the activity.

Related controls and activities: AC-01, AC-08, PM-09, PS-08, SI-02, SI-12.

Enhancements: None.

References:

- [TBS Policy on Government Security](#)
- Organizational cyber security and privacy risk management activities (ITSP.10.036)
- [TBS Directive on Security Management](#)
- [TBS Directive on Privacy Practices, Appendix C: Standard on Privacy Impact Assessment](#)

CA-02 Control assessments

Activity:

- A. Select the appropriate assessor or assessment team for the type of assessment to be conducted
- B. Develop a control assessment plan that describes the scope of the assessment including
 1. controls and control enhancements under assessment
 2. assessment procedures to be used to determine control effectiveness
 3. assessment environment, assessment team, and assessment roles and responsibilities
- C. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment
- D. Assess the controls in the system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements
- E. Produce a control assessment report that documents the results of the assessment
- F. Provide the results of the control assessment to [Assignment: organization-defined individuals or roles]

Discussion: Organizations ensure that control assessors possess the required skills and technical expertise to develop effective assessment plans and to conduct assessments of system-specific, hybrid, and common controls, as well as program and system development activities, as appropriate. In the same regard, privacy practitioners must have the required skills and technical expertise to assess a program activity's compliance to privacy requirements. The required skills may include general knowledge of risk management concepts and approaches, as well as comprehensive knowledge of and experience with the hardware, software, and firmware system components implemented. Knowledge of privacy obligations as documented in the legislation, regulations, jurisprudence, and policy suite is required to complete PIAs.

Organizations assess controls in systems and the environments in which those systems operate as part of initial and ongoing authorizations, continuous monitoring, system design and development, systems security engineering, privacy engineering, and the system development lifecycle as recommended in Organizational cyber security and privacy risk management activities (ITSP.10.036) and System lifecycle cyber security and privacy risk management activities (ITSP.10.037). Assessments help to ensure that organizations meet information security and privacy requirements, identify weaknesses and deficiencies in the system design and development process, provide essential information needed to make risk-based decisions as part of authorization processes, and comply with vulnerability mitigation procedures.

Organizations conduct assessments on the implemented controls as documented in security and privacy plans. While assessments can be conducted throughout the system development lifecycle as part of systems engineering and systems security engineering processes, it is recommended that assessments are conducted early in the design phase to ensure privacy and security are considered in the program or system design.

The design for controls can be assessed as requests for proposals (RFPs) are developed, responses are assessed, and design reviews are conducted. If a design to implement controls and subsequent implementation in accordance with the design are assessed during development, the final control testing can be a simple confirmation utilizing previously completed control assessment and aggregating the outcomes.

Organizations may develop a single, consolidated security and privacy assessment plan for the system or maintain separate plans. A consolidated assessment plan clearly delineates the roles and responsibilities for control assessment. If multiple organizations participate in assessing a system, a coordinated approach can reduce redundancies and associated costs.

Organizations can use other types of assessment activities, such as vulnerability scanning and system monitoring, to maintain the security and privacy posture of systems during the system lifecycle. Assessment reports document assessment results in sufficient detail, as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting requirements.

Assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of authorization decisions are provided to authorizing officials, appropriate privacy senior officials or executives, senior officials in the department's security governance, and authorizing official designated representatives.

To satisfy periodic assessment requirements, organizations can use assessment results from the following sources: initial or ongoing system authorizations, continuous monitoring, systems engineering processes, or system development lifecycle activities. Organizations ensure that assessment results are current, relevant to the determination of control effectiveness, and obtained with the appropriate level of assessor independence. Existing control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed.

After the initial authorizations, organizations assess controls during continuous monitoring. Organizations also establish the frequency for ongoing assessments in accordance with organizational continuous monitoring strategies. External audits, including audits by external entities such as regulatory agencies, are outside of the scope of CA-02.

GC discussion: If the system will create, collect, or store personal information, consider the completion of a Privacy Protocol or PIA, following the CORE PIA requirements as established in the TBS Directive on Privacy Practices, Appendix C: Standard on Privacy Impact Assessment. When the PIA or Privacy Protocol is approved, a summary must be posted on the institution's external facing web presence.

TBS requirements for periodic assessments of controls are in the Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control.

Related controls and activities: AC-20, CA-05, CA-06, CA-07, PM-09, RA-05, RA-10, SA-11, SA-400, SC-38, SI-03, SI-12, SR-02, SR-03.

Enhancements:

(01) Control assessments: Independent assessors

Employ independent assessors or assessment teams to conduct control assessments.

Discussion: Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of systems. Impartiality means that assessors are free from any perceived or actual conflicts of interest regarding the development, operation, sustainment, or management of the systems under assessment or the determination of control effectiveness. To achieve impartiality, assessors do not create a mutual or conflicting interest with the organizations where the assessments are being conducted, assess their own work, act as management or employees of the organizations they are serving, or place themselves in positions of advocacy for the organizations acquiring their services.

Independent assessments can be obtained from elements within organizations or can be contracted to public or private sector entities outside of organizations. Authorizing officials determine the required level of independence based on the security categories of systems and/or the risk to organizational operations, sensitivity of the

associated personal information, organizational assets, or individuals. Authorizing officials also determine if the level of assessor independence provides sufficient assurance that the results are sound and can be used to make credible, risk-based decisions.

Assessor independence determination includes whether contracted assessment services have sufficient independence, such as when system owners are not directly involved in contracting processes or cannot influence the impartiality of the assessors conducting the assessments. During the system design and development phase, having independent assessors is similar to having independent subject matter experts (SMEs) involved in design reviews.

When organizations that own the systems are small or the structures of the organizations require that assessments be conducted by individuals that are in the developmental, operational, or management chain of the system owners, independence in assessment processes can be achieved by ensuring that assessment results are carefully reviewed and analyzed by independent teams of experts to validate the completeness, accuracy, integrity, and reliability of the results. Assessments performed for purposes other than to support authorization decisions are more likely to be usable for such decisions when performed by assessors with sufficient independence, thereby reducing the need to repeat assessments.

Related controls and activities: None.

(02) **Control assessments: Specialized assessments**

Include as part of control assessments, [Assignment: organization-defined frequency], [Selection (1): announced; unannounced], [Selection (1 or more): in-depth monitoring; security instrumentation; automated security test cases; vulnerability scanning; malicious user testing; insider threat assessment; performance and load testing; data leakage or data loss assessment; [Assignment: organization-defined other forms of assessment]].

Discussion: Organizations can conduct specialized assessments, including verification and validation, system monitoring, insider threat assessments, malicious user testing, and other forms of testing. These assessments can improve readiness by exercising organizational capabilities and indicating current levels of performance as a means of focusing actions to improve security and privacy. Organizations conduct specialized assessments in accordance with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines. Authorizing officials approve the assessment methods in coordination with the organizational risk executive function.

Organizations can include vulnerabilities uncovered during assessments into vulnerability remediation processes. Specialized assessments can also be conducted early in the system development lifecycle (e.g., during initial design, development, and unit testing).

Related controls and activities: PE-03, SI-02.

(03) **Control assessments: Leveraging results from external organizations**

Leverage the results of control assessments performed by [Assignment: organization-defined external organization(s)] on [Assignment: organization-defined system] when the assessment meets [Assignment: organization-defined requirements].

Discussion: Organizations may rely on control assessments of organizational systems by external organizations. Using such assessments and reusing existing assessment evidence can decrease the time and resources required for assessments by limiting the independent assessment activities that organizations need to perform.

The factors that organizations consider in determining whether to accept assessment results from external organizations can vary. Such factors include the organization's past experience with the organization that conducted the assessment, the reputation of the assessment organization, the level of detail of supporting assessment evidence provided, and mandates imposed by applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines.

Accredited testing laboratories that support the Common Criteria Program (ISO 15408-1), the NIST-Cyber Centre Cryptographic Module Validation Program (CMVP), or the NIST Cryptographic Algorithm Validation Program (CAVP) can provide independent assessment results that organizations can leverage.

GC discussion: The TBS Directive on Privacy Practices, Appendix C: Standard on Privacy Impact Assessment requires sharing copies of the approved PIA and other relevant documentation with partners or other government institutions as required and in a manner that respects security requirements and any other confidentiality or legal consideration.

Related controls and activities: SA-04.

References:

- [TBS Policy on Government Security](#)
- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [TBS Directive on Privacy Practices, Appendix C: Standard on Privacy Impact Assessment](#)
- [ISO 15408-1 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 1: Introduction and general model](#)
- Organizational cyber security and privacy risk management activities (ITSP.10.036)
- System lifecycle cyber security and privacy risk management activities (ITSP.10.037)

CA-03 Information exchange

Control:

- A. Approve and manage the exchange of information between the system and other systems using [Selection (1 or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; information sharing agreements; information sharing arrangements; service level agreements; user agreements; non-disclosure agreements; [Assignment: organization-defined type of agreement]]
- B. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated
- C. Review and update the agreements [Assignment: organization-defined frequency]

Discussion: System information exchange requirements apply to information exchanges between 2 or more systems. System information exchanges include connections via leased lines or VPNs; connections to Internet service providers; database sharing or exchanges of database transaction information; connections and exchanges with cloud services; exchanges via web-based services; or exchanges of files via file transfer protocols network protocols (e.g., IPv4, IPv6), email, or other organization-to-organization communications.

The information exchanged should be limited to the minimum amount of personal information that is required. Organizations consider the risk related to new or increased threats that may be introduced when systems exchange information with other systems that may have different security and privacy requirements and controls. This includes systems within the same organization and systems that are external to the organization. A joint authorization of the systems exchanging information, as described in CA-06(01) or CA-06(02), may help to communicate and reduce risk.

Authorizing officials determine the risk associated with system information exchange and the controls needed for appropriate risk mitigation. The types of agreements selected are based on factors such as the impact level of the information being exchanged, the relationship between the organizations exchanging information (e.g., government to government, government to business, business to business, government or business to service provider, government or business to individual), or the level of access to the organizational system by users of the other system.

If systems that exchange information have the same authorizing official, organizations may not need to develop agreements. Instead, the interface characteristics between the systems (e.g., how the information is being exchanged, how the information is protected, and permissible uses of the information) are described in the respective security and privacy plans.

If the systems that exchange information have different authorizing officials within the same organization, the organizations can develop agreements or provide the same information that would be provided in the appropriate agreement type from CA-03A in the respective security and privacy plans for the systems.

Organizations may incorporate agreement information into formal contracts, especially for information exchanges established between federal departments and agencies and non-federal organizations (including service providers, contractors, system developers, and system integrators). Risk considerations include systems that share the same networks.

Related controls and activities: AC-04, AC-20, AC-21(400), AC-21(401), AU-16, CA-06, IA-03, IR-04, PL-02, PT-07, RA-03, SA-09, SC-07, SI-12.

Enhancements:

(01) Information exchange: Unclassified national security system connections

Withdrawn: Moved to SC-07(25).

(02) Information exchange: Classified national security system connections

Withdrawn: Moved to SC-07(26).

(03) Information exchange: Unclassified non-national security system connections

Withdrawn: Moved to SC-07(27).

(04) Information exchange: Connections to public networks

Withdrawn: Moved to SC-07(28).

(05) Information exchange: Restrictions on external system connections

Withdrawn: Moved to SC-07(05).

(06) Information exchange: Transfer authorizations

Verify that individuals or systems transferring data between interconnecting systems have the requisite authorizations (i.e., write permissions or privileges) prior to accepting such data.

Discussion: To prevent unauthorized individuals and systems from making information transfers to protected systems, the protected system verifies—via independent means— whether the individual or system attempting to transfer information is authorized to do so. Verification of the authorization to transfer information also applies to control plane traffic (e.g., routing and DNS) and services (e.g., authenticated SMTP relays).

Related controls and activities: AC-02, AC-03, AC-04.

(07) Information exchange: Transitive information exchanges

- a. Identify transitive (downstream) information exchanges with other systems through the systems identified in CA-03A
- b. Take measures to ensure that transitive (downstream) information exchanges cease when the controls on identified transitive (downstream) systems cannot be verified or validated

Discussion: Transitive or downstream information exchanges are information exchanges between the system or systems with which the organizational system exchanges information and other systems. For mission-essential systems, services, and applications, including high-value assets, it is necessary to identify such information exchanges. The transparency of the controls or protection measures in place in such downstream systems connected directly or indirectly to organizational systems is essential to understanding the security and privacy risks

resulting from those information exchanges. Organizational systems can inherit risk from downstream systems through transitive connections and information exchanges, which can make the organizational systems more susceptible to threats, hazards, and adverse impacts.

Related controls and activities: SC-07.

References:

- [Baseline security requirements for network security zones \(ITSP.80.022\)](#)
- [Network security zoning – Design considerations for placement of services within zones \(ITSG-38\)](#)
- [TBS Guidance on Preparing Information Sharing Agreements Involving Personal Information](#)

CA-04 Security certification

Withdrawn: Incorporated into CA-02.

CA-05 Plan of action and milestones

Activity:

- Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system
- Update existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities

Discussion: Plans of action and milestones are useful for any type of organization to track planned remedial actions. For privacy, the plan of action and milestones is often documented within the PIA. Management response to the associated risk and the custodian's commitment to mitigate the privacy risk should be documented in the plan of action and milestones artifact. Security and privacy plans of action and milestones document different aspects of required compliance. While there may be some overlap, generally, the documents do not list the same risks.

GC discussion: Plans of action and milestones are required in authorization packages and subject to federal reporting requirements established by TBS.

Related controls and activities: CA-02, CA-07, PM-04, PM-09, RA-07, SI-02, SI-12.

Enhancements:

(01) Plan of action and milestones: Automation support for accuracy and currency

Ensure the accuracy, currency, and availability of the plan of action and milestones for the system using [Assignment: organization-defined automated mechanisms].

Discussion: Using automated tools helps maintain the accuracy, currency, and availability of the plan of action and milestones and facilitates the coordination and sharing of security and privacy compliance assessment throughout the organization. Such coordination and information sharing help to identify systemic weaknesses or deficiencies in organizational systems and ensure that appropriate resources are directed at the most critical system vulnerabilities in a timely manner.

Related controls and activities: None.

References:

- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- System lifecycle cyber security and privacy risk management activities (ITSP.10.037)

CA-06 Authorization

Control:

- A. Assign a senior official as the authorizing official or custodian for the system
- B. Assign a senior official as the authorizing official or custodian for common controls available for inheritance by organizational systems
- C. Ensure that the authorizing official or custodian for the system, before commencing operations
 - 1. accepts the use of common controls inherited by the system
 - 2. authorizes the system to operate
- D. Ensure that the authorizing official or custodian for common controls authorizes the use of those controls for inheritance by organizational systems
- E. Update the authorizations [Assignment: organization-defined frequency]

Discussion: Authorizations are official management decisions by senior officials to authorize operation of systems, authorize the use of common controls for inheritance by organizational systems, and explicitly accept the risk to organizational operations and assets, individuals, other organizations, and Canada based on the implementation of agreed-upon controls.

Authorizing officials provide budgetary oversight for organizational systems and common controls or assume responsibility for the mission and business functions supported by those systems or common controls. Authorizing officials or custodians are both responsible and accountable for security and privacy risks associated with the operation and use of organizational systems. Non-federal organizations may have similar processes to authorize systems and senior officials that assume the authorization role and associated responsibilities.

Authorizing officials or custodians issue ongoing authorizations of systems based on evidence produced from implemented continuous monitoring programs. Robust continuous monitoring programs reduce the need for separate reauthorization processes. Through the employment of comprehensive continuous monitoring processes, the information contained in authorization packages (i.e., security and privacy plans, assessment reports, and plans of action and milestones) is updated on an ongoing basis. This provides authorizing officials or custodians, common control providers, and system owners with an up-to-date status of the security and privacy posture of their systems, controls, and operating environments.

To reduce the cost of reauthorization, authorizing officials or custodians can leverage the results of continuous monitoring processes to the maximum extent possible as the basis for rendering reauthorization decisions.

GC discussion: The authorization process is a federal government responsibility, and therefore, authorizing officials must be senior GC employees.

Related controls and activities: CA-02, CA-03, CA-07, PM-09, PM-10, RA-03, SA-10, SI-12.

Enhancements:

(01) Authorization: Joint authorization – intra-organization

Employ a joint authorization process for the system that includes multiple authorizing officials from the same organization conducting the authorization.

Discussion: Assigning multiple authorizing officials or custodians from the same organization to serve as co-authorizing officials for the system increases the level of independence in the risk-based decision-making process. It also implements the concepts of separation of duties and dual authorization as applied to the system authorization process. The intra-organization joint authorization process is most relevant for connected systems, shared systems, and systems with multiple information owners.

Related controls and activities: AC-06.

(02) Authorization: Joint Authorization – inter-organization

Employ a joint authorization process for the system that includes multiple authorizing officials with at least 1 authorizing official from an organization external to the organization conducting the authorization.

Discussion: Assigning multiple authorizing officials, at least one of whom comes from an external organization, to serve as co-authorizing officials for the system increases the level of independence in the risk-based decision-making process. It implements the concepts of separation of duties and dual authorization as applied to the system authorization process. Employing authorizing officials from external organizations to supplement the authorizing official from the organization that owns or hosts the system may be necessary when the external organizations have a vested interest or equities in the outcome of the authorization decision. The inter-organization joint authorization process is relevant and appropriate for connected systems, shared systems or services, and systems with multiple information owners. The authorizing officials from the external organizations are key stakeholders of the system undergoing authorization.

Related controls and activities: AC-06.

References:

- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- Organizational cyber security and privacy risk management activities (ITSP.10.036)

CA-07 Continuous monitoring

Control: Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:

- establishing the following system-level metrics to be monitored: [Assignment: organization-defined system-level metrics]
- establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessment of control effectiveness
- ongoing control assessments in accordance with the continuous monitoring strategy
- ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy
- correlation and analysis of information generated by control assessments and monitoring
- response actions to address results of the analysis of control assessment and monitoring information
- reporting the security and privacy status of the system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency]

Discussion: Continuous monitoring at the system level facilitates ongoing awareness of the system security and privacy posture to support organizational risk management decisions. The terms “continuous” and “ongoing” imply that organizations assess and monitor their controls and risks at a frequency sufficient to support risk-based decisions. Different types of controls may require different monitoring frequencies.

The results of continuous monitoring generate risk response actions by organizations. When monitoring the effectiveness of multiple controls that have been grouped into capabilities, a root-cause analysis may be needed to determine the specific control that has failed.

Continuous monitoring programs allow organizations to maintain the authorizations of systems and common controls in highly dynamic environments of operation with changing mission and business needs, threats, vulnerabilities, and technologies. Having access to security and privacy information on a continuing basis through reports and dashboards gives organizational officials the ability to make effective and timely risk management decisions, including ongoing authorization

decisions. At times, monitoring may involve the collection or creation of personal information, and the appropriate safeguards should be applied.

Automation supports more frequent updates to hardware, software, and firmware inventories, authorization packages, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of systems. Monitoring requirements, including the need for specific monitoring, may be referenced in other controls and control enhancements, such as AC-2G, AC-02(07), AC-02(12)a, AC-02(07)b, AC-02(07)c, AC-17(01), AT-04A, AU-13, AU-13(01), AU-13(02), CM-03F, CM-06D, CM-11C, IR-05, MA-02B, MA-03A, MA-04A, PE-03D, PE-06, PE-14B, PE-16, PE-20, PM-06, PM-23, PM-31, PS-07E, SA-09C, SR-04, SC-05(03)b, SC-07A, SC-07(24)b, SC-18B, SC-43B, and SI-04.

Related controls and activities: AC-02, AC-06, AC-08, AC-17, AT-04, AU-06, AU-13, CA-02, CA-05, CA-06, CM-03, CM-04, CM-06, CM-11, IA-05, IR-05, MA-02, MA-03, MA-04, PE-03, PE-06, PE-14, PE-16, PE-20, PL-02, PM-04, PM-06, PM-09, PM-10, PM-12, PM-14, PM-23, PM-28, PM-31, PS-07, PT-07, RA-03, RA-05, RA-07, RA-10, SA-08, SA-09, SA-11, SC-05, SC-07, SC-18, SC-38, SC-43, SI-02, SI-03, SI-04, SI-12, SR-06.

Enhancements:

(01) Continuous monitoring: Independent assessment

Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.

Discussion: Organizations maximize the value of control assessments by requiring that assessments be conducted by assessors with appropriate levels of independence. The level of required independence is based on organizational continuous monitoring strategies. Assessor independence provides a degree of impartiality to the monitoring process. To achieve such impartiality, assessors do not create a mutual or conflicting interest with the organizations where the assessments are being conducted, assess their own work, act as management or employees of the organizations they are serving, or place themselves in advocacy positions for the organizations acquiring their services.

Related controls and activities: None.

(02) Continuous monitoring: Types of assessments

Withdrawn: Incorporated into CA-02.

(03) Continuous monitoring: Trend analyses

Employ trend analyses to determine if control implementations, the frequency of continuous monitoring activities, and the types of activities used in the continuous monitoring process need to be modified based on empirical data.

Discussion: Trend analyses include examining recent threat information that addresses the types of threat events that have occurred in the organization, success rates of certain types of attacks, emerging vulnerabilities in technologies, evolving social engineering techniques, the effectiveness of configuration settings, results from multiple control assessments, and findings from auditors.

GC discussion: Trend analyses include examining recent threat information that addresses the types of threat events that have occurred in the federal department or agency or the GC, success rates of certain types of attacks, emerging vulnerabilities in technologies, evolving social engineering techniques, the effectiveness of configuration settings, results from multiple control assessments, and findings from Inspectors General or auditors. If the trend analysis involves the use or creation of personal information, individuals should have been informed through a system use notification about this use of their personal information in advance of the analytical work. In addition, consideration should be given to listing this use of the personal information as a consistent use in the associated PIB.

Related controls and activities: None.

(04) Continuous monitoring: Risk monitoring

Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:

- a. effectiveness monitoring
- b. compliance monitoring
- c. change monitoring

Discussion: Risk monitoring is informed by the established organizational risk tolerance. Effectiveness monitoring determines the ongoing effectiveness of the implemented risk response measures. Compliance monitoring verifies that required risk response measures are implemented. It also verifies that security and privacy requirements are satisfied. Change monitoring identifies changes to organizational systems and environments of operation that may affect security and privacy risk.

Related controls and activities: None.

(05) **Continuous monitoring: Consistency analysis**

Employ the following actions to validate that policies are established and implemented controls are operating in a consistent manner: [Assignment: organization-defined actions].

Discussion: Security and privacy controls are often added incrementally to a system. As a result, policies for selecting and implementing controls may be inconsistent, and the controls could fail to work together in a consistent or coordinated manner. At a minimum, the lack of consistency and coordination could mean that there are unacceptable security and privacy compliance gaps in the system. At worst, it could mean that some of the controls implemented in one location or by one component are actually impeding the functionality of other controls (e.g., encrypting internal network traffic can impede monitoring).

In other situations, failing to consistently monitor all implemented network protocols (e.g., a dual stack of IPv4 and IPv6) may create unintended vulnerabilities in the system that could be exploited by adversaries. It is important to validate—through testing, monitoring, and analysis—that the implemented controls are operating in a consistent, coordinated, non-interfering manner.

Related controls and activities: None.

(06) **Continuous monitoring: Automation support for monitoring**

Ensure the accuracy, currency, and availability of monitoring results for the system using [Assignment: organization-defined automated mechanisms].

Discussion: Using automated tools for monitoring helps to maintain the accuracy, currency, and availability of monitoring information which in turns helps to increase the level of ongoing awareness of the system security and privacy posture in support of organizational risk management decisions. If automated support is provided by a third party, safeguards related to the vendor collection and use of any associated personal information should be in place in the contracting vehicle.

Related controls and activities: None.

References:

- [TBS Policy on Government Security](#)
- [TBS Directive on Security Management](#)
- Organizational cyber security and privacy risk management activities (ITSP.10.036)

CA-08 Penetration testing

Control: Conduct penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined systems or system components].

Discussion: Penetration testing is a specialized type of assessment conducted on systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Penetration testing goes beyond automated vulnerability scanning and is conducted by agents and teams with demonstrable skills and experience that include technical expertise in network, operating system, and/or application-level security.

Penetration testing can be used to validate vulnerabilities or determine the degree of penetration resistance of systems to adversaries within specified constraints. Such constraints include time, resources, and skills. Penetration testing attempts to duplicate the actions of adversaries and provides a more in-depth analysis of security- and privacy-related weaknesses or deficiencies. Penetration testing is especially important when organizations are transitioning from older technologies to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols).

Organizations can use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted internally or externally on the hardware, software, or firmware components of a system and can exercise both physical and technical controls.

A standard method for penetration testing includes a pretest analysis based on full knowledge of the system, pretest identification of potential vulnerabilities based on the pretest analysis, and testing designed to determine the exploitability of vulnerabilities.

All parties agree to the rules of engagement before commencing penetration testing scenarios. Organizations correlate the rules of engagement for the penetration tests with the tools, techniques, and procedures that are anticipated to be employed by adversaries. Penetration testing may result in the exposure of information that is protected by laws or regulations, to individuals conducting the testing.

Rules of engagement, contracts, or other appropriate mechanisms can be used to communicate expectations for how to protect this information. Risk assessments guide the decisions on the level of independence required for the personnel conducting penetration testing.

Related controls and activities: RA-05, RA-10, SA-11, SR-05, SR-06.

Enhancements:

(01) Penetration testing: Independent penetration testing agent or team

Employ an independent penetration testing agent or team to perform penetration testing on the system or system components.

Discussion: Independent penetration testing agents or teams are individuals or groups who conduct impartial penetration testing of organizational systems. Impartiality implies that penetration testing agents or teams are free from perceived or actual conflicts of interest with respect to the development, operation, or management of the systems that are the targets of the penetration testing. CA-02(01) provides additional information on independent assessments that can be applied to penetration testing.

Related controls and activities: CA-02.

(02) Penetration testing: Red team exercises

Employ the following red-team exercises to simulate attempts by adversaries to compromise organizational systems in accordance with applicable rules of engagement: [Assignment: organization-defined red team exercises].

Discussion: Red team exercises extend the objectives of penetration testing by examining the security and privacy posture of organizations and the capability to implement effective cyber defences. Red team exercises simulate attempts by adversaries to compromise mission and business functions and provide a comprehensive assessment of the security and privacy posture of systems and organizations. Such attempts may include technology-based attacks and social engineering-based attacks.

Technology-based attacks include interactions with hardware, software, or firmware components and/or mission and business processes. Social engineering-based attacks include interactions via email, telephone, shoulder surfing, or personal conversations.

Red team exercises are most effective when conducted by penetration testing agents and teams with knowledge of and experience with current adversarial tactics, techniques, procedures, and tools. While penetration testing may be primarily laboratory-based testing, organizations can use red team exercises to provide more comprehensive assessments that reflect real-world conditions. The results from red team exercises can be used by organizations to improve security and privacy awareness and training and to assess control effectiveness.

Related controls and activities: None.

(03) **Penetration testing: Facility penetration testing**

Employ a penetration testing process that includes [Assignment: organization-defined frequency] [Selection (1 or more): announced; unannounced] attempts to bypass or circumvent controls associated with physical access points to the facility.

Discussion: Penetration testing of physical access points can provide information on critical vulnerabilities in the operating environments of organizational systems. Such information can be used to correct weaknesses or deficiencies in physical controls that are necessary to protect organizational systems.

Related controls and activities: CA-02, PE-03.

References: None.

CA-09 Internal system connections

Control:

- A. Authorize internal connections of [Assignment: organization-defined system components or classes of components] to the system
- B. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated
- C. Terminate internal system connections after [Assignment: organization-defined conditions]
- D. Review [Assignment: organization-defined frequency] the continued need for each internal connection

Discussion: Internal system connections are the connections between organizational systems and separate constituent system components (i.e., connections between components that are part of the same system) including components used for system development. Intra-system connections include connections with mobile devices, notebook and desktop computers, tablets, printers, copiers, facsimile machines, scanners, sensors, and servers.

Instead of authorizing each internal system connection individually, organizations can authorize internal connections for a class of system components with common characteristics and/or configurations, including printers, scanners, and copiers with a specified processing, transmission, and storage capability, or smart phones and tablets with a specific baseline configuration. The continued need for an internal system connection is reviewed from the perspective of whether it provides support for organizational missions or business functions.

Related controls and activities: AC-03, AC-04, AC-18, AC-19, CM-02, IA-03, SC-07, SI-12.

Enhancements:

(01) **Internal system connections: Compliance checks**

Perform security and privacy compliance checks on constituent system components prior to the establishment of the internal connection.

Discussion: Compliance checks include verification of the relevant baseline configuration.

Related controls and activities: CM-06.

References: [NIST SP 800-124 Rev. 2 Guidelines for Managing the Security of Mobile Devices in the Enterprise](#)

Family: Configuration management

The controls and activities in the Configuration management (CM) family support the management and control of all components of the system such as hardware, software, and configuration items.

CM-01 Configuration management policy and procedures

Activity:

- A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]
 - 1. [Selection (1 or more): Organization-level; Mission/business process-level; System-level] configuration management policy that
 - a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
 - b. is consistent with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines
 - 2. procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls
- B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the configuration management policy and procedures
- C. Review and update the current configuration management
 - 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]
 - 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]

Discussion: Configuration management policy and procedures address the controls in the CM family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of configuration management policy and procedures. In general, security and privacy program policies and procedures at the organization level are preferable and may remove the need for mission- or system-specific policies and procedures.

The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission/business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.

Events that may precipitate an update to configuration management policy and procedures include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, Orders in Council, jurisprudence, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related controls and activities: PM-09, PS-08, SA-08, SI-02, SI-12.

Enhancements: None.

References:

- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)

- Organizational cyber security and privacy risk management activities (ITSP.10.036)

CM-02 Baseline configuration

Control:

- A. Develop, document, and maintain under configuration control, a current baseline configuration of the system
- B. Review and update the baseline configuration of the system
 1. [Assignment: organization-defined frequency]
 2. when required due to [Assignment: organization-defined circumstances]
 3. when system components are installed or upgraded

Discussion: Baseline configurations for systems and system components include connectivity, operational, and communications aspects of systems. Baseline configurations are documented, formally reviewed, and agreed-upon specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, or changes to systems. They include security and privacy control implementations, operational procedures, information about system components, network topology, and logical placement of components in the system architecture. Maintaining baseline configurations requires creating new baselines as organizational systems change over time. Baseline configurations of systems reflect the current enterprise architecture. If the system facilitates the collection or use of personal information, baseline configurations should include providing privacy notice to users.

Related controls and activities: AC-08, AC-19, AU-06, CA-09, CM-01, CM-03, CM-05, CM-06, CM-08, CM-09, CP-09, CP-10, CP-12, MA-02, PL-08, PM-05, SA-08, SA-10, SA-15, SC-18.

Enhancements:

(01) Baseline configuration: Reviews and updates

Withdrawn: Incorporated into CM-02.

(02) Baseline configuration: Automation support for accuracy and currency

Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using [Assignment: organization-defined automated mechanisms].

Discussion: Automated mechanisms that help organizations maintain consistent baseline configurations for systems include configuration management tools, hardware, software, firmware inventory tools, and network management tools. Automated tools can be used at the organization level, mission and business process level, or system level on workstations, servers, notebook computers, network components, or mobile devices. Tools can be used to track version numbers on operating systems, applications, types of software installed, and current patch levels. Automation support for accuracy and currency can be satisfied by the implementation of CM-08(02) for organizations that combine system component inventory and baseline configuration activities.

Related controls and activities: CM-07, IA-03, RA-05.

(03) Baseline configuration: Retention of previous configurations

Retain [Assignment: organization-defined number] of previous versions of baseline configurations of the system to support rollback.

Discussion: Retaining previous versions of baseline configurations to support rollback include hardware, software, firmware, configuration files, configuration records, and associated documentation.

Related controls and activities: None.

(04) Baseline configuration: Unauthorized software

Withdrawn: Incorporated into CM-07(04).

(05) **Baseline configuration: Authorized software**

Withdrawn: Incorporated into CM-07(05).

(06) **Baseline configuration: Development and test environments**

Maintain a baseline configuration for system development and test environments that is managed separately from the operational baseline configuration.

Discussion: Establishing separate baseline configurations for development, testing, and operational environments protects systems from unplanned or unexpected events related to development and testing activities. Separate baseline configurations allow organizations to apply the configuration management that is most appropriate for each type of configuration. For example, the management of operational configurations typically emphasizes the need for stability, while the management of development or test configurations requires greater flexibility.

Configurations in the test environment mirror configurations in the operational environment to the extent possible so that the results of the testing are representative of the proposed changes to the operational systems. Separate baseline configurations do not necessarily require separate physical environments.

Related controls and activities: CM-04, SC-03, SC-07.

(07) **Baseline configuration: Configure systems and components for high-risk areas**

- a. Issue [Assignment: organization-defined systems or system components] with [Assignment: organization-defined configurations] to individuals traveling to locations that the organization deems to be of significant risk
- b. Apply the following controls to the systems or components when the individuals return from travel: [Assignment: organization-defined controls]

Discussion: When it is known that systems or system components will be in high-risk areas external to the organization, additional controls may be implemented to counter the increased threat in such areas. For example, organizations can take actions for notebook computers used by individuals departing on and returning from travel. Actions include determining the locations that are of concern, defining the required configurations for the components, ensuring that components are configured as intended before travel is initiated, and applying controls to the components after travel is completed. Specially configured notebook computers include computers with sanitized hard drives, limited applications, and more stringent configuration settings. Controls applied to mobile devices upon return from travel include examining the mobile device for signs of physical tampering and purging and reimaging disk drives. Protecting information that resides on mobile devices is addressed in the Media protection (MP) family.

Related controls and activities: MP-04, MP-05.

References:

- [NIST SP 800-124 Rev. 2 Guidelines for Managing the Security of Mobile Devices in the Enterprise](#)
- [TBS Guidance Document: Taking Privacy into Account Before Making Contracting Decisions](#)

CM-03 Configuration change control

Control:

- A. Determine and document the types of changes to the system that are configuration-controlled
- B. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses

- C. Document configuration change decisions associated with the system
- D. Implement approved configuration-controlled changes to the system
- E. Retain records of configuration-controlled changes to the system for [Assignment: organization-defined time period]
- F. Monitor and review activities associated with configuration-controlled changes to the system
- G. Coordinate and provide oversight for configuration change control activities through [Assignment: organization-defined configuration change control element] that convenes [Selection (1 or more): [Assignment: organization-defined frequency]]; when [Assignment: organization-defined configuration change conditions]]

Discussion: Configuration change control for organizational systems involves the systematic proposal, justification, implementation, testing, review, and disposition of system changes, including system upgrades and modifications. Configuration change control includes changes to baseline configurations, configuration items of systems, operational procedures, configuration settings for system components, remediate vulnerabilities, and unscheduled or unauthorized changes. Processes for managing configuration changes to systems include configuration control boards or change advisory boards that review and approve proposed changes. For new systems or major upgrades, organizations consider including representatives from the development organizations on the configuration control boards or change advisory boards. Auditing of changes includes activities before and after changes are made to systems and the auditing activities required to implement such changes. See also SA-10.

GC discussion: For changes that impact privacy risk, the appropriate privacy senior official or executive updates PIAs and PIBs.

Related controls and activities: CA-07, CM-02, CM-04, CM-05, CM-06, CM-09, CM-11, IA-03, MA-02, PE-16, PT-06, RA-08, SA-08, SA-10, SC-28, SC-34, SC-37, SI-02, SI-03, SI-04, SI-07, SI-10, SR-11.

Enhancements:

(01) Configuration change control: Automated documentation, notification, and prohibition of changes

Use [Assignment: organization-defined automated mechanisms] to:

- a. document proposed changes to the system
- b. notify [Assignment: organization-defined approval authorities] of proposed changes to the system and request change approval
- c. highlight proposed changes to the system that have not been approved or disapproved within [Assignment: organization-defined time period]
- d. prohibit changes to the system until designated approvals are received
- e. document all changes to the system
- f. notify [Assignment: organization-defined personnel] when approved changes to the system are completed

Discussion: None.

Related controls and activities: None.

(02) Configuration change control: Testing, validation, and documentation of changes

Test, validate, and document changes to the system before finalizing the implementation of the changes.

Discussion: Changes to systems include modifications to hardware, software, or firmware components and configuration settings defined in CM-06. Organizations ensure that testing does not interfere with system operations that support organizational mission and business functions. Individuals or groups conducting tests understand security and privacy policies and procedures; system security and privacy policies and procedures; and the health, safety, and environmental risks associated with specific facilities or processes. Operational systems may need to be

taken offline or replicated to the extent feasible, before testing can be conducted. If systems must be taken offline for testing, the tests are scheduled to occur during planned system outages whenever possible. If the testing cannot be conducted on operational systems, organizations employ compensating controls.

Related controls and activities: None.

(03) **Configuration change control: Automated change implementation**

Implement changes to the current system baseline and deploy the updated baseline across the installed base using [Assignment: organization-defined automated mechanisms].

Discussion: Automated tools can improve the accuracy, consistency, and availability of configuration baseline information. Automation can also provide data aggregation and data correlation capabilities, alerting mechanisms, and dashboards to support risk-based decision-making within the organization.

Related controls and activities: None.

(04) **Configuration change control: Security and privacy representatives**

Require [Assignment: organization-defined security and privacy representatives] to be members of the [Assignment: organization-defined configuration change control element].

Discussion: Information security and privacy representatives include system security officers, senior officials in the department's security governance, custodians, or appropriate privacy senior officials or executives. Representation by personnel with information security and privacy expertise is important because changes to system configurations can have unintended side effects, some of which may be security- or privacy-relevant. Detecting such changes early in the process can help avoid unintended, negative consequences that could ultimately affect the security and privacy posture of systems. The configuration change control element referred to in the second organization-defined parameter reflects the change control elements defined by organizations in CM-03G.

Related controls and activities: None.

(05) **Configuration change control: Automated security response**

Implement the following security responses automatically if baseline configurations are changed in an unauthorized manner: [Assignment: organization-defined security responses].

Discussion: Automated security responses include halting selected system functions, halting system processing, and issuing alerts or notifications to organizational personnel when there is an unauthorized modification of a configuration item.

Related controls and activities: None.

(06) **Configuration change control: Cryptography management**

Ensure that cryptographic mechanisms used to provide the following controls are under configuration management: [Assignment: organization-defined controls].

Discussion: The controls referenced in the control enhancement refer to security and privacy controls from the control catalogue. Regardless of the cryptographic mechanisms employed, processes and procedures are in place to manage those mechanisms. For example, if system components use certificates for identification and authentication, a process is implemented to address the expiration of those certificates.

Related controls and activities: SC-12.

(07) **Configuration change control: Review system changes**

Review changes to the system [Assignment: organization-defined frequency] or when [Assignment: organization-defined circumstances] to determine whether unauthorized changes have occurred.

Discussion: Indications that warrant a review of changes to the system and the specific circumstances justifying such reviews may be obtained from activities carried out by organizations during the configuration change process or continuous monitoring process. For systems that facilitate the collection or use of personal information, system changes that are substantial to the business process or logic may trigger the requirement for a PIA.

Related controls and activities: AU-06, AU-07, CM-03.

(08) **Configuration change control: Prevent or restrict configuration changes**

Prevent or restrict changes to the configuration of the system under the following circumstances: [Assignment: organization-defined circumstances].

Discussion: System configuration changes can adversely affect critical system security and privacy functionality. Change restrictions can be enforced through automated mechanisms.

Related controls and activities: None.

References:

- [NIST SP 800-124 Rev. 2 Guidelines for Managing the Security of Mobile Devices in the Enterprise](#)
- [TBS Directive on Privacy Practices, Appendix C: Standard on Privacy Impact Assessment](#)

CM-04 Impact analyses

Control: Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.

Discussion: Organizational personnel with security or privacy responsibilities conduct impact analyses. Individuals conducting impact analyses possess the necessary skills and technical expertise to analyze the changes to systems as well as the security or privacy ramifications. Impact analyses include reviewing security and privacy plans, policies, and procedures to understand control requirements; reviewing system design documentation and operational procedures to understand control implementation and how specific system changes might affect the controls; reviewing the impact of changes on organizational supply chain partners with stakeholders; and determining how potential changes to a system create new risks to the privacy of individuals. Impact analyses also include risk assessments to understand the impact of the changes and determine if additional controls are required. Completion of a PIA assesses compliance for privacy protections using the Fair Information Principles to determine how potential changes to a system may create new risks to the privacy of individuals and the ability of implemented controls to mitigate those risks.

GC discussion: If the system facilitates automated decision-making, it may also be a requirement to complete and release the final results of an algorithmic impact assessment prior to the production of any automated decision system.

Related controls and activities: CA-07, CM-03, CM-08, CM-09, MA-02, RA-03, RA-05, RA-08, SA-05, SA-08, SA-10, SI-02.

Enhancements:

(01) **Impact analyses: Separate test environments**

Analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.

Discussion: A separate test environment must be physically or logically separate and distinct from the operational environment. The separation is sufficient to ensure that activities in the test environment do not impact activities in the operational environment and that information in the operational environment is not inadvertently transmitted to the test environment. Separate environments can be achieved by physical or logical means. If physically separate test environments are not implemented, organizations determine the strength of mechanism required when implementing logical separation.

Related controls and activities: SA-11, SC-07.

(02) **Impact analyses: Verification of controls**

After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.

Discussion: Implementation in this context refers to installing changed code in the operational system that may have an impact on security or privacy controls.

Related controls and activities: SA-11, SC-03, SI-06.

References:

- [TBS Directive on Security Management](#)
- [TBS Directive on Privacy Practices, Appendix C: Standard on Privacy Impact Assessment](#)
- [TBS Directive on Automated Decision-Making](#)

CM-05 Access restrictions for change

Control: Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.

Discussion: Changes to the hardware, software, or firmware components of systems or the operational procedures related to the system can potentially have significant effects on the security of the systems or individuals' privacy. Therefore, organizations permit only qualified and authorized individuals to access systems for purposes of initiating changes. Access restrictions include physical and logical access controls (see AC-03 and PE-03), software libraries, workflow automation, media libraries, abstract layers (i.e., changes implemented into external interfaces rather than directly into systems), and change windows (i.e., changes occur only during specified times).

Related controls and activities: AC-03, AC-05, AC-06, CM-09, PE-03, SC-28, SC-34, SC-37, SI-02, SI-10.

Enhancements:

(01) Access restrictions for change: Automated access enforcement and audit records

- a. Enforce access restrictions using [Assignment: organization-defined automated mechanisms]
- b. Automatically generate audit records of the enforcement actions

Discussion: Organizations log system accesses associated with applying configuration changes to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes.

Related controls and activities: AU-02, AU-06, AU-07, AU-12, CM-06, CM-11, SI-12.

(02) Access restrictions for change: Review system changes

Withdrawn: Incorporated into CM-03(07).

(03) Access restrictions for change: Signed components

Withdrawn: Moved to CM-14.

(04) Access restrictions for change: Dual authorization

Enforce dual authorization for implementing changes to [Assignment: organization-defined system components and system-level information].

Discussion: Organizations employ dual authorization to help ensure that any changes to selected system components and information cannot occur unless 2 qualified individuals approve and implement such changes. The 2 individuals possess the skills and expertise to determine if the proposed changes are correct implementations of approved changes. The individuals are also accountable for the changes. Dual authorization may also be known as two-person control. To reduce the risk of collusion, organizations consider rotating dual authorization duties to other individuals. System-level information includes operational procedures.

Related controls and activities: AC-02, AC-05, CM-03.

(05) **Access restrictions for change: Privilege limitation for production and operation**

- a. Limit privileges to change system components and system-related information within a production or operational environment
- b. Review and re-evaluate privileges [Assignment: organization-defined frequency]

Discussion: In many organizations, systems support multiple mission and business functions. Limiting privileges to change system components with respect to operational systems is necessary because changes to a system component may have far-reaching effects on mission and business processes supported by the system. The relationships between systems and mission/business processes are, in some cases, unknown to developers. System-related information includes operational procedures.

Related controls and activities: AC-02.

(06) **Access restrictions for change: Limit library privileges**

Limit privileges to change software resident within software libraries.

Discussion: Software libraries include privileged programs.

Related controls and activities: AC-02.

(07) **Access restrictions for change: Automatic implementation of security safeguards**

Withdrawn: Incorporated into SI-07.

References:

- [NIST FIPS 140-3 Security Requirements for Cryptographic Modules](#)
- [NIST FIPS 186-5 Digital Signature Standard \(DSS\)](#)

CM-06 Configuration Settings

Control:

- A. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations]
- B. Implement the configuration settings
- C. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements]
- D. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures

Discussion: Configuration settings are the parameters that can be changed in the hardware, software, or firmware components of the system that affect the security and privacy posture or functionality of the system. Information technology products for which configuration settings can be defined include mainframe computers, servers, workstations, operating systems, mobile devices, input/output devices, protocols, and applications. Parameters that impact the security posture of systems include registry settings; account, file, or directory permission settings; and settings for functions, protocols, ports, services, and remote connections. Privacy parameters are parameters impacting the privacy posture of systems, including the parameters required to satisfy other privacy controls. Privacy parameters include settings for access controls, personal information, data accuracy requirements, data manipulation capabilities, data processing preferences, and information handling and retention permissions. Organizations establish organization-wide configuration settings and subsequently

derive specific configuration settings for systems. The established settings become part of the configuration baseline for the system.

Common secure configurations (also known as security configuration checklists, lockdown and hardening guides, and security reference guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for information technology products and platforms as well as instructions for configuring those products or platforms to meet operational requirements. Common secure configurations can be developed by a variety of organizations, including information technology product developers, manufacturers, vendors, federal agencies, consortia, academia, industry, and other organizations in the public and private sectors.

Implementation of a common secure configuration may be mandated at the organization level, mission and business process level, system level, or at a higher level, including by a regulatory agency. Common secure configurations include the Baseline security requirements for network security zones (ITSP.80.022), Common Criteria Evaluated Configuration Guides, and the US Department of Defense (DoD) security technical implementation guides (STIGs), which affect the implementation of CM-06 and other controls such as AC-19 and CM-07. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol provide an effective method to uniquely identify, track, and control configuration settings.

Related controls and activities: AC-03, AC-19, AU-02, AU-06, CA-09, CM-02, CM-03, CM-05, CM-07, CM-11, CP-07, CP-09, CP-10, IA-03, IA-05, PL-08, PL-09, RA-05, SA-04, SA-05, SA-08, SA-09, SC-18, SC-28, SC-43, SI-02, SI-04, SI-06.

Enhancements:

(01) Configuration settings: Automated management, application, and verification

Manage, apply, and verify configuration settings for [Assignment: organization-defined system components] using [Assignment: organization-defined automated mechanisms].

Discussion: Automated tools (for example, hardening tools, baseline configuration tools) can improve the accuracy, consistency, and availability of configuration settings information. Automation can also provide data aggregation and data correlation capabilities, alerting mechanisms, and dashboards to support risk-based decision-making within the organization.

Related controls and activities: CA-07.

(02) Configuration settings: Respond to unauthorized changes

Take the following actions in response to unauthorized changes to [Assignment: organization-defined configuration settings]: [Assignment: organization-defined actions].

Discussion: Responses to unauthorized changes to configuration settings include alerting designated organizational personnel, restoring established configuration settings, or—in extreme cases—halting affected system processing.

Related controls and activities: IR-04, IR-06, SI-07.

(03) Configuration settings: Unauthorized change detection

Withdrawn: Incorporated into SI-07.

(04) Configuration settings: Conformance demonstration

Withdrawn: Incorporated into CM-04.

References:

- [Baseline security requirements for network security zones \(ITSP.80.022\)](#)
- [TBS Directive on Service and Digital, Appendix G: Standard on Enterprise Information Technology Service Common Configurations](#)

CM-07 Least functionality

Control:

- A. Configure the system to provide only [Assignment: organization-defined mission essential capabilities]
- B. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services]

Discussion: Systems provide a wide variety of functions and services. Some of the functions and services routinely provided by default may not be necessary to support essential organizational missions, functions, or operations. Additionally, it is sometimes convenient to provide multiple services from a single system component but doing so increases risk over limiting the services provided by that single component.

Where feasible, organizations limit component functionality to a single function per component. Organizations consider removing unused or unnecessary software and disabling unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of components, transfer of information, and tunnelling. Organizations employ network scanning tools, intrusion detection and prevention systems, and end-point protection technologies, such as firewalls and host-based intrusion detection systems, to identify and prevent the use of prohibited functions, protocols, ports, and services.

Least functionality can also be achieved as part of the fundamental design and development of the system (see SA-08, SC-02, and SC-03). For the concept of least functionality, consideration should be limiting the volume of personal information to that which is required by the system, reducing the impact in the event of a breach.

Related controls and activities: AC-03, AC-04, CM-02, CM-05, CM-06, CM-11, RA-05, SA-04, SA-05, SA-08, SA-09, SA-15, SC-02, SC-03, SC-07, SC-37, SI-04, SI-400.

Enhancements:

(01) Least functionality: Periodic review

- a. Review the system [Assignment: organization-defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services
- b. Disable or remove [Assignment: organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure]

Discussion: Organizations review functions, ports, protocols, and services provided by systems or system components to determine the functions and services that are candidates for elimination. Such reviews are especially important during transition periods from older technologies to newer technologies (e.g., transition from IPv4 to IPv6). These technology transitions may require implementing the older and newer technologies simultaneously during the transition period and returning to minimum essential functions, ports, protocols, and services at the earliest opportunity. Organizations can either decide the relative security of the function, port, protocol, and/or service or base the security decision on the assessment of other entities. Unsecure protocols include Bluetooth, FTP, and peer-to-peer networking.

Related controls and activities: AC-18.

(02) Least functionality: Prevent program execution

Prevent program execution in accordance with [Selection (1 or more): [Assignment: organization-defined policies, rules of behaviour, and/or access agreements regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage].

Discussion: Prevention of program execution addresses organizational policies, rules of behaviour, and/or access agreements that restrict software usage and the terms and conditions imposed by the developer or manufacturer, including software licensing and copyrights. Restrictions include prohibiting auto-execute features, restricting roles

allowed to approve program execution, permitting, or prohibiting specific software programs, or restricting the number of program instances executed at the same time.

Related controls and activities: CM-08, PL-04, PL-09, PM-05, PS-06.

(03) **Least functionality: Registration compliance**

Ensure compliance with [Assignment: organization-defined registration requirements for functions, ports, protocols, and services].

Discussion: Organizations use the registration process to manage, track, and provide oversight for systems and implemented functions, ports, protocols, and services.

Related controls and activities: None.

(04) **Least functionality: Unauthorized software – Deny-by-exception**

- a. Identify [Assignment: organization-defined software programs not authorized to execute on the system]
- b. Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the system
- c. Review and update the list of unauthorized software programs [Assignment: organization-defined frequency]

Discussion: Unauthorized software programs can be limited to specific versions or from a specific source. The concept of prohibiting the execution of unauthorized software may also be applied to user actions, system ports and protocols, IP addresses/ranges, websites, and MAC addresses.

Related controls and activities: CM-06, CM-08, CM-10, PL-09, PM-05.

(05) **Least functionality: Authorized software – Allow-by-exception**

- a. Identify [Assignment: organization-defined software programs authorized to execute on the system]
- b. Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system
- c. Review and update the list of authorized software programs [Assignment: organization-defined frequency]

Discussion: Authorized software programs can be limited to specific versions or from a specific source. To facilitate a comprehensive authorized software process and increase the strength of protection for attacks that bypass application level authorized software, software programs may be decomposed into and monitored at different levels of detail. These levels include applications, application programming interfaces (APIs), application modules, scripts, system processes, system services, kernel functions, registries, drivers, and dynamic link libraries. The concept of permitting the execution of authorized software may also be applied to user actions, system ports and protocols, IP addresses/ranges, websites, and MAC addresses. Organizations consider verifying the integrity of authorized software programs using digital signatures, cryptographic checksums, or hash functions. Verification of authorized software can occur either prior to execution or at system start-up. The identification of authorized URLs for websites is addressed in CA-03(05) and SC-07.

Related controls and activities: CM-02, CM-06, CM-08, CM-10, PL-09, PM-05, SA-10, SC-34, SI-07.

(06) **Least functionality: Confined environments with limited privileges**

Require that the following user-installed software execute in a confined physical or virtual machine environment with limited privileges: [Assignment: organization-defined user-installed software].

Discussion: Organizations identify software that may be of concern regarding its origin or potential for containing malicious code. For this type of software, user installations occur in confined environments of operation to limit or contain damage from malicious code that may be executed.

Related controls and activities: CM-11, SC-44.

(07) **Least functionality: Code execution in protected environments**

Allow execution of binary or machine-executable code only in confined physical or virtual machine environments and with the explicit approval of [Assignment: organization-defined personnel or roles] when such code is:

- a. obtained from sources with limited or no warranty
- b. without the provision of source code

Discussion: Code execution in protected environments applies to all sources of binary or machine-executable code, including commercial software and firmware and open-source software.

Related controls and activities: CM-10, SC-44.

(08) **Least functionality: Binary or machine executable code**

- a. Prohibit the use of binary or machine-executable code from sources with limited or no warranty or without the provision of source code
- b. Allow exceptions only for compelling mission or operational requirements and with the approval of the authorizing official

Discussion: Binary or machine executable code applies to all sources of binary or machine-executable code, including commercial software and firmware and open-source software. Organizations assess software products without accompanying source code or from sources with limited or no warranty for potential security impacts. The assessments address the fact that software products without the provision of source code may be difficult to review, repair, or extend. In addition, there may be no owners to make such repairs on behalf of organizations. If open-source software is used, the assessments address the fact that there is no warranty, the open-source software could contain backdoors or malware, and there may be no support available.

Related controls and activities: SA-05, SA-22.

(09) **Least functionality: Prohibiting the use of unauthorized hardware**

- a. Identify [Assignment: organization-defined hardware components authorized for system use]
- b. Prohibit the use or connection of unauthorized hardware components
- c. Review and update the list of authorized hardware components [Assignment: organization-defined frequency]

Discussion: Hardware components provide the foundation for organizational systems and the platform for the execution of authorized software programs. Managing the inventory of hardware components and controlling which hardware components are permitted to be installed or connected to organizational systems is essential to provide adequate security.

Related controls and activities: None.

References:

- [Application allow lists \(ITSAP.10.095\)](#)
- [Top 10 IT security action items: No. 10 Implement application allow lists \(ITSM.10.095\)](#)
- [Top 10 IT security actions: Number 4 harden operating systems and applications \(ITSM.10.090\)](#)
- [NIST FIPS 140-3 Security Requirements for Cryptographic Modules](#)
- [NIST FIPS 180-4 Secure Hash Standard \(SHS\)](#)

- [NIST FIPS 186-5 Digital Signature Standard \(DSS\)](#)
- [NIST FIPS 202 SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions](#)

CM-08 System component inventory

Control:

- A. Develop and document an inventory of system components that
 1. accurately reflects the system
 2. includes all components within the system
 3. does not include duplicate accounting of components or components assigned to any other system
 4. is at the level of granularity deemed necessary for tracking and reporting
 5. includes the following information to achieve system component accountability: [Assignment: organization-defined information deemed necessary to achieve effective system component accountability]
- B. Review and update the system component inventory [Assignment: organization-defined frequency]

Discussion: System components are discrete, identifiable IT assets that include hardware, software, and firmware. Organizations may choose to implement centralized system component inventories that include components from all organizational systems. In such situations, organizations ensure that the inventories include system-specific information required for component accountability. The information necessary for effective accountability of system components includes the system name, software owners, software version numbers, hardware inventory specifications, software license information, and for networked components, the machine names and network addresses across all implemented protocols (e.g., IPv4, IPv6). Inventory specifications include date of receipt, cost, model, serial number, manufacturer, supplier information, component type, and physical location.

Preventing duplicate accounting of system components addresses the lack of accountability that occurs when component ownership and system association is unknown, especially in large or complex connected systems. Effective prevention of duplicate accounting of system components necessitates the use of a unique identifier for each component. For software inventory, centrally managed software that is accessed via other systems is addressed as a component of the system on which it is installed and managed. Software installed on multiple organizational systems and managed at the system level is addressed for each individual system and may appear more than once in a centralized component inventory, necessitating a system association for each software instance in the centralized inventory to avoid duplicate accounting of components. Scanning systems implementing multiple network protocols (e.g., IPv4 and IPv6) can result in duplicate components being identified in different address spaces. The implementation of CM-08(07) can help to eliminate duplicate accounting of components.

Related controls and activities: CM-02, CM-07, CM-09, CM-10, CM-11, CM-13, CP-02, CP-09, MA-02, MA-06, PE-20, PL-09, PM-05, SA-04, SA-05, SI-02, SR-04.

Enhancements:

(01) System component inventory: Updates during installation and removal

Update the inventory of system components as part of component installations, removals, and system updates.

Discussion: Organizations can improve the accuracy, completeness, and consistency of system component inventories if the inventories are updated as part of component installations or removals or during general system updates. If inventories are not updated at these key times, there is a greater likelihood that the information will not be appropriately captured and documented. System updates include hardware, software, and firmware components.

Related controls and activities: PM-16.

(02) System component inventory: Automated maintenance

Maintain the currency, completeness, accuracy, and availability of the inventory of system components using [Assignment: organization-defined automated mechanisms].

Discussion: Organizations maintain system inventories to the extent feasible. For example, virtual machines can be difficult to monitor because such machines are not visible to the network when not in use. In such cases, organizations maintain as up-to-date, complete, and accurate an inventory as is deemed reasonable. Automated maintenance can be achieved by the implementation of CM-02(02) for organizations that combine system component inventory and baseline configuration activities.

Related controls and activities: None.

(03) **System component inventory: Automated unauthorized component detection**

- a. Detect the presence of unauthorized hardware, software, and firmware components within the system using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]
- b. Take the following actions when unauthorized components are detected: [Selection (1 or more): disable network access by such components; isolate the components; notify [Assignment: organization-defined personnel or roles]]

Discussion: Automated unauthorized component detection is applied in addition to the monitoring for unauthorized remote connections and mobile devices. Monitoring for unauthorized system components may be accomplished on an ongoing basis or by the periodic scanning of systems for that purpose. Automated mechanisms may also be used to prevent the connection of unauthorized components (see CM-07(09)). Automated mechanisms can be implemented in systems or in separate system components. When acquiring and implementing automated mechanisms, organizations consider whether such mechanisms depend on the ability of the system component to support an agent or supplicant to be detected since some types of components do not have or cannot support agents (e.g., Internet of things (IoT) devices, sensors). Isolation can be achieved, for example, by placing unauthorized system components in separate domains or subnets or quarantining such components. This type of component isolation is commonly referred to as sandboxing.

Related controls and activities: AC-19, CA-07, RA-05, SC-03, SC-39, SC-44, SI-03, SI-04, SI-07.

(04) **System component inventory: Accountability information**

Include in the system component inventory information, a means for identifying by [Selection (1 or more): name; position; role], individuals responsible and accountable for administering those components.

Discussion: Identifying individuals who are responsible and accountable for administering system components ensures that the assigned components are properly administered and that organizations can contact those individuals if some action is required (e.g., when the component is determined to be the source of a breach, needs to be recalled or replaced, or needs to be relocated).

Related controls and activities: AC-03.

(05) **System component inventory: No duplicate accounting of components**

Withdrawn: Incorporated into CM-08.

(06) **System component inventory: Assessed configurations and approved deviations**

Include assessed component configurations and any approved deviations to current deployed configurations in the system component inventory.

Discussion: Assessed configurations and approved deviations focus on configuration settings established by organizations for system components, the specific components that have been assessed to determine compliance with the required configuration settings, and any approved deviations from established configuration settings.

Related controls and activities: None.

(07) System component inventory: Centralized repository

Provide a centralized repository for the inventory of system components.

Discussion: Organizations may implement centralized system component inventories that include components from all organizational systems. Centralized repositories of component inventories provide opportunities for efficiencies in accounting for organizational hardware, software, and firmware assets. Such repositories may also help organizations rapidly identify the location and responsible individuals of components that have been compromised, breached, or are otherwise in need of mitigation actions. Organizations ensure that the resulting centralized inventories include system-specific information required for proper component accountability.

Related controls and activities: None.

(08) System component inventory: Automated location tracking

Support the tracking of system components by geographic location using [Assignment: organization-defined automated mechanisms].

Discussion: The use of automated mechanisms to track the location of system components can increase the accuracy of component inventories. Such capability may help organizations rapidly identify the location and responsible individuals of system components that have been compromised, breached, or are otherwise in need of mitigation actions. The use of tracking mechanisms should be coordinated with appropriate privacy senior officials or executives as there may be implications that affect individual privacy.

Related controls and activities: None.

(09) System component inventory: Assignment of components to systems

- a. Assign system components to a system
- b. Receive an acknowledgement from [Assignment: organization-defined personnel or roles] of this assignment

Discussion: System components that are not assigned to a system may be unmanaged, lack the required protection, and become an organizational vulnerability.

Related controls and activities: None.

References:

- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [TBS Patch Management Guidance](#)
- [TBS Policy on Privacy Protection](#)
- [Privacy Act](#)

CM-09 Configuration management plan

Control: Develop, document, and implement a configuration management plan for the system that

- A. addresses roles, responsibilities, and configuration management processes and procedures
- B. establishes a process for identifying configuration items throughout the system development lifecycle and for managing the configuration of the configuration items
- C. defines the configuration items for the system and places the configuration items under configuration management
- D. is reviewed and approved by [Assignment: organization-defined personnel or roles]
- E. protects the configuration management plan from unauthorized disclosure and modification

Discussion: Configuration management activities occur throughout the system development lifecycle. As such, there are developmental configuration management activities (e.g., the control of code and software libraries) and operational configuration management activities (e.g., control of installed components and how the components are configured). Configuration management plans satisfy the requirements in configuration management policies while being tailored to individual systems. Configuration management plans define processes and procedures for how configuration management is used to support system development lifecycle activities.

Configuration management plans are generated during the development and acquisition stage of the system development lifecycle. The plans describe how to advance changes through change management processes; update configuration settings and baselines; maintain component inventories; control development, test, and operational environments; and develop, release, and update key documents.

Organizations can employ templates to help ensure the consistent and timely development and implementation of configuration management plans. Templates can represent a configuration management plan for the organization with subsets of the plan implemented on a system-by-system basis.

Configuration management approval processes include the designation of key stakeholders responsible for reviewing and approving proposed changes to systems, and personnel who conduct security and privacy impact analyses prior to the implementation of changes to the systems. Configuration items are the system components, such as the hardware, software, firmware, and documentation to be configuration managed. As systems continue through the system development lifecycle, new configuration items may be identified, and some existing configuration items may no longer need to be under configuration control.

Related controls and activities: CM-02, CM-03, CM-04, CM-05, CM-08, PL-02, RA-08, SA-10, SI-12.

Enhancements:

(01) Configuration management plan: Assignment of responsibility

Assign responsibility for developing the configuration management process to organizational personnel that are not directly involved in system development.

Discussion: In the absence of dedicated configuration management teams assigned within organizations, system developers may be tasked with developing configuration management processes using personnel who are not directly involved in system development or system integration. This separation of duties ensures that organizations establish and maintain a sufficient degree of independence between the system development and integration processes and configuration management processes to facilitate quality control and more effective oversight.

Related controls and activities: None.

References:

- [TBS Directive on Service and Digital, Appendix G: Standard on Enterprise Information Technology Service Common Configurations](#)
- [NIST SP 800-128 Guide for Security-Focused Configuration Management of Information Systems](#)

CM-10 Software use restrictions

Control:

- Use software and associated documentation in accordance with contract agreements and copyright laws
- Track the use of software and associated documentation protected by quantity licenses to control copying and distribution
- Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work

Discussion: Software license tracking can be accomplished by manual or automated methods, depending on organizational needs. Examples of contract agreements include software license agreements and non-disclosure agreements.

Related controls and activities: AC-17, AU-06, CM-07, CM-08, PM-30, SC-07.

Enhancements:

(01) **Software usage restrictions: Open-source software**

Establish the following restrictions on the use of open-source software: [Assignment: organization-defined restrictions].

Discussion: Open-source software refers to software that is available in source code form. Certain software rights normally reserved for copyright holders are routinely provided under software license agreements that permit individuals to study, change, and improve the software. From a security perspective, the major advantage of open-source software is that it provides organizations with the ability to examine the source code. In some cases, there is an online community associated with the software that inspects, tests, updates, and reports on issues found in software on an ongoing basis. However, remediating vulnerabilities in open-source software may be problematic. There may also be licensing issues associated with open-source software, including the constraints on derivative use of such software.

GC discussion: Collections of any personal information facilitated by open-source software is governed by the same restrictions set by the *Privacy Act* for collection, use and potential disclosure.

Related controls and activities: SI-07.

References:

- [Top 10 IT security actions to protect Internet connected networks and information \(ITSM.10.089\)](#)
- [Top 10 IT security action items: No. 10 Implement application allow lists \(ITSM.10.095\)](#)
- [TBS Guideline on Service and Digital](#)
- [Privacy Act](#)
- [TBS Policy on Privacy Protection](#)

CM-11 User-installed software

Control:

- A. Establish [Assignment: organization-defined policies] governing the installation of software by users
- B. Enforce software installation policies through the following methods: [Assignment: organization-defined methods]
- C. Monitor policy compliance [Assignment: organization-defined frequency]

Discussion: If provided the necessary privileges, users can install software in organizational systems. To maintain control over the software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations include updates and security patches to existing software and downloading new applications from organization-approved app stores. Prohibited software installations include software with unknown or suspect pedigrees or software that organizations consider potentially malicious. Policies selected for governing user-installed software are organization-developed or provided by some external entity. Policy enforcement methods can include procedural methods and automated methods.

Related controls and activities: AC-03, AU-06, CM-02, CM-03, CM-05, CM-06, CM-07, CM-08, PL-04, SI-04, SI-07.

Enhancements:

(01) **User-installed software: Alerts for unauthorized installations**

Withdrawn: Incorporated into CM-08(03).

(02) **User-installed software: Software installation with privileged status**

Allow user installation of software only with explicit privileged status.

Discussion: Privileged status can be obtained, for example, by serving in the role of system administrator.

Related controls and activities: AC-05, AC-06.

(03) **User-installed software: Automated enforcement and monitoring**

Enforce and monitor compliance with software installation policies using [Assignment: organization-defined automated mechanisms].

Discussion: Organizations enforce and monitor compliance with software installation policies using automated mechanisms, which allow for quicker detection and response to unauthorized software installation which can be an indicator of an internal or external hostile attack.

Related controls and activities: None.

References:

- [TBS Directive on Service and Digital, Appendix B: Examples of Unacceptable Network and Device Use](#)
- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)

CM-12 Information location

Control:

- Identify and document the location of [Assignment: organization-defined information] and the specific system components on which the information is processed and stored
- Identify and document the users who have access to the system and system components where the information is processed and stored
- Document changes to the location (i.e., system or system components) where the information is processed and stored

Discussion: Information location addresses the need to understand where information is being processed and stored and reflects data residency requirements. Information location includes identifying where specific information types and information reside in system components and how information is being processed so that information flow can be understood and adequate protection and policy management provided for such information and system components. The location of the information and system components is also a factor in the architecture and design of the system (see SA-04, SA-08, SA-17). There may be information location implications for systems that handle personal information.

GC discussion: The security category of the information is also a factor in determining the controls necessary to protect the information and the system component where the information resides (see TBS Standard on Security Categorization).

Related controls and activities: AC-02, AC-03, AC-04, AC-06, AC-23, CM-08, PM-05, RA-02, SA-04, SA-08, SA-17, SA-400, SC-04, SC-16, SC-28, SI-04, SI-07.

Enhancements:

(01) **Information location: Automated tools to support information location**

Use automated tools to identify [Assignment: organization-defined information by information type] on [Assignment: organization-defined system components] to ensure controls are in place to protect organizational information and individual privacy.

Discussion: The use of automated tools helps to increase the effectiveness and efficiency of the information location capability implemented within the system. Automation also helps organizations manage the data produced

during information location activities and share such information across the organization. The output of automated information location tools can be used to guide and inform system architecture and design decisions.

Related controls and activities: None.

References:

- [TBS Directive on Security Management, Appendix J: Standard on Security Categorization](#)

CM-13 Data action mapping

Control: Develop and document a map of system data actions.

Discussion: Data actions are system operations, and some data actions involve personal information. The handling of such information encompasses the full information lifecycle, which includes collection, creation, transformation, use, disclosure, retention, and disposition.

A map of system data actions includes discrete data actions, identifying which elements of personal information are in use for the data actions, system components involved in the data actions, information custodians, and the owners or operators of the system components. Understanding what personal information is being handled (e.g., the sensitivity of the personal information), how personal information is being handled (e.g., if the data action is visible to the individual or is handled in another part of the system), and by whom provides a number of contextual factors that are important to assessing the degree of privacy risk associated with the system.

Data maps can be illustrated in different ways, and the level of detail may vary based on the mission and business needs of the organization. The data map may be an overlay of any system design artifact that the organization is using. The development of this map may necessitate coordination between the privacy and security programs regarding the covered data actions and the components that are identified as part of the system. Users whose activities are mapped should be given notice of the activity.

Related controls and activities: AC-03, AC-08, CM-04, CM-12, PM-05, PM-27, PT-02, PT-03, RA-03, RA-08.

Enhancements: None.

References:

- [Privacy Act](#)
- [TBS Policy on Privacy Protection](#)

CM-14 Signed components

Control: Prevent the installation of [Assignment: organization-defined software and firmware components] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

Discussion: Software and firmware components prevented from installation unless signed with recognized and approved certificates include software and firmware version updates, patches, service packs, device drivers, and basic input/output system updates. Organizations can identify applicable software and firmware components by type, by specific items, or a combination of both. Digital signatures and organizational verification of such signatures is a method of code authentication.

Related controls and activities: CM-07, SC-12, SC-13, SI-07.

Enhancements: None.

References: None.

Family: Contingency planning

The controls and activities in the Contingency planning (CP) family support the establishment, maintenance, and implementation of plans for emergency response, backup operations, and post-disaster recovery for organizational systems to ensure the availability of critical resources and continuity of operations in emergency situations.

CP-01 Contingency planning policy and procedures

Activity:

- A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]
 - 1. [Selection (1 or more): Organization-level; Mission/business process-level; System-level] contingency planning policy that
 - a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
 - b. is consistent with applicable laws, Orders in Council, directives, regulations, jurisprudence, policies, standards, and guidelines
 - 2. procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls
- B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the contingency planning policy and procedures
- C. Review and update the current contingency planning
 - 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]
 - 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]

Discussion: Contingency planning policy and procedures address the controls in the contingency planning family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of contingency planning policy and procedures.

In general, security and privacy program policies and procedures at the organization level are preferable and may remove the need for mission- or system-specific policies and procedures. The policy can be included as part of a general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations.

Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.

Events that may precipitate an update to contingency planning policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, Orders in Council, directives, regulations, jurisprudence, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related controls and activities: PM-09, PS-08, SI-02, SI-12.

Enhancements: None.

References:

- [TBS Directive on Security Management, Appendix D: Mandatory Procedures for Business Continuity Management Control](#)
- Directive for the Control of COMSEC Material in the Government of Canada (ITSD-03A) (upon request to the Cyber Centre)
- [TBS Policy on Privacy Protection](#)
- [TBS Directive on Privacy Practices](#)
- [TBS Directive on Privacy Practices, Appendix C: Standard on Privacy Impact Assessment](#)
- [TBS Directive on Personal Information Requests and Correction of Personal Information](#)
- [TBS Directive on Social Insurance Number](#)

CP-02 Contingency plan

Control:

- A. Develop a contingency plan for the system that
 1. identifies essential mission and business functions and associated contingency requirements
 2. provides recovery objectives, restoration priorities, and metrics
 3. addresses contingency roles, responsibilities, and assigned individuals with contact information
 4. addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure
 5. addresses eventual, full system restoration without deterioration of the controls originally planned and implemented
 6. addresses the integrity of the data held within the system, including personal information
 7. addresses the impact, injury, or consequence of a system compromise, including with respect to personal information
 8. addresses the sharing of contingency information
 9. is reviewed and approved by [Assignment: organization-defined personnel or roles]
- B. Distribute copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]
- C. Ensure individuals with responsibilities review the contingency plan and understand their roles
- D. Coordinate contingency planning activities with incident handling activities
- E. Review the contingency plan for the system [Assignment: organization-defined frequency]
- F. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing
- G. Communicate contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]
- H. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training
- AA. Protect the contingency plan from unauthorized disclosure and modification

Discussion: Contingency planning for systems is part of an overall program for achieving continuity of operations for organizational mission and business functions. Contingency planning addresses system restoration and implementation of alternative mission or business processes when systems are compromised or breached. Contingency planning is considered throughout the system development lifecycle and is a fundamental part of the system design.

Systems can be designed for redundancy, to provide backup capabilities, and for resilience. Contingency plans reflect the degree of restoration required for organizational systems since not all systems need to fully recover to achieve the level of

continuity of operations desired. System recovery objectives reflect applicable laws, Orders in Council, directives, regulations, jurisprudence, policies, standards, guidelines, organizational risk tolerance, and system impact level.

Actions addressed in contingency plans include orderly system degradation, system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By coordinating contingency planning with incident handling activities, organizations ensure that the necessary planning activities are in place and activated in the event of an incident. Organizations should consider whether continuity of operations during an incident conflicts with the capability to automatically disable the system, as specified in IR-04(05). Incident response planning is part of contingency planning for organizations and is addressed in the IR (incident response) family.

Related controls and activities: CP-03, CP-04, CP-06, CP-07, CP-08, CP-09, CP-10, CP-11, CP-13, IR-04, IR-06, IR-08, IR-09, MA-06, MP-02, MP-04, MP-05, PL-02, PM-08, PM-11, SA-15, SA-20, SC-07, SC-23, SI-12.

Enhancements:

(01) Contingency plan: Coordinate with related plans

Coordinate contingency plan development with organizational elements responsible for related plans.

Discussion: Plans that are related to contingency plans include business continuity, disaster recovery, critical infrastructure, continuity of operations, crisis communications, insider threat implementation, data breach response, privacy breach protocols, cyber incident response, breach response, and occupant emergency.

Related controls and activities: None.

(02) Contingency plan: Capacity planning

Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

Discussion: Capacity planning is needed because different threats can result in a reduction of the available processing, telecommunications, and support services intended to support essential mission and business functions. Organizations anticipate degraded operations during contingency operations and factor the degradation into capacity planning. For capacity planning, environmental support refers to any environmental factor for which the organization determines that it needs to provide support in a contingency situation, even if in a degraded state. Such determinations are based on an organizational assessment of risk, system categorization (impact level), and organizational risk tolerance.

Related controls and activities: PE-11, PE-12, PE-13, PE-14, PE-18, SC-05.

(03) Contingency plan: Resume mission and business functions

Plan for the resumption of [Selection (1): all; essential] mission and business functions within [Assignment: organization-defined time period] of contingency plan activation.

Discussion: Organizations may choose to conduct contingency planning activities to resume mission and business functions as part of business continuity planning or as part of business impact analyses. Organizations prioritize the resumption of mission and business functions. The time period for resuming mission and business functions may be dependent on the severity and extent of the disruptions to the system and its supporting infrastructure. Care should be taken to assess potential modifications to any personal information held within a compromised system.

Related controls and activities: None.

(04) Contingency plan: Resume all mission and business functions

Withdrawn: Incorporated into CP-02(03).

(05) Contingency plan: Continue mission and business functions

Plan for the continuance of [Selection (1): all; essential] mission and business functions with minimal or no loss of operational continuity and sustain that continuity until full system restoration at primary processing and/or storage sites.

Discussion: Organizations may choose to conduct contingency planning activities to continue mission and business functions as part of business continuity planning or business impact analyses. Primary processing and/or storage sites defined by organizations as part of contingency planning may change depending on the circumstances associated with the contingency.

Related controls and activities: None.

(06) **Contingency plan: Alternate processing and storage sites**

Plan for the transfer of [Selection (1): all; essential] mission and business functions to alternate processing and/or storage sites with minimal or no loss of operational continuity and sustain that continuity through system restoration to primary processing and/or storage sites.

Discussion: Organizations may choose to conduct contingency planning activities for alternate processing and storage sites as part of business continuity planning or business impact analyses. Primary processing and/or storage sites defined by organizations as part of contingency planning may change depending on the circumstances associated with the contingency.

Related controls and activities: None.

(07) **Contingency plan: Coordinate with external service providers**

Coordinate the contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.

Discussion: When the capability of an organization to carry out its mission and business functions is dependent on external service providers, developing a comprehensive and timely contingency plan may become more challenging. When mission and business functions are dependent on external service providers, organizations coordinate contingency planning activities with the external entities to ensure that the individual plans reflect the overall contingency needs of the organization. Ensure contract vehicles include clauses that require the external service provider(s) to notify and collaborate with the organization in the event that a system holding personal information is compromised.

Related controls and activities: SA-09.

(08) **Contingency plan: Identify critical assets**

Identify critical system assets supporting [Selection (1): all; essential] mission and business functions.

Discussion: Organizations may choose to identify critical assets as part of criticality analysis, business continuity planning, or business impact analyses. Organizations identify critical system assets so that additional controls can be employed (beyond the controls routinely implemented) to help ensure that organizational mission and business functions can continue to be conducted during contingency operations. The identification of critical information assets also facilitates the prioritization of organizational resources. Critical system assets include technical and operational aspects. Technical aspects include system components, IT services, IT products, and mechanisms. Operational aspects include procedures (i.e., manually executed operations) and personnel (i.e., individuals operating technical controls and/or executing manual procedures). Organizational program protection plans can assist in identifying critical assets. If critical assets are resident within or supported by external service providers, organizations should consider implementing CP-02(07) as a control enhancement.

Related controls and activities: CM-08, RA-09.

References:

- [TBS Directive on Security Management, Appendix D: Mandatory Procedures for Business Continuity Management Control](#)
- [TBS Directive on Security Management, Appendix G: Mandatory Procedures for Security Event Management Control](#)
- [Developing your IT recovery plan \(ITSAP.40.004\)](#)
- Directive for the Control of COMSEC Material in the Government of Canada (ITSD-03A) (upon request to the Cyber Centre)
- [TBS Guidance Document: Taking Privacy into Account Before Making Contracting Decisions](#)

CP-03 Contingency training

Control:

- A. Provide contingency training to system users consistent with assigned roles and responsibilities
 1. within [Assignment: organization-defined time period] of assuming a contingency role or responsibility
 2. when required by system changes
 3. [Assignment: organization-defined frequency] thereafter
- B. Review and update contingency training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]

Discussion: Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, some individuals may only need to know when and where to report for duty during contingency operations and if normal duties are affected; system administrators may require additional training on how to establish systems at alternate processing and storage sites; and organizational officials may receive more specific training on how to conduct mission-essential functions in designated off-site locations and how to establish communications with other governmental entities for purposes of coordination on contingency-related activities.

Training for contingency roles or responsibilities reflects the specific continuity requirements in the contingency plan. Events that may precipitate an update to contingency training content include, but are not limited to, contingency plan testing or an actual contingency (lessons learned), assessment or audit findings, security incidents or breaches, or changes in laws, Orders in Council, directives, regulations, jurisprudence, policies, standards, and guidelines. At the discretion of the organization, participation in a contingency plan test or exercise, including lessons learned sessions subsequent to the test or exercise, may satisfy contingency plan training requirements.

Related controls and activities: AT-02, AT-03, AT-04, CP-02, CP-04, CP-08, IR-02, IR-04, IR-09.

Enhancements:

(01) Contingency training: Simulated events

Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.

Discussion: The use of simulated events creates an environment for personnel to experience actual threat events, including cyber attacks that disable websites, ransomware attacks that encrypt organizational data on servers, hurricanes that damage or destroy organizational facilities, or hardware or software failures.

Related controls and activities: None.

(02) Contingency training: Mechanisms used in training environments

Employ mechanisms used in operations to provide a more thorough and realistic contingency training environment.

Discussion: Operational mechanisms refer to processes that have been established to accomplish an organizational goal or a system that supports a particular organizational mission or business objective. Actual mission and

business processes, systems, and/or facilities may be used to generate simulated events and enhance the realism of simulated events during contingency training.

Related controls and activities: None.

References: [TBS Directive on Security Management, Appendix H: Mandatory Procedures for Security Awareness and Training Control](#)

CP-04 Contingency plan testing

Control:

- A. Test the contingency plan for the system [Assignment: organization-defined frequency] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [Assignment: organization-defined tests]
- B. Review the contingency plan test results
- C. Initiate corrective actions, if needed

Discussion: Methods for testing contingency plans to determine the effectiveness of the plans and identify potential weaknesses include checklists, walk-through and tabletop exercises, simulations (parallel or full interrupt), and comprehensive exercises. Organizations conduct testing based on the requirements in contingency plans and include a determination of the effects on organizational operations, assets, and individuals due to contingency operations. Organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions.

Related controls and activities: AT-03, CP-02, CP-03, CP-08, CP-09, IR-03, IR-04, PL-02, PM-14, SR-02.

Enhancements:

(01) Contingency plan testing: Coordinate with related plans

Coordinate contingency plan testing with organizational elements responsible for related plans.

Discussion: Plans related to contingency planning for organizational systems include business continuity, disaster recovery, continuity of operations, crisis communications, critical infrastructure, cyber incident response, and occupant emergency. Coordination of contingency plan testing does not require organizations to create organizational elements to handle related plans or to align such elements with specific plans. However, it does require that if such organizational elements are responsible for related plans, organizations coordinate with those elements.

Related controls and activities: IR-08, PM-08.

(02) Contingency plan testing: Alternate processing site

Test the contingency plan at the alternate processing site to:

- a. familiarize contingency personnel with the facility and available resources
- b. evaluate the capabilities of the alternate processing site to support contingency operations

Discussion: Conditions at the alternate processing site may be significantly different than the conditions at the primary site. Having the opportunity to visit the alternate site and experience the actual capabilities available at the site can provide valuable information on potential vulnerabilities that could affect essential organizational mission and business functions. The onsite visit can also provide an opportunity to refine the contingency plan to address the vulnerabilities discovered during testing.

Related controls and activities: CP-07.

(03) Contingency plan testing: Automated testing

Test the contingency plan using [Assignment: organization-defined automated mechanisms].

Discussion: Automated mechanisms facilitate thorough and effective testing of contingency plans by providing more complete coverage of contingency issues, selecting more realistic test scenarios and environments, and effectively stressing the system and supported mission and business functions.

Related controls and activities: None.

(04) **Contingency plan testing: Full recovery and reconstitution**

Include a full recovery and reconstitution of the system to a known state as part of contingency plan testing.

Discussion: Recovery is executing contingency plan activities to restore organizational mission and business functions. Reconstitution takes place following recovery and includes activities for returning systems to fully operational states. Organizations establish a known state for systems that includes system state information for hardware, software programs, and data. Preserving system state information facilitates system restart and return to the operational mode of organizations with less disruption of mission and business processes.

Related controls and activities: CP-10, SC-24.

(05) **Contingency plan testing: Self-challenge**

Employ [Assignment: organization-defined mechanisms] to [Assignment: organization-defined system or system component] to disrupt and adversely affect the system or system component.

Discussion: Often, the best method of assessing system resilience is to disrupt the system in some manner. The mechanisms used by the organization could disrupt system functions or system services in many ways, including terminating or disabling critical system components, changing the configuration of system components, degrading critical functionality (e.g., restricting network bandwidth), or altering privileges. Automated, ongoing, and simulated cyber attacks and service disruptions can reveal unexpected functional dependencies and help the organization determine its ability to ensure resilience in the face of an actual cyber attack.

Related controls and activities: None.

References:

- [TBS Directive on Security Management, Appendix D: Mandatory Procedures for Business Continuity Management Control](#)
- [TBS Directive on Security Management, Appendix H: Mandatory Procedures for Security Awareness and Training Control](#)

CP-05 Contingency plan update

Withdrawn: Incorporated into CP-02.

CP-06 Alternate storage site

Control:

- Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information
- Ensure that the alternate storage site provides controls equivalent to that of the primary site

Discussion: Alternate storage sites are geographically distinct from primary storage sites and maintain duplicate copies of information and data if the primary storage site is not available. Similarly, alternate processing sites provide processing capability if the primary processing site is not available. Geographically distributed architectures that support contingency requirements may be considered alternate storage sites.

Items covered by alternate storage site agreements include environmental conditions at the alternate sites, access rules for systems and facilities, physical and environmental protection requirements, and coordination of delivery and retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential mission and business functions despite compromise, failure, or disruption in organizational systems.

Related controls and activities: CP-02, CP-07, CP-08, CP-09, CP-10, MP-04, MP-05, PE-03, SC-36, SI-13, SA-400.

Enhancements:

(01) Alternate storage site: Separation from primary site

Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.

Discussion: Threats that affect alternate storage sites are defined in organizational risk assessments and include natural disasters, structural failures, hostile attacks, and errors of omission or commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate storage sites based on the types of threats that are of concern. For threats such as hostile attacks, the degree of separation between sites is less relevant.

Related controls and activities: RA-03.

(02) Alternate storage site: Recovery time and recovery point objectives

Configure the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

Discussion: Organizations establish recovery time and recovery point objectives as part of contingency planning. Configuration of the alternate storage site includes physical facilities and the systems supporting recovery operations that ensure accessibility and correct execution.

Related controls and activities: None.

(03) Alternate storage site: Accessibility

Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

Discussion: Area-wide disruptions refer to those types of disruptions that are broad in geographic scope with such determinations made by organizations based on organizational assessments of risk. Explicit mitigation actions include duplicating backup information at other alternate storage sites if access problems occur at originally designated alternate sites or planning for physical access to retrieve backup information if electronic accessibility to the alternate site is disrupted.

Related controls and activities: RA-03.

References: [TBS Directive on Service and Digital, Appendix J: Standard on Systems that Manage Information and Data](#)

CP-07 Alternate processing site

Control:

- A. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] when the primary processing capabilities are unavailable

- B. Make available at the alternate processing site the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption
- C. Provide controls at the alternate processing site that are equivalent to those at the primary site

Discussion: Alternate processing sites are geographically distinct from primary processing sites and provide processing capability if the primary processing site is not available. The alternate processing capability may be addressed using a physical processing site or other alternatives, such as failover to a cloud-based service provider or other internally or externally provided processing service. Geographically distributed architectures that support contingency requirements may also be considered alternate processing sites. Controls that are covered by alternate processing site agreements include the environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and the coordination for the transfer and assignment of personnel. Requirements are allocated to alternate processing sites that reflect the requirements in contingency plans to maintain essential mission and business functions despite disruption, compromise, or failure in organizational systems.

Related controls and activities: CP-02, CP-06, CP-08, CP-09, CP-10, MA-06, PE-03, PE-11, PE-12, PE-17, SC-36, SI-13, SA-400.

Enhancements:

(01) Alternate processing site: Separation from primary site

Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.

Discussion: Threats that affect alternate processing sites are defined in organizational assessments of risk and include natural disasters, structural failures, hostile attacks, and errors of omission or commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate processing sites based on the types of threats that are of concern. For threats such as hostile attacks, the degree of separation between sites is less relevant.

Related controls and activities: RA-03.

(02) Alternate processing site: Accessibility

Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Discussion: Area-wide disruptions refer to those types of disruptions that are broad in geographic scope with such determinations made by organizations based on organizational assessments of risk.

Related controls and activities: RA-03.

(03) Alternate processing site: Priority of service

Develop alternate processing site agreements that contain priority of service provisions in accordance with availability requirements (including recovery time objectives).

Discussion: Priority of service agreements refer to negotiated agreements with service providers that ensure that organizations receive priority treatment consistent with their availability requirements and the availability of information resources for logical alternate processing and/or at the physical alternate processing site. Organizations establish recovery time objectives as part of contingency planning.

Related controls and activities: None.

(04) Alternate processing site: Preparation for use

Prepare the alternate processing site so that the site can serve as the operational site supporting essential mission and business functions.

Discussion: Site preparation includes establishing configuration settings for systems at the alternate processing site consistent with the requirements for such settings at the primary site and ensuring that essential supplies and logistical considerations are in place.

Related controls and activities: CM-02, CM-06, CP-04.

(05) **Alternate processing site: Equivalent information security safeguards**

Withdrawn: Incorporated into CP-07.

(06) **Alternate processing site: Inability to return to primary site**

Plan and prepare for circumstances that preclude returning to the primary processing site.

Discussion: There may be situations that preclude an organization from returning to the primary processing site, such as if a natural disaster (e.g., flood or a hurricane) damaged or destroyed a facility and it was determined that rebuilding in the same location was not prudent.

Related controls and activities: None.

References: [TBS Directive on Service and Digital, Appendix J: Standard on Systems that Manage Information and Data](#)

CP-08 Telecommunications services

Control: Establish alternate telecommunications services, including necessary agreements to permit the resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Discussion: Telecommunications services (for data and voice) for primary and alternate processing and storage sites are in scope for CP-08. Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential mission and business functions despite the loss of primary telecommunications services. Organizations may specify different time periods for primary or alternate sites. Alternate telecommunications services include additional organizational or commercial ground-based circuits or lines, network-based approaches to telecommunications, or the use of satellites. Organizations consider factors such as availability, quality of service, and access when entering into alternate telecommunications agreements.

Related controls and activities: CP-02, CP-06, CP-07, CP-11, SC-07, SA-400.

Enhancements:

(01) **Telecommunications services: Priority of service provisions**

- a. Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives)
- b. Request priority access for dialing via Innovation, Science and Economic Development Canada (ISED) for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier (see ISED's Priority Access for Dialling telecommunications services in times of crisis)

Discussion: Organizations should consider the potential mission or business impact in situations where telecommunications service providers are servicing other organizations with similar priority of service provisions.

GC discussion: No longer available in Canada.

Related controls and activities: None.

(02) **Telecommunications services: Single points of failure**

Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

Discussion: In certain circumstances, telecommunications service providers or services may share the same physical lines, which increases the vulnerability of a single failure point. It is important to have provider transparency for the actual physical transmission capability for telecommunication services.

Related controls and activities: None.

(03) **Telecommunications services: Separation of primary and alternate providers**

Obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.

Discussion: Threats that affect telecommunications services are defined in organizational assessments of risk and include natural disasters, structural failures, cyber or physical attacks, and errors of omission or commission. Organizations can reduce common susceptibilities by minimizing shared infrastructure among telecommunications service providers and achieving sufficient geographic separation between services. Organizations may consider using a single service provider in situations where the service provider can provide alternate telecommunications services that meet the separation needs addressed in the risk assessment.

Related controls and activities: None.

(04) **Telecommunications services: Provider contingency plan**

- a. Require primary and alternate telecommunications service providers to have contingency plans
- b. Review provider contingency plans to ensure that the plans meet organizational contingency requirements
- c. Obtain evidence of contingency testing and training by providers [Assignment: organization-defined frequency]

Discussion: Reviews of provider contingency plans should consider the proprietary nature of such plans. In some situations, a summary of provider contingency plans may be sufficient evidence for organizations to satisfy the review requirement.

GC discussion: Telecommunications service providers may also participate in ongoing disaster recovery exercises in coordination with Public Safety Canada and provincial, municipal, and territorial governments. Organizations may use these types of activities to satisfy evidentiary requirements related to service provider contingency plan reviews, testing, and training.

Related controls and activities: CP-03, CP-04.

(05) **Telecommunications services: Alternate telecommunications service testing**

Test alternate telecommunications services [Assignment: organization-defined frequency].

Discussion: Alternate telecommunications services testing is arranged through contractual agreements with service providers. The testing may occur in parallel with normal operations to ensure that there is no degradation in organizational missions or functions.

Related controls and activities: CP-03.

References:

- [Industry Canada, Priority Access for Dialing: telecommunications services in times of crisis](#)

CP-09 System backup

Control:

- A. Conduct backups of user-level information contained in [Assignment: organization-defined system components] [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]
- B. Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]
- C. Conduct backups of system documentation, including security- and privacy-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]
- D. Protect the confidentiality, integrity, and availability of backup information
- AA. The organization determines retention periods for essential business information and archived backup

Discussion: System-level information includes system state information, operating system software, middleware, application software, and licenses. User-level information includes information other than system-level information. Mechanisms employed to protect the integrity of system backups include digital signatures and cryptographic hashes. Protection of system backup information while in transit is addressed by MP-05 and SC-08.

System backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information. Organizations may be subject to laws, Orders in Council, directives, regulations, or policies with requirements regarding specific categories of information (e.g., personal health information). Organizational personnel consult with the appropriate privacy senior official or executive and legal counsel regarding such requirements.

Related controls and activities: CP-02, CP-06, CP-10, MP-04, MP-05, SA-400, SC-08, SC-12, SC-13, SI-04, SI-13.

Enhancements:

(01) System backup: Testing for reliability and integrity

Test backup information [Assignment: organization-defined frequency] to verify media reliability and information integrity.

Discussion: Organizations need assurance that backup information can be reliably retrieved. Reliability pertains to the systems and system components where the backup information is stored, the operations used to retrieve the information, and the integrity of the information being retrieved. Independent and specialized tests can be used for each of the aspects of reliability. For example, decrypting and transporting (or transmitting) a random sample of backup files from the alternate storage or backup site and comparing the information to the same information at the primary processing site can provide such assurance.

Related controls and activities: CP-04.

(02) System backup: Test restoration using sampling

Use a sample of backup information in the restoration of selected system functions as part of contingency plan testing.

Discussion: Organizations need assurance that system functions can be restored correctly and can support established organizational missions. To ensure that the selected system functions are thoroughly exercised during contingency plan testing, a sample of backup information is retrieved to determine whether the functions are operating as intended. Organizations can determine the sample size for the functions and backup information based on the level of assurance needed.

Related controls and activities: CP-04.

(03) System backup: Separate storage for critical information

Store backup copies of [Assignment: organization-defined critical system software and other security-related information] in a separate facility or in a fire rated container that is not collocated with the operational system.

Discussion: Separate storage for critical information applies to all critical information regardless of the type of backup storage media. Critical system software includes operating systems, middleware, cryptographic key management systems, and intrusion detection systems. Security-related information includes inventories of system hardware, software, and firmware components.

Alternate storage sites, including geographically distributed architectures, serve as separate storage facilities for organizations. Organizations may provide separate storage by implementing automated backup processes at alternative storage sites (e.g., data centres). The Royal Canadian Mounted Police (RCMP) establish standards and specifications for security and fire-rated containers.

Related controls and activities: CM-02, CM-06, CM-08.

(04) **System backup: Protection from unauthorized modification**

Withdrawn: Incorporated into CP-09.

(05) **System backup: Transfer to alternate storage site**

Transfer system backup information to the alternate storage site [Assignment: organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives].

Discussion: System backup information can be transferred to alternate storage sites either electronically or by the physical shipment of storage media, ensuring adherence to security protocols for handling and transmission.

Related controls and activities: CP-07, MP-03, MP-04, MP-05.

(06) **System backup: Redundant secondary system**

Conduct system backup by maintaining a redundant secondary system that is not collocated with the primary system and that can be activated without loss of information or disruption to operations.

Discussion: The effect of system backup can be achieved by maintaining a redundant secondary system that mirrors the primary system, including the replication of information. If this type of redundancy is in place and there is sufficient geographic separation between the 2 systems, the secondary system can also serve as the alternate processing site.

Related controls and activities: CP-07.

(07) **System backup: Dual authorization for deletion or destruction**

Enforce dual authorization for the deletion or destruction of [Assignment: organization-defined backup information].

Discussion: Dual authorization ensures that deletion or destruction of backup information cannot occur unless 2 qualified individuals carry out the task. Individuals deleting or destroying backup information possess the skills or expertise to determine if the proposed deletion or destruction of information reflects organizational policies and procedures. Dual authorization may also be known as two-person control. To reduce the risk of collusion, organizations consider rotating dual authorization duties to other individuals.

Related controls and activities: AC-03, AC-05, MP-02.

(08) **System backup: Cryptographic protection**

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of [Assignment: organization-defined backup information].

Discussion: The selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of backup information. The strength of mechanisms selected is commensurate with the security category or classification of the information. Cryptographic protection applies to system backup information in storage at

both primary and alternate locations. Organizations that implement cryptographic mechanisms to protect information at rest also consider cryptographic key management solutions.

Related controls and activities: SC-12, SC-13, SC-28.

References:

- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [TBS Directive on Security Management, Appendix C: Mandatory Procedures for Physical Security Control](#)
- [Tips for backing up your information \(ITSAP.40.002\)](#)
- [RCMP G1-001 Security Equipment Guide](#) (restricted to GC)

CP-10 System recovery and reconstitution

Control: Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] after a disruption, compromise, or failure.

Discussion: Recovery is executing contingency plan activities to restore organizational mission and business functions. Reconstitution takes place following recovery and includes activities for returning systems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities, recovery point, recovery time, and reconstitution objectives, and organizational metrics consistent with contingency plan requirements. Reconstitution includes the deactivation of interim system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored system capabilities, re-establishment of continuous monitoring activities, system reauthorization (if required), and activities to prepare the system and organization for future disruptions, breaches, compromises, or failures. Recovery and reconstitution capabilities can include automated mechanisms and manual procedures. Organizations establish recovery time and recovery point objectives as part of contingency planning.

Related controls and activities: CP-02, CP-04, CP-06, CP-07, CP-09, IR-04, SA-08, SC-24, SI-13.

Enhancements:

(01) System recovery and reconstitution: Contingency plan testing

Withdrawn: Incorporated into CP-04.

(02) System recovery and reconstitution: Transaction recovery

Implement transaction recovery for systems that are transaction-based.

Discussion: Transaction-based systems include database management systems and transaction processing systems. Mechanisms supporting transaction recovery include transaction rollback and transaction journalling.

Related controls and activities: None.

(03) System recovery and reconstitution: Compensating security controls

Withdrawn: Addressed through tailoring.

(04) System recovery and reconstitution: Restore within time period

Provide the capability to restore system components within [Assignment: organization-defined restoration time periods] from configuration-controlled and integrity-protected information representing a known, operational state for the components.

Discussion: Restoration of system components includes reimaging, which restores the components to known, operational states.

Related controls and activities: CM-02, CM-06.

(05) System recovery and reconstitution: Failover capability

Withdrawn: Incorporated into SI-13.

(06) **System recovery and reconstitution: Component protection**

Protect system components used for recovery and reconstitution.

Discussion: Protection of system recovery and reconstitution components (i.e., hardware, firmware, and software) includes physical and technical controls. Backup and restoration components used for recovery and reconstitution include router tables, compilers, and other system software.

Related controls and activities: AC-03, AC-06, MP-02, MP-04, PE-03, PE-06.

References:

- [TBS Directive on Service and Digital](#)
- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [TBS Government of Canada Cyber Security Event Management Plan \(GC CSEMP\)](#)

CP-11 Alternate communications protocols

Control: Provide the capability to employ [Assignment: organization-defined alternative communications protocols] in support of maintaining continuity of operations.

Discussion: Contingency plans and the contingency training or testing associated with those plans incorporate an alternate communications protocol capability as part of establishing resilience in organizational systems. Switching communications protocols may affect software applications and operational aspects of systems. Organizations assess the potential side effects of introducing alternate communications protocols prior to implementation.

Related controls and activities: CP-02, CP-08, CP-13.

Enhancements: None.

References: None.

CP-12 Safe mode

Control: When [Assignment: organization-defined conditions] are detected, enter a safe mode of operation with [Assignment: organization-defined restrictions of safe mode of operation].

Discussion: For systems that support critical mission and business functions—including military operations, civilian space operations, nuclear power plant operations, and air traffic control operations (especially real-time operational environments)—organizations can identify certain conditions under which those systems revert to a predefined safe mode of operation. The safe mode of operation, which can be activated either automatically or manually, restricts the operations that systems can execute when those conditions are encountered. Restriction includes allowing only selected functions to execute that can be carried out under limited power or with reduced communications bandwidth.

Related controls and activities: CM-02, SA-08, SC-24, SI-13, SI-17.

Enhancements: None.

References: None.

CP-13 Alternative security mechanisms

Control: Employ [Assignment: organization-defined alternative or supplemental security mechanisms] for satisfying [Assignment: organization-defined security functions] when the primary means of implementing the security function is unavailable or compromised.

Discussion: Use of alternative security mechanisms supports system resiliency, contingency planning, and continuity of operations. To ensure mission and business continuity, organizations can implement alternative or supplemental security mechanisms. The mechanisms may be less effective than the primary mechanisms. However, having the capability to readily employ alternative or supplemental mechanisms enhances mission and business continuity that might otherwise be adversely impacted if operations had to be curtailed until the primary means of implementing the functions was restored.

Given the cost and level of effort required to provide such alternative capabilities, the alternative or supplemental mechanisms are only applied to critical security capabilities provided by systems, system components, or system services. For example, an organization may issue one-time pads to senior executives, officials, and system administrators if multi-factor tokens—the standard means for achieving secure authentication—are compromised.

Related controls and activities: CP-02, CP-11, SI-13.

Enhancements: None.

References: None.

Family: Identification and authentication

The controls and activities in the Identification and authentication (IA) family support the unique identification of users, processes acting on behalf of users and devices. They also support the authentication or verification of the identities of those users, processes or devices as a prerequisite to allowing access to organizational systems.

IA-01 Identification and authentication policy and procedures

Activity:

- A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]
 - 1. [Selection (1 or more): Organization-level; Mission/business process-level; System-level] identification and authentication (IA) policy that
 - a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
 - b. is consistent with applicable laws, jurisprudence, Orders in Council, directives, regulations, policies, standards, and guidelines
 - 2. procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls
- B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the identification and authentication policy and procedures
- C. Review and update the current identification and authentication
 - 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]
 - 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]

Discussion: Identification and authentication policy and procedures address the controls in the IA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of identification and authentication policy and procedures.

In general, security and privacy program policies and procedures at the organization level are preferable and may remove the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations.

Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.

Events that may precipitate an update to identification and authentication policy and procedures include assessment or audit findings, security incidents or breaches, including those related to privacy, or changes in applicable laws, jurisprudence, Orders in Council, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Under PIPEDA, there is a carve-out in the legislation that states that names and contact information of individuals at work are not considered to be personal information.

GC discussion: Under the federal *Privacy Act*, individuals' names or contact information at work is defined as personal information. For example, if non-organizational users rely on email addresses as part of their credentials, this would be a collection of personal information, with the associated controls required.

Related controls and activities: AC-01, PM-09, PS-08, SI-02, SI-12.

Enhancements: None.

References:

- [TBS Policy on Government Security](#)
- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [TBS Directive on Identity Management](#)
- [TBS Directive on Identity Management, Appendix A: Standard on Identity and Credential Assurance](#)
- [TBS Guideline on Defining Authentication Requirements](#)
- [TBS Guideline on Service and Digital](#)

IA-02 Identification and authentication (organizational users)

Control: Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

Discussion: Organizational users include employees or individuals whom organizations consider to be of an equivalent status to employees (e.g., contractors and guest researchers). Unique identification and authentication of users applies to all accesses other than those that are explicitly identified in AC-14 and that occur through the authorized use of group authenticators without individual authentication. Since processes execute on behalf of groups and roles, organizations may require unique identification of individuals in group accounts or for detailed accountability of individual activity.

Organizations employ passwords, physical authenticators, or biometrics to authenticate user identities or, in the case of multi-factor authentication (MFA), some combination thereof. Identity credentials and biometric authenticators may, at times, be considered personal information. Consideration of the privacy concept of necessity versus proportionality requires that organizations collect just enough personal information required to ensure accurate authentication.

Access to organizational systems is defined as either local access or network access. Local access is any access to organizational systems by users or processes acting on behalf of users, where access is obtained through direct connections without the use of networks. Network access is access to organizational systems by users (or processes acting on behalf of users) where access is obtained through network connections (i.e., non-local accesses). Remote access is a type of network access that involves communication through external networks. Internal networks include local area networks and wide area networks.

The use of encrypted VPNs for network connections between organization-controlled endpoints and non-organization-controlled endpoints may be treated as internal networks with respect to protecting the confidentiality and integrity of information traversing the network. Identification and authentication requirements for non-organizational users are described in IA-08.

GC discussion: Organizations can satisfy the identification and authentication requirements by complying with the requirements set by TBS.

Related controls and activities: AC-02, AC-03, AC-04, AC-14, AC-17, AC-18, AU-01, AU-06, IA-04, IA-05, IA-08, IA-13, MA-04, MA-05, PE-02, PL-04, SA-04, SA-08.

Enhancements:

(01) **Identification and authentication (organizational users): Strong MFA to privileged accounts**

Implement strong MFA for access to privileged accounts.

Discussion: MFA requires the use of 2 or more different factors to achieve authentication. The authentication factors are defined as follows: something you know (e.g., a personal identification number (PIN)), something you have (e.g., a physical authenticator such as a cryptographic private key), or something you are (e.g., a biometric).

MFA solutions that feature physical authenticators include hardware authenticators that provide time-based or challenge-response outputs and smart cards. In addition to authenticating users at the system level (i.e., at logon), organizations may employ authentication mechanisms at the application level, at their discretion, to provide increased security. Regardless of the type of access (i.e., local, network, remote), privileged accounts are authenticated using multi-factor options appropriate for the level of risk. Organizations can add additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.

GC discussion: In the GC, privileged users should have Level of Assurance 4 (LoA4) MFA.

Related controls and activities: AC-05, AC-06.

(02) **Identification and authentication (organizational users): MFA to non-privileged accounts**

Implement MFA for access to non-privileged accounts.

Discussion: MFA requires the use of 2 or more different factors to achieve authentication. The authentication factors are defined as follows: something you know (e.g., a PIN), something you have (e.g., a physical authenticator such as a cryptographic private key), or something you are (e.g., a biometric).

MFA solutions that feature physical authenticators include hardware authenticators that provide time-based or challenge-response outputs and smart cards. In addition to authenticating users at the system level, organizations may also employ authentication mechanisms at the application level, at their discretion, to provide increased information security. Regardless of the type of access (i.e., local, network, remote), non-privileged accounts are authenticated using multi-factor options appropriate for the level of risk. Organizations can provide additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.

GC discussion: In the GC, non-privileged users should have a minimum Level of Assurance 3 (LoA3) MFA.

Related controls and activities: AC-05.

(03) **Identification and authentication (organizational Users): Local access to privileged accounts**

Withdrawn: Incorporated into IA-02(01).

(04) **Identification and authentication (organizational users): Local access to non-privileged accounts**

Withdrawn: Incorporated into IA-02(02).

(05) **Identification and authentication (organizational users): Individual authentication with group authentication**

When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.

Discussion: Individual authentication prior to shared group authentication mitigates the risk of using group accounts or authenticators.

Related controls and activities: None.

(06) **Identification and authentication (organizational users): Access to accounts – separate device**

Implement MFA for [Selection (1 or more): local; network; remote] access to [Selection (1 or more): privileged accounts; non-privileged accounts] such that

- a. one of the factors is provided by a device separate from the system gaining access
- b. the device meets [Assignment: organization-defined strength of mechanism requirements]

Discussion: The purpose of requiring a device that is separate from the endpoint physical host through which the user is attempting to gain access as one of the factors during MFA is to reduce the likelihood of compromising the required secrets for authentication.

Adversaries may have endpoint-focused exploits to be able to compromise such secrets and subsequently impersonate authorized users. Implementing one of the factors on a separate device (e.g., a hardware token), provides a greater strength of mechanism and an increased level of assurance in the authentication process by requiring heterogeneous exploits to simultaneously compromise the secrets processed by the endpoint and by the separate device.

At times, the use of a separate device may involve the collection of personal information such as biometrics. Consideration of the privacy concept of necessity versus proportionality requires that organizations collect just enough personal information required to ensure accurate authentication.

Related controls and activities: AC-06.

(07) **Identification and authentication (organizational users): Network access to non-privileged accounts – separate device**

Withdrawn: Incorporated into IA-02(06).

(08) **Identification and authentication (organizational users): Access to accounts – replay resistant**

Implement replay-resistant authentication mechanisms for access to [Selection (1 or more): privileged accounts; non-privileged accounts].

Discussion: Authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include protocols that use nonces or challenges such as time-synchronous or cryptographic authenticators.

Related controls and activities: None.

(09) **Identification and authentication (organizational users): Network access to non-privileged accounts – replay resistant**

Withdrawn: Incorporated into IA-02(08).

(10) **Identification and authentication (organizational users): Single sign-on**

Provide a single sign-on capability for [Assignment: organization-defined system accounts and services].

Discussion: Single sign-on enables users to login once and gain access to multiple system resources. Organizations consider the operational efficiencies provided by single sign-on capabilities with the risk introduced by allowing access to multiple systems via a single authentication event. Single sign-on can present opportunities to improve system security, for example by providing the ability to add MFA for applications and systems (existing and new) that may not be able to natively support MFA.

Related controls and activities: None.

(11) **Identification and authentication (organizational users): Remote access – separate device**

Withdrawn: Incorporated into IA-02(06).

(12) **Identification and authentication (organizational users): Use of hardware token GC-issued PKI-based credentials**

Accept and electronically verify GC-issued hardware token public key infrastructure (PKI)-based credentials.

Discussion: None.

GC discussion: It is recommended that GC-issued hardware token PKI-based credentials apply to organizations implementing logical access control and physical access control systems. At times, these credentials may contain

personal information. Consideration of the privacy concept of necessity versus proportionality requires that organizations collect just enough personal information required to ensure accurate authentication.

Related controls and activities: None.

(13) **Identification and authentication (organizational users): Out-of-band authentication**

Implement the following out-of-band authentication mechanisms under [Assignment: organization-defined conditions]: [Assignment: organization-defined out-of-band authentication].

Discussion: Out-of-band authentication refers to the use of 2 separate communication paths to identify and authenticate users or devices to an information system. The first path (i.e., the in-band path) is used to identify and authenticate users or devices and is generally the path through which information flows. The second path (i.e., the out-of-band path) is used to independently verify the authentication and/or requested action.

For example, a user authenticates via a notebook computer to a remote server to which the user desires access and requests some action of the server via that communication path. Subsequently, the server contacts the user via the user's cell phone to verify that the requested action originated from the user. The user may confirm the intended action to an individual on the telephone or provide an authentication code via the telephone.

Out-of-band authentication can be used to mitigate actual or suspected adversary-in-the-middle attacks. The conditions or criteria for activation include suspicious activities, new threat indicators, elevated threat levels, or the impact or classification level of information in requested transactions.

Related controls and activities: IA-10, IA-11, SC-37.

(400) **Identification and authentication (organizational users): MFA for remote access to privileged accounts**

Withdrawn: Incorporated into IA-02(01) and IA-02(06).

References:

- [User authentication guidance for information technology systems \(ITSP.30.031\)](#)
- [Guidance on securely configuring network protocols \(ITSP.40.062\)](#)
- [RCMP GCPSG-006 Access Management Guide](#) (restricted to GC)
- [TBS Directive on Identity Management, Appendix A: Standard on Identity and Credential Assurance](#)

IA-03 Device identification and authentication

Control: Uniquely identify and authenticate [Assignment: organization-defined devices and/or types of devices] before establishing a [Selection (1 or more): local; remote; network] connection.

Discussion: Devices that require unique device-to-device identification and authentication are defined by type, device, or a combination of type and device. Organization-defined device types include devices that are not owned by the organization. Systems use shared known information (e.g., MAC or Transmission Control Protocol/Internet Protocol (TCP/IP) addresses) for device identification or organizational authentication solutions (e.g., Institute of Electrical and Electronics Engineers (IEEE) 802.1x and Extensible Authentication Protocol (EAP), RADIUS server with EAP-TLS authentication, or Kerberos) to identify and authenticate devices on local and wide area networks.

Organizations determine the required strength of authentication mechanisms based on the security categories of systems and mission or business requirements. Because of the challenges of implementing device authentication on a large scale, organizations can restrict the application of the control to a limited number/type of devices based on mission or business needs.

Related controls and activities: AC-17, AC-18, AC-19, AU-06, CA-03, CA-09, IA-04, IA-05, IA-09, IA-11, IA-13, SI-04.

Enhancements:

(01) **Device identification and authentication: Cryptographic bidirectional authentication**

Authenticate [Assignment: organization-defined devices and/or types of devices] before establishing [Selection (1 or more): local; remote; network] connection using bidirectional authentication that is cryptographically based.

Discussion: A local connection is a connection with a device that communicates without the use of a network. A network connection is a connection with a device that communicates through a network. A remote connection is a connection with a device that communicates through an external network. Bidirectional authentication provides stronger protection to validate the identity of other devices for connections that are of greater risk.

Related controls and activities: SC-08, SC-12, SC-13.

(02) **Device identification and authentication: Cryptographic bidirectional network authentication**

Withdrawn: Incorporated into IA-03(01).

(03) **Device identification and authentication: Dynamic address allocation**

- a. Where addresses are allocated dynamically, standardize dynamic address allocation lease information and the lease duration assigned to devices in accordance with [Assignment: organization-defined lease information and lease duration]
- b. Audit lease information when assigned to a device

Discussion: The Dynamic Host Configuration Protocol (DHCP) is an example of a means by which clients can dynamically receive network address assignments.

Related controls and activities: AU-02.

(04) **Device identification and authentication: Device attestation**

Handle device identification and authentication based on attestation by [Assignment: organization-defined configuration management process].

Discussion: Device attestation refers to the identification and authentication of a device based on its configuration and known operating state. Device attestation can be determined via a cryptographic hash of the device. If device attestation is the means of identification and authentication, then it is important that patches and updates to the device are handled via a configuration management process such that the patches and updates are done securely and do not disrupt identification and authentication to other devices.

Related controls and activities: CM-02, CM-03, CM-06.

References: None.

IA-04 Identifier management

Control: Manage system identifiers by:

- A. receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, service, or device identifier
- B. selecting an identifier that identifies an individual, group, role, service, or device
- C. assigning the identifier to the intended individual, group, role, service, or device
- D. preventing reuse of identifiers for [Assignment: organization-defined time period]

Discussion: Common device identifiers include MAC addresses, IP addresses, or device-unique token identifiers. The management of individual identifiers is not applicable to shared system accounts. Typically, individual identifiers are the usernames of the system accounts assigned to those individuals. In such instances, the account management activities of AC-02 use account names provided by IA-04.

Identifier management also addresses individual identifiers not necessarily associated with system accounts. Preventing the reuse of identifiers implies preventing the assignment of previously used individual, group, role, service, or device identifiers to different individuals, groups, roles, services, or devices. At times, identifier management may require the collection of personal information. Consideration of the privacy concept of necessity versus proportionality requires that organizations collect just enough personal information required to ensure accurate authentication.

Related controls and activities: AC-05, IA-02, IA-03, IA-05, IA-08, IA-09, IA-12, MA-04, PE-02, PE-03, PE-04, PL-04, PM-12, PS-03, PS-04, PS-05, SC-37.

Enhancements:

(01) Identifier management: Prohibit account identifiers as public identifiers

Prohibit the use of system account identifiers that are the same as public identifiers for individual accounts.

Discussion: Prohibiting account identifiers as public identifiers applies to any publicly disclosed account identifier used for communication, such as email and instant messaging. Prohibiting the use of systems account identifiers that are the same as some public identifier, such as the individual identifier section of an email address, makes it more difficult for adversaries to guess user identifiers. Prohibiting account identifiers as public identifiers without the implementation of other supporting controls only complicates guessing of identifiers. Additional protections are required for authenticators and credentials to protect the account.

Related controls and activities: AT-02, PT-07.

(02) Identifier management: Supervisor authorization

Withdrawn: Incorporated into IA-12(01).

(03) Identifier management: Multiple forms of certification

Withdrawn: Incorporated into IA-12(02).

(04) Identifier management: Identify user status

Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].

Discussion: Characteristics that identify the status of individuals include contractors, foreign nationals, and non-organizational users. Identifying the status of individuals by these characteristics provides additional information about the people with whom organizational personnel are communicating.

GC discussion: For example, it might be useful for a government employee to know that one of the individuals on an email message is a contractor. This is generally intended for use with national security systems.

Related controls and activities: None.

(05) Identifier management: Dynamic management

Manage individual identifiers dynamically in accordance with [Assignment: organization-defined dynamic identifier policy].

Discussion: In contrast with conventional approaches to identification that presume static accounts for preregistered users, many distributed systems establish identifiers at runtime for entities that were previously unknown. When identifiers are established at runtime for previously unknown entities, organizations can anticipate and provision for the dynamic establishment of identifiers. Pre-established trust relationships and mechanisms with appropriate authorities to validate credentials and related identifiers are essential.

Related controls and activities: AC-16.

(06) Identifier management: Cross-organization management

Coordinate with the following external organizations for cross-organization management of identifiers: [Assignment: organization-defined external organizations].

Discussion: Cross-organization identifier management provides the capability to identify individuals, groups, roles, or devices when conducting cross-organization activities involving the processing, storage, or transmission of information.

GC discussion: If there is a necessity to share personal information (such as identifiers) for cross-organization management - for example during a security investigation - consideration should be given to implementing an information sharing arrangement or agreement or contract documents designed to protect the personal identifiers.

Related controls and activities: AU-16, IA-02, IA-05.

(07) **Identifier management: In-person registration**

Withdrawn: Incorporated into IA-12(04).

(08) **Identifier management: Pairwise pseudonymous identifiers**

Generate pairwise pseudonymous identifiers.

Discussion: A pairwise pseudonymous identifier is an opaque unguessable subscriber identifier generated by an identity provider for use at a specific individual relying party. Generating distinct pairwise pseudonymous identifiers with no identifying information about a subscriber discourages the tracking and profiling of subscriber activity beyond the operational requirements established by an organization. The pairwise pseudonymous identifiers are unique to each relying party except in situations where relying parties can show a demonstrable relationship justifying an operational need for correlation, or all parties consent to being correlated in such a manner.

Related controls and activities: IA-05.

(09) **Identifier management: Attribute maintenance and protection**

Maintain the attributes for each uniquely identified individual, device, or service in [Assignment: organization-defined protected central storage].

Discussion: For each of the entities covered in IA-02, IA-03, IA-08, and IA-09, it is important to maintain the attributes for each authenticated entity on an ongoing basis in a central (protected) store.

Related controls and activities: None.

(400) **Identifier management: Biometrics protection**

Maintain adequate protection for biometrics in accordance with privacy regulations.

Discussion: Information collected about the individual for authentication purposes may constitute personal information and should be safeguarded appropriately. In cases where the biometrics are kept in their personally identifiable forms and are not hashed, it is important that they be protected in accordance with privacy regulations. It is not recommended to keep biometrics data in personally identifiable form for identification purposes.

Related controls and activities: None.

(401) **Identifier management: Biometrics integrity**

Ensure the integrity of collected biometrics.

Discussion: None.

GC discussion: The federal *Privacy Act* requires that organizations take all reasonable steps to ensure that personal information used for an administrative purpose by the institution is as accurate, up-to-date, and complete as possible.

Related controls and activities: None.

References:

- [TBS Directive on Identity Management](#)
- [Privacy Act](#)

IA-05 Authenticator management

Control: Manage system authenticators by:

- verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator
- establishing initial authenticator content for any authenticators issued by the organization
- ensuring that authenticators have sufficient strength of mechanism for their intended use
- establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators
- changing default authenticators prior to first use
- changing or refreshing authenticators [Assignment: organization-defined time period by authenticator type] or when [Assignment: organization-defined events] occur
- protecting authenticator content from unauthorized disclosure and modification
- requiring individuals to take, and having devices implement, specific controls to protect authenticators
- changing authenticators for group or role accounts when membership to those accounts changes

Discussion: Authenticators include passwords, cryptographic devices, biometrics, certificates, one-time password devices, and ID badges. Device authenticators include certificates and passwords. Initial authenticator content is the actual content of the authenticator (e.g., the initial password). In contrast, the requirements for authenticator content contain specific criteria or characteristics (e.g., minimum password length).

Developers may deliver system components with factory default authentication credentials (i.e., passwords) to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant risk. The requirement to protect individual authenticators may be implemented via control PL-04 or PS-06 for authenticators in the possession of individuals and by controls AC-03, AC-06, and SC-28 for authenticators stored in organizational systems, including passwords stored in hashed or encrypted formats or files containing encrypted or hashed passwords accessible with administrator privileges.

Systems support authenticator management by organization-defined settings and restrictions for various authenticator characteristics (e.g., minimum password length, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication). Actions can be taken to safeguard individual authenticators, including maintaining possession of authenticators, not sharing authenticators with others, and immediately reporting lost, stolen, or compromised authenticators. Authenticator management includes issuing and revoking authenticators for temporary access when no longer needed.

Related controls and activities: AC-03, AC-06, CM-06, IA-02, IA-04, IA-07, IA-08, IA-09, MA-04, PE-02, PL-04, SC-12, SC-13.

Enhancements:**(01) Authenticator management: Password-based authentication**

For password-based authentication:

- maintain a list of commonly used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly

- b. when users create or update passwords, verify that the passwords are not found on the list of commonly used, expected, or compromised passwords in IA-05(01)a
- c. transmit passwords only over cryptographically protected channels
- d. store passwords using an approved salted key derivation function, preferably using a keyed hash
- e. require immediate selection of a new password upon account recovery
- f. allow user selection of long passwords and passphrases, including spaces and all printable characters
- g. employ automated tools to assist the user in selecting strong password authenticators
- h. enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity rules]

Discussion: Password-based authentication applies to passwords regardless of whether they are used in single-factor or multi-factor authentication. Long passwords or passphrases are preferable over shorter passwords. Enforced composition rules provide marginal security benefits while decreasing usability. However, organizations may choose to establish certain rules for password generation (e.g., minimum character length for long passwords) under certain circumstances and can enforce this requirement in IA-05(01)h.

Account recovery can occur, for example, in situations when a password is forgotten. Cryptographically protected passwords include salted one-way cryptographic hashes of passwords. The list of commonly used, compromised, or expected passwords includes passwords obtained from previous breach corpuses, dictionary words, and repetitive or sequential characters. The list includes context-specific words, such as the name of the service, username, and derivatives thereof.

Recovery questions often require users to provide personal information. Consideration of the privacy concept of necessity versus proportionality requires that organizations collect just enough personal information required to ensure accurate authentication. The use of pre-registered knowledge tokens is not recommended for account recovery.

Related controls and activities: IA-06.

(02) **Authenticator management: Public key-based authentication**

- a. For public key-based authentication
 - 1) enforce authorized access to the corresponding private key
 - 2) map the authenticated identity to the account of the individual or group
- b. When PKI is used
 - 1) validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information
 - 2) implement a local cache of revocation data to support path discovery and validation

Discussion: Public key cryptography is a valid authentication mechanism for individuals, machines, and devices. For PKI solutions, status information for certification paths includes certificate revocation lists or certificate status protocol responses. Implementing a local cache of revocation data to support path discovery and validation also supports system availability in situations where organizations are unable to access revocation information via the network.

Related controls and activities: IA-03, SC-17.

(03) **Authenticator management: In-person or trusted external party registration**

Withdrawn: Incorporated into IA-12(04).

(04) Authenticator management: Automated support for password strength determination

Withdrawn: Incorporated into IA-05(01).

(05) Authenticator management: Change authenticators prior to delivery

Require developers and installers of system components to provide unique authenticators or change default authenticators prior to delivery and installation.

Discussion: Changing authenticators prior to the delivery and installation of system components extends the requirement for organizations to change default authenticators upon system installation by requiring developers and/or installers to provide unique authenticators or change default authenticators for system components prior to delivery and/or installation. However, it typically does not apply to developers of COTS IT products. Requirements for unique authenticators can be included in acquisition documents prepared by organizations when procuring systems or system components.

Related controls and activities: None.

(06) Authenticator management: Protection of authenticators

Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.

Discussion: For systems that contain multiple security categories of information without reliable physical or logical separation between categories, authenticators used to grant access to the systems are protected commensurate with the highest security category of information on the systems. Security categories of information are determined as part of the security categorization process.

Related controls and activities: RA-02.

(07) Authenticator management: No embedded unencrypted static authenticators

Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage.

Discussion: In addition to applications, other forms of static storage include access scripts and function keys. Organizations exercise caution when determining whether embedded or stored authenticators are in encrypted or unencrypted form. If authenticators are used in the manner stored, then those representations are considered unencrypted authenticators.

Related controls and activities: None.

(08) Authenticator management: Multiple system accounts

Implement [Assignment: organization-defined security controls] to manage the risk of compromise due to individuals having accounts on multiple systems.

Discussion: When individuals have accounts on multiple systems and use the same authenticators such as passwords, there is the risk that a compromise of one account may lead to the compromise of other accounts. Alternative approaches include having different authenticators (passwords) on all systems, employing a single sign-on or federation mechanism, or using some form of one-time passwords on all systems. Organizations can also use rules of behaviour (see PL-04) and access agreements (see PS-06) to mitigate the risk of multiple system accounts.

Related controls and activities: PS-06.

(09) Authenticator management: Federated credential management

Use the following external organizations to federate credentials: [Assignment: organization-defined external organizations].

Discussion: Federation provides organizations with the capability to authenticate individuals and devices when conducting cross-organization activities involving the processing, storage, or transmission of information. Using a

specific list of approved external organizations for authentication helps to ensure that those organizations are vetted and trusted.

Related controls and activities: AU-07, AU-16.

(10) **Authenticator management: Dynamic credential binding**

Bind identities and authenticators dynamically using the following rules: [Assignment: organization-defined binding rules].

Discussion: Authentication requires some form of binding between an identity and the authenticator that is used to confirm the identity. In conventional approaches, binding is established by pre-provisioning both the identity and the authenticator to the system. For example, the binding between a username (i.e., identity) and a password (i.e., authenticator) is accomplished by provisioning the identity and authenticator as a pair in the system.

New authentication techniques allow the binding between the identity and the authenticator to be implemented external to a system. For example, with smartcard credentials, the identity and authenticator are bound together on the smartcard. Using these credentials, systems can authenticate identities that have not been pre-provisioned, dynamically provisioning the identity after authentication. In these situations, organizations can anticipate the dynamic provisioning of identities. Pre-established trust relationships and mechanisms with appropriate authorities to validate identities and related credentials are essential.

Related controls and activities: AU-16, IA-05.

(11) **Authenticator management: Hardware token-based authentication**

Withdrawn: Incorporated into IA-02(01) and IA-02(02).

(12) **Authenticator management: Biometric authentication performance**

For biometric-based authentication, employ mechanisms that satisfy the following biometric quality requirements [Assignment: organization-defined biometric quality requirements].

Discussion: Unlike password-based authentication, which provides exact matches of user-input passwords to stored passwords, biometric authentication does not provide exact matches. Depending on the type of biometric and the type of collection mechanism, there is likely to be some divergence from the presented biometric and the stored biometric that serves as the basis for comparison. Matching performance is the rate at which a biometric algorithm correctly results in a match for a genuine user and rejects other users. Biometric performance requirements include the match rate, which reflects the accuracy of the biometric matching algorithm used by a system.

GC discussion: The federal *Privacy Act* requires that organizations take all reasonable steps to ensure that personal information that is used for an administrative purpose by the institution is as accurate, up-to-date, and complete as possible.

Related controls and activities: AC-07.

(13) **Authenticator management: Expiration of cached authenticators**

Prohibit the use of cached authenticators after [Assignment: organization-defined time period].

Discussion: Cached authenticators are used to authenticate to the local machine when the network is not available. If cached authentication information is out of date, the validity of the authentication information may be questionable.

Related controls and activities: None.

(14) **Authenticator management: Managing content of PKI trust stores**

For PKI-based authentication, employ an organization-wide methodology for managing the content of PKI trust stores installed across all platforms, including networks, operating systems, browsers, and applications.

Discussion: An organization-wide methodology for managing the content of PKI trust stores helps improve the accuracy and currency of PKI-based authentication credentials across the organization.

Related controls and activities: None.

(15) **Authenticator management: Identity, credential and authentication assurance levels compliant products and services**

Use only products and services for identity, credential, authentication, and access management that are compliant with the required assurance levels.

Discussion: None.

GC discussion: Products and services need to be compliant with the requirements set by TBS in its Standard on Identity and Credential Assurance and by the Cyber Centre in User authentication guidance for information technology systems (ITSP.30.031). The required identity, credential and authentication levels of assurance need to be documented and controls that mitigate risks and allow to achieve requirements must be applied.

Related controls and activities: None.

(16) **Authenticator management: In-person or trusted external party authenticator issuance**

Require that the issuance of [Assignment: organization-defined types of and/or specific authenticators] be conducted [Selection (1): in person; by a trusted external party] before [Assignment: organization-defined registration authority] with authorization by [Assignment: organization-defined personnel or roles].

Discussion: Issuing authenticators in person or by a trusted external party enhances and reinforces the trustworthiness of the identity proofing process.

Related controls and activities: IA-12.

(17) **Authenticator management: Presentation attack detection for biometric authenticators**

Employ presentation attack detection mechanisms for biometric-based authentication.

Discussion: Biometric characteristics do not constitute authentication secrets. Such characteristics can be obtained by online web accesses, taking a picture of someone with a camera phone to obtain facial images with or without their knowledge, lifting from objects that someone has touched (e.g., a latent fingerprint), or capturing a high-resolution image (e.g., an iris pattern). Presentation attack detection technologies, including liveness detection, can mitigate the risk of these types of attacks by making it difficult to produce artifacts intended to defeat the biometric sensor.

Related controls and activities: AC-07.

(18) **Authenticator management: Password managers**

- a. Employ [Assignment: organization-defined password managers] to generate and manage passwords
- b. Protect the passwords using [Assignment: organization-defined controls]

Discussion: For systems where static passwords are employed, it is often a challenge to ensure that the passwords are suitably complex and that the same passwords are not employed on multiple systems. A password manager is a solution to this problem as it automatically generates and stores strong and different passwords for various accounts. A potential risk of using password managers is that adversaries can target the collection of passwords generated by the password manager. Therefore, the collection of passwords requires protection including encrypting the passwords (see IA-05(01)d) and storing the collection offline in a token.

Related controls and activities: None.

References:

- [User authentication guidance for information technology systems \(ITSP.30.031\)](#)

- [TBS Policy on Government Security](#)
- [TBS Directive on Identity Management](#)
- [TBS Directive on Identity Management, Appendix A: Standard on Identity and Credential Assurance](#)
- [Privacy Act](#)

IA-06 Authentication feedback

Control: Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

Discussion: Authentication feedback from systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of systems, such as desktops or notebooks with relatively large monitors, the threat (referred to as shoulder surfing) may be significant. For other types of systems, such as mobile devices with small displays, the threat may be less significant and is balanced against the increased likelihood of typographic input errors due to small keyboards. Thus, the means for obscuring authentication feedback is selected accordingly. Obscuring authentication feedback includes displaying asterisks when users type passwords into input devices or displaying feedback for a very limited time before obscuring it.

Related controls and activities: AC-03.

Enhancements: None.

References: None.

IA-07 Cryptographic module authentication

Control: Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Orders in Council, directives, policies, regulations, standards, and guidelines for such authentication.

Discussion: Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role.

Related controls and activities: AC-03, IA-05, SA-04, SC-12, SC-13.

Enhancements: None.

References:

- [Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B information \(ITSP.40.111\)](#)
- [User authentication guidance for information technology systems \(ITSP.30.031\)](#)
- [NIST FIPS 140-3 Security Requirements for Cryptographic Modules](#)

IA-08 Identification and authentication (non-organizational users)

Control: Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

Discussion: Non-organizational users include system users other than organizational users explicitly covered by IA-02. Non-organizational users are uniquely identified and authenticated for accesses other than those explicitly identified and documented in AC-14. Identification and authentication of non-organizational users accessing federal systems may be required to protect federal, proprietary, or personal information (with exceptions noted for national security systems).

Organizations consider many factors – including security, privacy, scalability, and practicality – when balancing the need to ensure ease of use for access to federal information and systems with the need to protect and adequately mitigate risk.

Related controls and activities: AC-02, AC-06, AC-14, AC-17, AC-18, AU-06, IA-02, IA-04, IA-05, IA-10, IA-11, IA-13, MA-04, RA-03, SA-04, SC-08.

Enhancements:

(01) **Identification and authentication (non-organizational users): Acceptance of PKI-based credentials from other agencies**

Accept and electronically verify PKI-based credentials from other GC departments and agencies.

Discussion: None.

GC discussion: Acceptance of PKI-based credentials from other GC departments and agencies applies to both logical and physical access control systems.

Related controls and activities: PE-03.

(02) **Identification and authentication (non-organizational users): Acceptance of external authenticators**

- a. Accept only external authenticators that are compliant with ITSP.30.031-appropriate level of assurance
- b. Document and maintain a list of accepted external authenticators

Discussion: None.

GC discussion: Approved external authenticators meet or exceed the minimum GC technical, security, privacy, and organizational maturity requirements. Meeting or exceeding GC requirements allows GC relying parties to trust external authenticators in connection with an authentication transaction at a specified authenticator assurance level. Examples of this in the GC are the Sign-In Partners and GCKey programs.

Sign-In Partners are private sector organizations that have partnered with SecureKey Technologies to enable their customers to use their online credentials to access GC services. GCKey is the government-branded issued credential. Both have the same authentication process and security requirements and are compliant with the *Privacy Act*.

Related controls and activities: None.

(03) **Identification and authentication (non-organizational users): Use of Federal Identity, Credential, and Access Management (FICAM)-approved products**

Withdrawn: Incorporated into IA-08(02) and specific to the US.

(04) **Identification and authentication (non-organizational users): Use of defined profiles**

Conform to the following profiles for identity management [Assignment: organization-defined identity management profiles].

Discussion: Organizations define profiles for identity management based on open identity management standards. To ensure that open identity management standards are viable, robust, reliable, sustainable, and interoperable as documented, the GC assesses and scopes the standards and technology implementations against applicable laws, Orders in Council, directives, policies, regulations, standards, and guidelines.

Related controls and activities: None.

(05) **Identification and authentication (non-organizational users): Acceptance of Personal Identity Verification (PIV)-I credentials**

Accept and verify federated or PKI credentials that meet [Assignment: organization-defined policy].

Discussion: Acceptance of PIV-I credentials can be implemented by PIV, PIV-I, and other commercial or external identity providers. The acceptance and verification of PIV-I-compliant credentials in Canada is only possible for logical access control systems. The acceptance and verification of PIV-I credentials address non-federal issuers of identity cards that desire to interoperate with the GC PKI-based systems and that can be trusted by GC-relying parties.

The PIV-I meets the token requirements of the X.509 certificate policy for the Canadian Federal PKI Bridge. PIV-I credentials are the credentials issued by a PIV-I provider whose PIV-I certificate policy maps to the Canadian Federal PKI Bridge. A PIV-I provider is cross-certified with the Federal Bridge CA (directly or through another PKI bridge) with policies that have been mapped and approved as meeting the requirements defined in the Canadian Federal PKI Bridge certificate policy.

Related controls and activities: None.

(06) **Identification and authentication (non-organizational users): Disassociability**

Implement the following measures to disassociate user attributes or identifier assertion relationships among individuals, credential service providers, and relying parties: [Assignment: organization-defined measures].

Discussion: Federated identity solutions can create increased privacy risks due to the tracking and profiling of individuals. Using identifier mapping tables or cryptographic techniques to blind credential service providers and relying parties from each other or to make identity attributes less visible to transmitting parties can reduce these privacy risks.

Related controls and activities: None.

(400) **Identification and authentication (non-organizational users): Identity and credential assurance**

Withdrawn: Incorporated into IA-05(15).

References:

- [User authentication guidance for information technology systems \(ITSP.30.031\)](#)
- [TBS Directive on Identity Management](#)
- [TBS Directive on Identity Management, Appendix A: Standard on Identity and Credential Assurance](#)
- [TBS Guideline on Defining Authentication Requirements](#)
- [TBS Guideline on the Management of Public Key Infrastructure in the Government of Canada](#)
- [TBS Guideline on Identity Assurance](#)
- [Privacy Act](#)

IA-09 Service identification and authentication

Control: Uniquely identify and authenticate [Assignment: organization-defined system services and applications] before establishing communications with devices, users, or other services or applications.

Discussion: Services that may require identification and authentication include web applications using digital certificates or services or applications that query a database. Identification and authentication methods for system services and applications include information or code signing, provenance graphs, and electronic signatures that indicate the sources of services. Decisions regarding the validity of identification and authentication claims can be made by services separate from the services acting on those decisions. This can occur in distributed system architectures. In such situations, the identification and authentication decisions (instead of actual identifiers and authentication data) are provided to the services that need to act on those decisions.

Related controls and activities: IA-03, IA-04, IA-05, IA-13, SC-08.

Enhancements:

(01) **Service identification and authentication: Information exchange**

Withdrawn: Incorporated into IA-09.

(02) **Service identification and authentication: Transmission of decisions**

Withdrawn: Incorporated into IA-09.

References: None.

IA-10 Adaptive authentication

Control: Require individuals accessing the system to employ [Assignment: organization-defined supplemental authentication techniques or mechanisms] under specific [Assignment: organization-defined circumstances or situations].

Discussion: Adversaries may compromise individual authentication mechanisms employed by organizations and subsequently attempt to impersonate legitimate users. To address this threat, organizations may employ specific techniques or mechanisms and establish protocols to assess suspicious behaviour. Suspicious behaviour may include accessing information that individuals do not typically access as part of their duties, roles, or responsibilities; accessing greater quantities of information than individuals would routinely access; or attempting to access information from suspicious network addresses.

When pre-established conditions or triggers occur, organizations can require individuals to provide additional authentication information. Another potential use for adaptive authentication is to increase the strength of mechanism based on the number or types of records being accessed. Adaptive authentication does not replace and is not used to avoid the use of MFA mechanisms but can augment implementations of MFA.

Related controls and activities: IA-02, IA-08.

Enhancements: None.

References:

- [A zero-trust approach to security architecture \(ITSM.10.008\)](#)
- [Steps for effectively deploying multi-factor authentication \(MFA\) \(ITSAP.00.105\)](#)

IA-11 Re-authentication

Control: Require users to re-authenticate when [Assignment: organization-defined circumstances or situations requiring re-authentication].

Discussion: In addition to the re-authentication requirements associated with device locks, organizations may require re-authentication of individuals in certain situations, including when roles, authenticators, or credentials change, when security categories of systems change, when the execution of privileged functions occurs, after a fixed time period, or periodically.

Related controls and activities: AC-03, AC-11, IA-02, IA-03, IA-04, IA-08.

Enhancements: None.

References: None.

IA-12 Identity proofing

Control:

- Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines
- Resolve user identities to a unique individual

C. Collect, validate, and verify identity evidence

Discussion: Identity proofing is the process of collecting, validating, and verifying a user's identity information for the purposes of establishing credentials for accessing a system. The information required for identity proofing may require the collection or confirmation of personal information data elements, such as date of birth. Identity proofing is intended to mitigate threats to the registration of users and the establishment of their accounts.

Organizations may be subject to laws, Orders in Council, directives, regulations, or policies that address the collection of identity evidence. Organizational personnel should consult with the appropriate privacy senior official or executive and legal counsel regarding such requirements. Any personal information requested from an individual for identity proofing requires that the organization collecting the information have lawful authority for the collection.

GC discussion: Standards and guidelines specifying identity assurance levels for identity proofing include Appendix A: Standard on Identity and Credential Assurance of the TBS Directive on Identity Management.

Related controls and activities: AC-05, IA-01, IA-02, IA-03, IA-04, IA-05, IA-06, IA-08, IA-13.

Enhancements:

(01) Identity proofing: Supervisor authorization

Require that the registration process to receive an account for logical access includes supervisor or sponsor authorization.

Discussion: Including supervisor or sponsor authorization as part of the registration process provides an additional level of scrutiny to ensure that the user's management chain is aware of the account, the account is essential to carry out organizational missions and functions, and the user's privileges are appropriate for the anticipated responsibilities and authorities within the organization.

Related controls and activities: None.

(02) Identity proofing: Identity evidence

Require evidence of individual identification be presented to the registration authority.

Discussion: Identity evidence, such as documentary evidence or a combination of documents and biometrics, reduces the likelihood of individuals using fraudulent identification to establish an identity or at least increases the work factor of potential adversaries. The forms of acceptable evidence are consistent with the risks to the systems, roles, and privileges associated with the user's account.

Most forms of identity evidence are considered to be personal information; in the case of biometrics, this information may be subject to additional safeguard requirements. Biometric information, if collected for individual identification, should only be used for the purpose for which it was collected. When considering the use of biometrics, the registration authority should consider if the collection is demonstrably necessary; likely to be effective; considers the loss of individual privacy against the benefit gained; and whether there is a less privacy-invasive approach that achieves the same identity confirmation.

Related controls and activities: None.

(03) Identity proofing: Identity evidence validation and verification

Require that the presented identity evidence be validated and verified through [Assignment: organizational defined methods of validation and verification].

Discussion: Validation and verification of identity evidence increases the assurance that accounts and identifiers are being established for the correct user and authenticators are being bound to that user. Validation refers to the process of confirming that the evidence is genuine and authentic, and the data contained in the evidence is correct, current, and related to an individual. Verification confirms and establishes a linkage between the claimed identity and the actual existence of the user presenting the evidence. Acceptable methods for validating and verifying

identity evidence are consistent with the risks to the systems, roles, and privileges associated with the user's account.

GC discussion: Validation and verification of identity evidence is a requirement of the *Privacy Act*.

Related controls and activities: None.

(04) **Identity proofing: In-person validation and verification**

Require that the validation and verification of identity evidence be conducted in person before a designated registration authority.

Discussion: In-person proofing reduces the likelihood of fraudulent credentials being issued because it requires the physical presence of individuals, the presentation of physical identity documents, and actual face-to-face interactions with designated registration authorities.

Related controls and activities: None.

(05) **Identity proofing: Address confirmation**

Require that a [Selection (1): registration code; notice of proofing] be delivered through an out-of-band channel to verify the users address (physical or digital) of record.

Discussion: To make it more difficult for adversaries to pose as legitimate users during the identity proofing process, organizations can use out-of-band methods to ensure that the individual associated with an address of record is the same individual that participated in the registration. Confirmation can take the form of a temporary enrollment code or a notice of proofing. The delivery address for these artifacts is obtained from records and not self-asserted by the user. The address can include a physical or digital address. A home address is an example of a physical address. Email addresses and telephone numbers are examples of digital addresses.

Related controls and activities: IA-12.

(06) **Identity proofing: Accept externally proofed identities**

Accept externally proofed identities at [Assignment: organization-defined identity assurance level].

Discussion: To limit unnecessary re-proofing of identities, particularly of users without GC-issued PKI credentials, organizations accept proofing conducted at a commensurate level of assurance by other agencies or organizations. Proofing is consistent with organizational security policy and the identity assurance level appropriate for the system, application, or information accessed. Accepting externally proofed identities is a fundamental component of managing federated identities across agencies and organizations.

Related controls and activities: IA-03, IA-04, IA-05, IA-08.

References:

- [TBS Directive on Identity Management, Appendix A: Standard on Identity and Credential Assurance](#)
- [TBS Guideline on Defining Authentication Requirements](#)
- [TBS Guideline on Identity Assurance](#)
- [Privacy Act](#)

IA-13 Identity providers and authorization servers

Control: Employ identity providers and authorization servers to manage user, device, and non-person entity (NPE) identities, attributes, and access rights supporting authentication and authorization decisions in accordance with [Assignment: organization-defined identification and authentication policy] using [Assignment: organization-defined mechanisms].

Discussion: Identity providers, both internal and external to the organization, manage the user, device and NPE authenticators, and issue statements, often called identity assertions, attesting to identities of other systems or systems components.

Authorization servers create and issue access tokens to identified and authenticated users and devices that can be used to gain access to system or information resources. For example, single sign-on (SSO) provides identity provider and authorization server functions. Authenticator management (to include credential management) is covered by IA-05.

Related controls and activities: AC-03, IA-02, IA-03, IA-08, IA-09, IA-12.

Enhancements:

(01) Identity providers and authorization servers: Protection of cryptographic keys

Cryptographic keys that protect access tokens are generated, managed, and protected from disclosure and misuse.

Discussion: Identity assertions and access tokens are typically digitally signed. The private keys used to sign these assertions and tokens are protected commensurate with the impact of the system and information resources that can be accessed.

Related controls and activities: SC-12, SC-13.

(02) Identity providers and authorization servers: Verification of identity assertions and access tokens

The source and integrity of identity assertions and access tokens are verified before granting access to system and information resources.

Discussion: This includes verification of digital signatures protecting identity assertions and access tokens, as well as included metadata. Metadata includes information about the access request such as information unique to the user, system, or information resource being accessed, or the transaction itself such as time. Protected system and information resources could include connected networks, applications, and APIs.

Related controls and activities: None.

(03) Identity providers and authorization servers: Token management

In accordance with [Assignment: organization-defined identification and authentication policy], assertions and access tokens are:

- a. generated
- b. issued
- c. refreshed
- d. revoked
- e. time-restricted
- f. audience-restricted

Discussion: An access token is a piece of data that represents the authorization granted to a user or NPE to access specific systems or information resources. Access tokens enable controlled access to services and resources. Properly managing the lifecycle of access tokens, including their issuance, validation, and revocation, is crucial to maintaining confidentiality of data and systems. Restricting token validity to a specific audience – for example, an application or security domain – and restricting token validity lifetimes are important practices. Access tokens are revoked or invalidated if they are compromised, lost, or are no longer needed to mitigate the risks associated with stolen or misused tokens.

Related controls and activities: None.

References:

- [TBS Directive on Identity Management, Appendix A: Standard on Identity and Credential Assurance](#)

- [NIST FIPS 186-5 Digital Signature Standard \(DSS\)](#)
- [NIST FIPS 198-1 The Keyed-Hash Message Authentication Code \(HMAC\)](#)

Family: Incident response

The controls and activities in the Incident response (IR) family support the establishment of an operational incident handling capability for organizational systems, that includes adequate preparation, monitoring, detection, analysis, containment, recovery, and response. Incidents are monitored, documented, and reported to appropriate organizational officials and authorities.

IR-01 Incident response policy and procedures

Activity:

- A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]
 - 1. [Selection (1 or more): Organization-level; Mission/business process-level; System-level] incident response policy that
 - a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
 - b. is consistent with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines
 - 2. procedures to facilitate the implementation of the incident response policy and the associated incident response controls
- B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the incident response policy and procedures
- C. Review and update the current incident response
 - 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]
 - 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]

Discussion: Incident response policy and procedures address the controls in the IR family that are implemented within systems and organizations. Incident response must include privacy-specific measures when personal information is involved. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of incident response policy and procedures.

In general, security and privacy program policies and procedures at the organization level are preferable and may remove the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations.

Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to incident response policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, Orders in Council, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure. It is recommended that an organization's incident response policy and procedures incorporate heightened levels of readiness during emergency and heightened cyber threat situations.

GC discussion: GC departments' and agencies' incident response policy and procedures shall incorporate heightened levels of readiness during emergency and heightened cyber threat situations in accordance with the TBS Directive on Security

Management, Appendix G: Mandatory Procedures for Security Event Management Control and Appendix B: Mandatory Procedures for Information Technology Security Control.

Related controls and activities: PM-09, PS-08, SI-02, SI-12.

Enhancements: None.

References:

- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [TBS Directive on Security Management, Appendix G: Mandatory Procedures for Security Event Management Control](#)
- [TBS Directive on Security Management, Appendix I: Standard on Security Event Reporting](#)
- [TBS Directive on Security Management, Appendix J: Standard on Security Categorization](#)
- [TBS Directive on Privacy Practices](#)
- [OPC Contain a privacy breach at your business](#)
- [TBS Government of Canada Digital Operations Strategic Plan](#)
- Directive for the Control of COMSEC Material in the Government of Canada (ITSD-03A) (upon request to the Cyber Centre)
- [TBS Significant Event Information Sharing Protocol](#) (restricted to GC)

IR-02 Incident response training

Control:

- A. Provide incident response training to system users consistent with assigned roles and responsibilities
 1. within [Assignment: organization-defined time period] of assuming an incident response role or responsibility or acquiring system access
 2. when required by system changes
 3. [Assignment: organization-defined frequency] thereafter
- B. Review and update incident response training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]

Discussion: Incident response training is associated with the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail are included in such training. For example, users may only need to know who to call or how to recognize an incident; system administrators may require additional training on how to handle incidents; and incident responders may receive more specific training on forensics, data collection techniques, reporting, system recovery, and system restoration.

Incident response training includes user training in identifying and reporting suspicious activities from external and internal sources. Incident response training for users may be provided as part of AT-02 or AT-03. Events that may precipitate an update to incident response training content include, but are not limited to, incident response plan testing or response to an actual incident (lessons learned), assessment or audit findings, or changes in applicable laws, jurisprudence, Orders in Council, directives, regulations, policies, standards, and guidelines.

GC discussion: Executives should engage their institution's Access to Information and Privacy (ATIP) Office or Chief Privacy Officer (CPO) to determine what training opportunities related to assessing and mitigating privacy breaches may be provided to suit their particular needs or to identify what services may be offered to support their program area.

Related controls and activities: AT-02, AT-03, AT-04, CP-03, IR-03, IR-04, IR-08, IR-09.

Enhancements:

(01) **Incident response training: Simulated events**

Incorporate simulated events into incident response training to facilitate the required response by personnel in crisis situations.

Discussion: Organizations establish requirements for responding to incidents in incident response plans. Incorporating simulated events into incident response training helps to ensure that personnel understand their individual responsibilities and what specific actions to take in crisis situations.

Related controls and activities: None.

(02) Incident response training: Automated training environments

Provide an incident response training environment using [Assignment: organization-defined automated mechanisms].

Discussion: Automated mechanisms can provide a more thorough and realistic incident response training environment. This can be accomplished, for example, by providing more complete coverage of incident response issues, selecting more realistic training scenarios and environments, and stressing the response capability.

Related controls and activities: None.

(03) Incident response training: Privacy breach

Provide incident response training on how to identify and respond to a privacy breach, including the organization's process for reporting a privacy breach.

Discussion: The incident response training emphasizes the obligation of individuals to report both confirmed and suspected breaches involving information in any medium or form, including paper, oral, and electronic. Incident response training includes tabletop exercises that simulate a breach. See IR-02(01).

GC discussion: For federal departments and agencies, an incident that involves personal information is considered a privacy breach. A privacy breach results in the loss of control, compromise, unauthorized disclosure, unpermitted use, unlawful collection, improper retention or disposal, or a similar occurrence where a person other than an authorized user accesses or potentially accesses or an authorized user accesses or potentially accesses such information for other than authorized purposes.

The incident response training includes the organization's process for reporting a privacy breach to the OPC or TBS.

Related controls and activities: None.

References:

- [TBS Directive on Security Management, Appendix D: Mandatory Procedures for Business Continuity Management Control](#)
- [Developing your incident response plan \(ITSAP.40.003\)](#)
- [TBS Directive on Personal Information Requests and Correction of Personal Information, Appendix B: Mandatory Procedures for Privacy Training](#)
- [TBS Directive on Privacy Practices, Appendix B: Mandatory Procedures for Privacy Breaches](#)
- [TBS Privacy Breach Management Toolkit](#)
- [TBS Government of Canada Cyber Security Event Management Plan \(GC CSEMP\)](#)

IR-03 Incident response testing

Control: Test the effectiveness of the incident response capability for the system [Assignment: organization-defined frequency] using the following tests: [Assignment: organization-defined tests].

Discussion: Organizations test incident response capabilities to determine their effectiveness and identify potential weaknesses or deficiencies. Incident response testing includes the use of checklists, walk-through or tabletop exercises, and simulations (parallel or full interrupt). Incident response testing can include a determination of the effects on

organizational operations and assets and individuals due to incident response. The use of qualitative and quantitative data aids in determining the effectiveness of incident response processes.

Related controls and activities: CP-03, CP-04, IR-02, IR-04, IR-08, PM-14.

Enhancements:

(01) Incident response testing: Automated testing

Test the incident response capability using [Assignment: organization-defined automated mechanisms].

Discussion: Organizations use automated mechanisms to test incident response capabilities more thoroughly and effectively. This can be accomplished by providing more complete coverage of incident response issues, selecting realistic test scenarios and environments, and stressing the response capability.

Related controls and activities: None.

(02) Incident response testing: Coordination with related plans

Coordinate incident response testing with organizational elements responsible for related plans.

Discussion: Organizational plans related to incident response testing include business continuity plans, disaster recovery plans, continuity of operations plans, contingency plans, crisis communications plans, critical infrastructure plans, and occupant emergency plans.

Related controls and activities: None.

(03) Incident response testing: Continuous improvement

Use qualitative and quantitative data from testing to:

- a. determine the effectiveness of incident response processes
- b. continuously improve incident response processes
- c. provide incident response measures and metrics that are accurate, consistent, and in a reproducible format
- d. identify trends to facilitate the identification of underlying patterns with respect to information-handling practices to prevent further breaches

Discussion: To help incident response activities function as intended, organizations may use metrics and evaluation criteria to assess incident response programs as part of an effort to continually improve response performance. These efforts facilitate improvement in incident response efficacy and lessen the impact of incidents.

Related controls and activities: None.

References:

- [TBS Government of Canada Cyber Security Event Management Plan \(GC CSEMP\)](#)
- [TBS Directive on Security Management, Appendix D: Mandatory Procedures for Business Continuity Management Control](#)
- [Developing your incident response plan \(ITSAP.40.003\)](#)
- [TBS Privacy Breach Management Toolkit](#)

IR-04 Incident handling

Control:

- A. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery

- B. Coordinate incident handling activities with contingency planning activities
- C. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly
- D. Ensure the rigour, intensity, scope, and results of incident handling activities are comparable and predictable across the organization

Discussion: Organizations recognize that incident response capabilities are dependent on the capabilities of organizational systems and the mission and business processes being supported by those systems. Organizations should consider incident response as part of the definition, design, and development of mission and business processes and systems. Incident-related information can be obtained from a variety of sources, including audit monitoring, physical access monitoring, and network monitoring; user or administrator reports; complaints from the public or oversight bodies; and reported supply chain events.

An effective incident handling capability includes coordination among many organizational entities (e.g., mission or business owners, system owners, authorizing officials, human resources offices, physical security offices, personnel security offices, legal departments, risk executive [function], operations personnel, or procurement offices).

Suspected security incidents include the receipt of suspicious email communications that can contain malicious code. Suspected supply chain incidents include the insertion of counterfeit hardware or malicious code into organizational systems or system components.

GC discussion: For federal departments and agencies, an incident that involves personal information is considered a privacy breach. A privacy breach results in the loss of control, compromise, unauthorized disclosure, unpermitted use, unlawful collection, improper retention or disposal, or a similar occurrence where a person other than an authorized user accesses or potentially accesses or an authorized user accesses or potentially accesses such information for other than authorized purposes.

If the incident involves the breach of personal information, the response steps include preliminary assessment and containment; full assessment; notification of affected individuals; mitigation and prevention; notification to the OPC or TBS; and lessons learned.

Breaches of personal information can be considered material breaches if they involve sensitive personal information, could reasonably be expected to cause serious injury or harm to the individual, or involve a large number of affected individuals. Notification procedures may be different for material breaches.

Related controls and activities: AC-19, AU-06, AU-07, CM-06, CP-02, CP-03, CP-04, IR-02, IR-03, IR-05, IR-06, IR-08, PE-06, PL-02, PM-12, SA-08, SA-15, SC-05, SC-07, SI-02, SI-03, SI-04, SI-07.

Enhancements:

(01) Incident handling: Automated incident handling processes

Support the incident handling process using [Assignment: organization-defined automated mechanisms].

Discussion: Automated mechanisms that support incident handling processes include online incident management systems and tools that support the collection of live response data, full network packet capture, and forensic analysis.

Related controls and activities: None.

(02) Incident handling: Dynamic reconfiguration

Include the following types of dynamic reconfiguration for [Assignment: organization-defined system components] as part of the incident response capability: [Assignment: organization-defined types of dynamic reconfiguration].

Discussion: Dynamic reconfiguration includes changes to router rules, access control lists, intrusion detection or prevention system parameters, and filter rules for guards or firewalls. Organizations may perform dynamic reconfiguration of systems to stop attacks, misdirect attackers, and isolate components of systems, thus limiting

the extent of the damage from breaches or compromises. Organizations should include specific time frames for achieving the reconfiguration of systems in the definition of the reconfiguration capability, considering the potential need for rapid response to effectively address cyber threats.

Related controls and activities: AC-02, AC-04, CM-02.

(03) **Incident handling: Continuity of operations**

Identify [Assignment: organization-defined classes of incidents] and take the following actions in response to those incidents to ensure continuation of organizational mission and business functions: [Assignment: organization-defined actions to take in response to classes of incidents].

Discussion: Classes of incidents include malfunctions due to design or implementation errors and omissions, targeted malicious attacks, and untargeted malicious attacks. Incident response actions include orderly system degradation, system shutdown, fall-back to manual mode or activation of alternative technology whereby the system operates differently, employing deceptive measures, alternate information flows, or operating in a mode that is reserved for when systems are under attack.

Organizations should consider whether continuity of operations requirements during an incident conflict with the capability to automatically disable the system as specified as part of IR-04(05).

Related controls and activities: None.

(04) **Incident handling: Information correlation**

Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

Discussion: Sometimes, a threat event, such as a hostile cyber attack, can only be observed by bringing together information from different sources, including various reports and reporting procedures established by organizations.

Related controls and activities: None.

(05) **Incident handling: Automatic disabling of system**

Implement a configurable capability to automatically disable the system if [Assignment: organization-defined security violations] are detected.

Discussion: Organizations should consider whether the capability to automatically disable the system conflicts with continuity of operations requirements specified as part of CP-02 or IR-04(03). Security violations include cyber attacks that have compromised the integrity of the system or exfiltrated organizational information and serious errors in software programs that could adversely impact organizational missions or functions or jeopardize the safety of individuals. Automatic disabling of a system may be used as a technique to contain the privacy breach, in the event that the incident involves the compromise of personal information held within a system.

Related controls and activities: None.

(06) **Incident handling: Insider threats**

Implement an incident handling capability for incidents involving insider threats.

Discussion: Explicit focus on handling incidents involving insider threats highlights the seriousness of this type of threat and the need for specific incident handling capabilities to respond appropriately and in a timely manner.

Related controls and activities: None.

(07) **Incident Handling: Insider threats – intra-organization coordination**

Coordinate an incident handling capability for insider threats that includes the following organizational entities [Assignment: organization-defined entities].

Discussion: Incident handling (e.g., preparation, detection and analysis, containment, eradication, and recovery) for insider threat incidents requires coordination among many organizational entities, including mission or business owners, system owners, human resources offices, procurement offices, personnel offices, physical security offices, senior agency information security officer, operations personnel, risk executive (function), appropriate privacy senior official or executive, and legal counsel. In addition, organizations may require external support from federal, provincial, territorial, municipal, and First Nations law enforcement agencies. There are specific requirements related to the disclosure of personal information to law enforcement; for details, contact the organization's privacy delegate.

Related controls and activities: None.

(08) **Incident handling: Correlation with external organizations**

Coordinate with [Assignment: organization-defined external organizations] to correlate and share [Assignment: organization-defined incident information] to achieve a cross-organizational perspective on incident awareness and more effective incident responses.

Discussion: The coordination of incident information with external organizations—including mission or business partners, military or coalition partners, customers, and developers—can provide significant benefits. Cross-organizational coordination can serve as an important risk management capability. This capability allows organizations to leverage information from a variety of sources to effectively respond to incidents and privacy breaches that could potentially affect the organization's operations, assets, and individuals. Care should be taken when collaboration requires the disclosure of personal information. Contact the organization's privacy delegate for details.

Related controls and activities: AU-16, PM-16.

(09) **Incident handling: Dynamic response capability**

Employ [Assignment: organization-defined dynamic response capabilities] to respond to incidents.

Discussion: The dynamic response capability addresses the timely deployment of new or replacement organizational capabilities in response to incidents. This includes capabilities implemented at the mission and business process level and at the system level.

Related controls and activities: None.

(10) **Incident handling: Supply chain coordination**

Coordinate incident handling activities involving supply chain events with other organizations involved in the supply chain.

Discussion: Organizations involved in supply chain activities include product developers, system integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Supply chain incidents can occur anywhere through or to the supply chain and include compromises or privacy breaches that involve primary or sub-tier providers, IT products, system components, development processes or personnel, and distribution processes or warehousing facilities. Organizations should include in their supply chain information exchange agreements processes for protecting and sharing incident information, and should consider their obligations for reporting incidents to government oversight bodies.

GC discussion: Federal departments and agencies should include in their supply chain information exchange agreements processes for protecting and sharing incident information, and should consider their obligations for reporting incidents to government oversight bodies (e.g., TBS, OPC).

Related controls and activities: CA-03, MA-02, SA-09, SR-08.

(11) **Incident handling: Integrated incident response team**

Establish and maintain an integrated incident response team that can be deployed to any location identified by the organization in [Assignment: organization-defined time period].

Discussion: An integrated incident response team is a team of experts that assesses, documents, and responds to incidents so that organizational systems and networks can recover quickly and implement the necessary controls to avoid future incidents. Incident response team personnel include forensic and malicious code analysts, tool developers, systems security architects or engineers and privacy practitioners, and real-time operations personnel. The incident handling capability includes performing rapid forensic preservation of evidence and analysis of and response to intrusions. For some organizations, the incident response team can be a cross-organizational entity.

An integrated incident response team facilitates information sharing and allows organizational personnel (e.g., developers, implementers, and operators) to leverage team knowledge of the threat and implement defensive measures that enable organizations to deter intrusions more effectively. Moreover, integrated teams promote the rapid detection of intrusions, the development of appropriate mitigations, and the deployment of effective defensive measures.

For example, when an intrusion is detected, the integrated team can rapidly develop an appropriate response for operators to implement, correlate the new incident with information on past intrusions, and augment ongoing cyber intelligence development.

Integrated incident response teams are better able to identify adversary tactics, techniques, and procedures that are linked to the operations tempo or specific mission and business functions and to define responsive actions in a way that does not disrupt those mission and business functions. Incident response teams can be distributed within organizations to make the capability resilient.

Related controls and activities: AT-03.

(12) **Incident handling: Malicious code and forensic analysis**

Analyze malicious code and/or other residual artifacts remaining in the system after the incident.

Discussion: When conducted carefully in an isolated environment, analyzing malicious code and other residual artifacts of a security incident or breach can give the organization insight into adversary tactics, techniques, and procedures. It can also indicate the identity or some defining characteristics of the adversary. In addition, malicious code analysis can help the organization develop responses to future incidents.

Related controls and activities: None.

(13) **Incident handling: Behaviour analysis**

Analyze anomalous or suspected adversarial behaviour in or related to [Assignment: organization-defined environments or resources].

Discussion: If the organization maintains a deception environment, an analysis of behaviours in that environment, including resources targeted by the adversary and timing of the incident or event, can provide insight into adversarial tactics, techniques, and procedures. External to a deception environment, the analysis of anomalous adversarial behaviour (e.g., changes in system performance or usage patterns) or suspected behaviour (e.g., changes in searches for the location of specific resources) can give the organization such insight. At times, an analysis of behavioural information may reveal information about an identifiable individual, and lawful authority and safeguards related to personal information should be considered.

Related controls and activities: None.

(14) **Incident handling: Security operations centre**

Establish and maintain a security operations centre.

Discussion: A security operations centre (SOC) is the focal point for security operations and computer network defence for an organization. The purpose of the SOC is to defend and monitor an organization's systems and

networks (i.e., cyber infrastructure) on an ongoing basis. The SOC is also responsible for detecting, analyzing, and responding to cyber security incidents in a timely manner.

The organization staffs the SOC with skilled technical and operational personnel (e.g., security analysts, incident response personnel, systems security engineers) and implements a combination of technical, management, and operational controls (including monitoring, scanning, and forensics tools) to monitor, fuse, correlate, analyze, and respond to threat and security-relevant event data from multiple sources. These sources include perimeter defences, network devices (e.g., routers, switches), and endpoint agent data feeds.

The SOC provides a holistic situational awareness capability to help organizations determine the security posture of the system and organization. A SOC capability can be obtained in a variety of ways. Larger organizations may implement a dedicated SOC while smaller organizations may employ third-party organizations to provide such a capability.

In the event that a security incident involves the compromise of personal information, SOC personnel should engage organizational privacy professionals. For organizations with significant holdings of personal information, consideration should be given to having regular privacy expertise represented in their SOC as part of their skilled technical and operational personnel.

Related controls and activities: None.

(15) **Incident handling: Public relations, reputation repair, and notification**

- a. Manage public relations associated with an incident
- b. Employ measures to repair the reputation of the organization
- c. If applicable, notify individuals whose personal information has been compromised

Discussion: It is important for an organization to have a strategy in place for addressing incidents that have been brought to the attention of the general public, have cast the organization in a negative light, have affected the organization's constituents (e.g., partners, customers), or have affected individuals whose personal information has been compromised. Such publicity can be extremely harmful to the organization and affect its ability to carry out its mission and business functions. Taking proactive steps to repair the organization's reputation is an essential aspect of re-establishing the trust and confidence of its constituents. Notifying these individuals enables them to take protective measures to prevent further harm from the compromised information.

Related controls and activities: None.

References:

- Directive for the Control of COMSEC Material in the Government of Canada (ITSD-03A) (upon request to the Cyber Centre)
- [TBS Directive on Security Management](#)
- [TBS Directive on Security Management, Appendix D: Mandatory Procedures for Business Continuity Management Control](#)
- [TBS Directive on Security Management, Appendix G: Mandatory Procedures for Security Event Management Control](#)
- [TBS Directive on Security Management, Appendix I: Standard on Security Event Reporting](#)
- [TBS Directive on Service and Digital, Appendix C: Mandatory Procedures for Privacy and Monitoring of Network and Device Use Information Notices](#)
- [TBS Policy on Privacy Protection](#)
- [TBS Directive on Privacy Practices](#)
- [OPC Contain a privacy breach at your business](#)
- [TBS Privacy Breach Management Toolkit](#)
- [TBS Directive on Privacy Practices, Appendix E: Standard on Privacy in Web Analytics](#)

- [TBS Government of Canada Cyber Security Event Management Plan \(GC CSEMP\)](#)
- [Developing your incident response plan \(ITSAP.40.003\)](#)
- [RCMP GCPSPG-003 Security Operations Centre Design Considerations Guide](#)

IR-05 Incident monitoring

Control: Track and document incidents.

Discussion: Documenting incidents includes maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, as well as evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources, including network monitoring, incident reports, incident response teams, user complaints, supply chain partners, audit monitoring, physical access monitoring, and user and administrator reports. IR-04 provides information on the types of incidents that are appropriate for monitoring.

Related controls and activities: AU-06, AU-07, IR-04, IR-06, IR-08, PE-06, PM-05, SC-05, SC-07, SI-03, SI-04, SI-07.

Enhancements:

(01) **Incident monitoring: Automated tracking, data collection, and analysis**

Track incidents and collect and analyze incident information using [Assignment: organization-defined automated mechanisms].

Discussion: Automated mechanisms for tracking incidents and collecting and analyzing incident information include computer incident response centres or other electronic databases of incidents and network monitoring devices. If the data collection requires the collection or creation of personal information, the organization should ensure it has the lawful authority for the collection and should limit the personal information to only the information required to effectively monitor.

Related controls and activities: None.

References:

- [TBS Directive on Security Management, Appendix D: Mandatory Procedures for Business Continuity Management Control](#)
- [TBS Directive on Security Management, Appendix G: Mandatory Procedures for Security Event Management Control](#)
- [Developing your incident response plan \(ITSAP.40.003\)](#)
- [TBS Government of Canada Cyber Security Event Management Plan \(GC CSEMP\)](#)

IR-06 Incident reporting

Control:

- A. Require personnel to report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period]
- B. Report incident information to [Assignment: organization-defined authorities]

Discussion: The types of incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable laws, jurisprudence, Orders in Council, directives, regulations, policies, standards, and guidelines. Incident information can inform risk assessments, control effectiveness assessments, security requirements for acquisitions, and selection criteria for technology products. The sharing or disclosure of personal information should be limited unless it is required for effective reporting.

Related controls and activities: CM-06, CP-02, IR-04, IR-05, IR-08, IR-09, SI-02.

Enhancements:

(01) Incident reporting: Automated reporting

Report incidents using [Assignment: organization-defined automated mechanisms].

Discussion: The recipients of incident reports are specified in IR-06B. Automated reporting mechanisms include email, posting on websites (with automatic updates), and automated incident response tools and programs.

Related controls and activities: IR-07.

(02) Incident reporting: Vulnerabilities related to incidents

Report system vulnerabilities associated with reported incidents to [Assignment: organization-defined personnel or roles].

Discussion: Reported incidents that uncover system vulnerabilities are analyzed by organizational personnel including system owners, mission and business owners, senior officials in the department's security governance, appropriate privacy senior officials or executives, authorizing officials, and the risk executive (function). The analysis can serve to prioritize and initiate mitigation actions to address the discovered system vulnerability.

Related controls and activities: None.

(03) Incident reporting: Supply chain coordination

Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.

Discussion: Organizations involved in supply chain activities include product developers, system integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Entities that provide supply chain governance include Public Services and Procurement Canada (PSPC). Supply chain incidents include compromises or breaches that involve IT products, system components, development processes or personnel, distribution processes, or warehousing facilities. Organizations should determine the appropriate information to share and should consider the value gained from informing external organizations about supply chain incidents, including the ability to improve processes or to identify the root cause of an incident.

Related controls and activities: SR-08.

References:

- Directive for the Control of COMSEC Material in the Government of Canada (ITSD-03A) (upon request to the Cyber Centre)
- [TBS Directive on Security Management, Appendix G: Mandatory Procedures for Security Event Management Control](#)
- [TBS Government of Canada Cyber Security Event Management Plan \(GC CSEMP\)](#)
- [TBS Significant Event Information Sharing Protocol](#) (restricted to GC)
- [TBS Policy on Privacy Protection](#)
- [TBS Directive on Privacy Practices](#)
- [TBS Privacy Breach Management Toolkit](#)
- [OPC Contain a privacy breach at your business](#)
-

IR-07 Incident response assistance

Control: Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.

Discussion: Incident response support resources provided by organizations include help desks, assistance groups, automated ticketing systems to open and track incident response tickets, and access to forensics services or consumer redress services, when required.

Related controls and activities: AT-02, AT-03, IR-04, IR-06, IR-08, PM-22, PM-26, SA-09, SI-18.

Enhancements:

(01) Incident response assistance: Automation support for availability of information and support

Increase the availability of incident response information and support using [Assignment: organization-defined automated mechanisms].

Discussion: Automated mechanisms can provide a push or pull capability for users to obtain incident response assistance. For example, individuals may have access to a website to query the assistance capability, or the assistance capability can proactively send incident response information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.

Related controls and activities: None.

(02) Incident response assistance: Coordination with external providers

- a. Establish a direct, cooperative relationship between the organization's incident response capability and external providers of a system protection capability
- b. Identify organizational incident response team members to the external providers

Discussion: External providers of a system protection capability include tools and services provided by the Cyber Centre. External providers may help to protect, monitor, analyze, detect, and respond to unauthorized activity within organizational information systems and networks. It may be beneficial to have agreements in place with external providers to clarify the roles and responsibilities of each party before an incident occurs.

GC discussion: It is recommended to have information sharing agreements, information sharing arrangements, or contracting documents in place with external providers to clarify the roles and responsibilities of each party before an incident occurs.

Related controls and activities: None.

References:

- [TBS Government of Canada Cyber Security Event Management Plan \(GC CSEMP\)](#)
- [Developing your incident response plan \(ITSAP.40.003\)](#)
- [TBS Policy on Privacy Protection](#)
- [TBS Directive on Privacy Practices](#)
- [OPC Contain a privacy breach at your business](#)
-
- [TBS Privacy Breach Management Toolkit](#)

IR-08 Incident response plan

Activity:

- A. Develop an incident response plan that
 1. provides the organization with a roadmap for implementing its incident response capability
 2. describes the structure and organization of the incident response capability
 3. provides a high-level approach for how the incident response capability fits into the overall organization
 4. meets the unique requirements of the organization which relate to mission, size, structure, and functions
 5. defines reportable incidents
 6. provides metrics for measuring the incident response capability within the organization
 7. defines the resources and management support needed to effectively maintain and mature an incident response capability

8. addresses the sharing of incident information
 9. is reviewed and approved by [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency]
 10. explicitly designates responsibility for incident response to [Assignment: organization-defined entities, personnel, or roles]
- B. Distribute copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]
 - C. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing
 - D. Communicate incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]
 - E. Protect the incident response plan from unauthorized disclosure and modification

Discussion: It is important that organizations develop and implement a coordinated approach to incident response. Organizational mission and business functions determine the structure of incident response capabilities. As part of the incident response capabilities, organizations consider the coordination and sharing of information with external organizations, including external service providers and other organizations involved in the supply chain. For incidents involving personal information (i.e., privacy breaches), include a process to determine whether notice to oversight organizations or affected individuals is appropriate and provide that notice accordingly.

Related controls and activities: AC-02, CP-02, CP-04, IR-04, IR-07, IR-09, PE-06, PL-02, SA-15, SI-02, SI-12, SR-08.

Enhancements:

(01) Incident response plan: Privacy breaches

For privacy breaches involving personal information, include the following in the incident response plan:

- a. a process to determine if notice to individuals or other organizations, including oversight organizations, is needed
- b. an assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms
- c. identification of applicable privacy requirements

Discussion: Organizations may be required by law, regulation, or policy to follow specific procedures relating to breaches, which include: notifying individuals, affected organizations, and oversight bodies; standards of harm; and mitigation or other specific requirements. Organizations subject to the PIPEDA are required to report breaches involving personal information posing a real risk of significant harm to the OPC. They also need to notify the individuals about the breaches and to keep records of the breaches.

GC discussion: In the event of a privacy breach under the *Privacy Act*, GC departments and agencies are responsible for meeting the requirements set out in Appendix B: Mandatory Procedures for Privacy Breaches of the TBS Directive on Privacy Practices. GC departments and agencies need to notify the individuals about the breaches and to keep records of the breaches.

Related controls and activities: PT-01, PT-02, PT-03, PT-04, PT-05, PT-07.

References:

- [TBS Policy on Privacy Protection](#)
- [TBS Directive on Privacy Practices](#)
- [TBS Directive on Privacy Practices, Appendix B: Mandatory Procedures for Privacy Breaches](#)
- [TBS Directive on Security Management, Appendix G: Mandatory Procedures for Security Event Management Control](#)
- [TBS Directive on Security Management, Appendix I: Standard on Security Event Reporting](#)

- [TBS Government of Canada Cyber Security Event Management Plan \(GC CSEMP\)](#)
- [Developing your incident response plan \(ITSAP.40.003\)](#)
- [Public Safety Canada, Developing an Operational Technology and Information Technology Incident Response Plan](#)
- [Breach of Security Safeguards Regulations SOR/2018-64](#)

IR-09 Information spillage response

Control: Respond to information spills by:

- assigning [Assignment: organization-defined personnel or roles] with responsibility for responding to information spills
- identifying the specific information involved in the system contamination
- alerting [Assignment: organization-defined personnel or roles] of the information spill using a method of communication not associated with the spill
- isolating the contaminated system or system component
- eradicating the information from the contaminated system or component
- identifying other systems or system components that may have been subsequently contaminated
- performing the following additional actions: [Assignment: organization-defined actions]

Discussion: Information spillage refers to instances where information is placed on systems that are not authorized to process such information. Information spills occur when information that is thought to be a certain classification or impact level is transmitted to a system and subsequently is determined to be of a higher classification or impact level. At that point, corrective action is required.

The nature of the response is based on the classification or impact level of the spilled information, the security capabilities of the system, the specific nature of the contaminated storage media, and the access authorizations of individuals with authorized access to the contaminated system.

The methods used to communicate information about the spill after the fact do not involve methods directly associated with the actual spill so as to minimize the risk of further spreading the contamination before such contamination is isolated and eradicated. In the event that information spillage involves personal information, officials should review the situation to assess whether a privacy breach has occurred, and the organization's privacy breach protocol should be followed, as specified in IR-08.

Related controls and activities: CP-02, IR-06, IR-08, PM-26, PM-27, PT-02, PT-03, PT-07, RA-07.

Enhancements:

(01) Information spillage response: Responsible personnel

Withdrawn: Incorporated into IR-09.

(02) Information spillage response: Training

Provide information spillage response training [Assignment: organization-defined frequency].

Discussion: Organizations establish requirements for responding to information spillage incidents in incident response plans. Incident response training on a regular basis helps to ensure that organizational personnel understand their individual responsibilities and what specific actions to take when spillage incidents occur.

Related controls and activities: AT-02, AT-03, CP-03, IR-02.

(03) Information spillage response: Post-spill operations

Implement the following procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions: [Assignment: organization-defined procedures].

Discussion: Corrective actions for systems contaminated due to information spillages may be time-consuming. Personnel may not have access to the contaminated systems while corrective actions are being taken, which may affect their ability to conduct organizational business.

Related controls and activities: None.

(04) **Information spillage response: Exposure to unauthorized personnel**

Employ the following controls for personnel exposed to information not within assigned access authorizations: [Assignment: organization-defined controls].

Discussion: Controls include ensuring that personnel who are exposed to spilled information are made aware of the laws, Orders in Council, directives, regulations, policies, standards, and guidelines regarding the information and the restrictions imposed based on exposure to such information.

Related controls and activities: None.

References:

- [Steps to address data spillage in the cloud \(ITSAP.50.112\)](#)

IR-10 Integrated information security analysis team

Withdrawn: Moved to IR-04(11).

Family: Maintenance

The controls and activities in the Maintenance (MA) family support periodic and timely maintenance on organizational systems and provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance to ensure its ongoing availability.

MA-01 Maintenance policy and procedures

Activity:

- A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]
 - 1. [Selection (1 or more): Organization-level; Mission/business process-level; System-level] maintenance policy that
 - a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
 - b. is consistent with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines
 - 2. procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls
- B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the maintenance policy and procedures
- C. Review and update the current maintenance
 - 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]
 - 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]

Discussion: Maintenance policy and procedures address the controls in the MA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of maintenance policy and procedures.

In general, security and privacy program policies and procedures at the organization level are preferable and may remove the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations.

Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.

Events that may precipitate an update to maintenance policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, jurisprudence, Orders in Council, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related controls and activities: PM-09, PS-08, SI-02, SI-12.

Enhancements: None.

References:

- [TBS Directive on Security Management](#)

- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [TBS Directive on Security Management, Appendix C: Mandatory Procedures for Physical Security Control](#)
- [TBS Policy on the Planning and Management of Investments](#)
- [TBS Directive on the Management of Material](#)

MA-02 Controlled maintenance

Control:

- Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements
- Approve and monitor all maintenance activities, whether performed onsite or remotely and whether the system or system components are serviced onsite or removed to another location
- Require that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the system or system components from organizational facilities for offsite maintenance, repair, or replacement
- Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for offsite maintenance, repair, or replacement: [Assignment: organization-defined information]
- Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions
- Include the following information in organizational maintenance records: [Assignment: organization-defined information]

Discussion: Controlling system maintenance addresses the information security aspects of the system maintenance program and applies to all types of maintenance to system components conducted by local or non-local entities. Maintenance includes peripherals such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes the date and time of maintenance, a description of the maintenance performed, names of the individuals or group performing the maintenance, name of the escort, and system components or equipment that are removed or replaced. Organizations should consider the supply chain-related risks associated with replacement components for systems.

Related controls and activities: CM-02, CM-03, CM-04, CM-05, CM-08, MA-04, MP-06, PE-16, SI-02, SR-03, SR-04, SR-11.

Enhancements:

(01) **Controlled maintenance: Record content**

Withdrawn: Incorporated into MA-02.

(02) **Controlled maintenance: Automated maintenance activities**

- Schedule, conduct, and document maintenance, repair, and replacement actions for the system using [Assignment: organization-defined automated mechanisms]
- Produce up-to-date, accurate, and complete records of all maintenance, repair, and replacement actions requested, scheduled, in process, and completed

Discussion: The use of automated mechanisms to manage and control system maintenance programs and activities helps to ensure the generation of timely, accurate, complete, and consistent maintenance records.

Related controls and activities: MA-03.

References: [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)

MA-03 Maintenance tools

Control:

- A. Approve, control, and monitor the use of system maintenance tools
- B. Review previously approved system maintenance tools [Assignment: organization-defined frequency]

Discussion: Approving, controlling, monitoring, and reviewing maintenance tools address security-related issues associated with maintenance tools that are not within system authorization boundaries and that are used specifically for diagnostic and repair actions on organizational systems. Organizations have flexibility in determining roles for the approval of maintenance tools and how that approval is documented.

A periodic review of maintenance tools facilitates the withdrawal of approval for outdated, unsupported, irrelevant, or no-longer-used tools. Maintenance tools can include hardware, software, and firmware items and may be pre-installed, brought in with maintenance personnel on media, cloud-based, or downloaded from a website. Such tools can be vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into systems. Maintenance tools can include hardware and software diagnostic test equipment and packet sniffers.

The hardware and software components that support maintenance and are a part of the system (including the software implementing utilities such as ping, ls, ipconfig, or the hardware and software implementing the monitoring port of an Ethernet switch) are not addressed by maintenance tools.

Related controls and activities: MA-02, PE-16, SA-400.

Enhancements:

(01) Maintenance tools: Inspect tools

Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.

Discussion: Maintenance tools can be directly brought into a facility by maintenance personnel or downloaded from a vendor's website. If, upon inspection of the maintenance tools, organizations determine that the tools have been modified in an improper manner or the tools contain malicious code, the incident is handled consistent with organizational policies and procedures for incident handling.

Related controls and activities: SI-07.

(02) Maintenance tools: Inspect media

Check media containing diagnostic and test programs for malicious code before the media is used in the system.

Discussion: If, upon inspection of media containing maintenance, diagnostic, and test programs, organizations determine that the media contains malicious code, the incident is handled consistent with organizational incident handling policies and procedures.

Related controls and activities: SI-03.

(03) Maintenance tools: Prevent unauthorized removal

Prevent the unauthorized removal of maintenance equipment containing organizational or personal information by:

- a. verifying that no organizational or personal information is contained on the equipment
- b. sanitizing or destroying the equipment
- c. retaining the equipment within the facility
- d. obtaining an exemption from [Assignment: organization-defined personnel or roles] explicitly authorizing removal of the equipment from the facility

Discussion: Organizational information includes all information owned by organizations and any information provided to organizations for which the organizations serve as information stewards.

Related controls and activities: MP-06.

(04) **Maintenance tools: Restricted tool use**

Restrict the use of maintenance tools to authorized personnel only.

Discussion: Restricting the use of maintenance tools to only authorized personnel applies to systems that are used to carry out maintenance functions.

Related controls and activities: AC-03, AC-05, AC-06.

(05) **Maintenance tools: Execution with privilege**

Monitor the use of maintenance tools that execute with increased privilege.

Discussion: Maintenance tools that execute with increased system privilege can result in unauthorized access to organizational information and assets that would otherwise be inaccessible.

Related controls and activities: AC-03, AC-06.

(06) **Maintenance tools: Software updates and patches**

Inspect maintenance tools to ensure the latest software updates and patches are installed.

Discussion: Maintenance tools using outdated and/or unpatched software can provide a threat vector for adversaries and result in a significant vulnerability for organizations.

Related controls and activities: AC-03, AC-06.

References: [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)

MA-04 Non-local maintenance

Control:

- A. Approve and monitor non-local maintenance and diagnostic activities
- B. Allow the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system
- C. Employ strong authentication in the establishment of non-local maintenance and diagnostic sessions
- D. Maintain records for non-local maintenance and diagnostic activities
- E. Terminate session and network connections when non-local maintenance is completed

Discussion: Non-local maintenance and diagnostic activities are conducted by individuals who communicate through either an external or internal network. Local maintenance and diagnostic activities are carried out by individuals who are physically present at the system location and not communicating across a network connection.

Authentication techniques used to establish non-local maintenance and diagnostic sessions reflect the network access requirements in IA-02. Strong authentication requires authenticators that are resistant to replay attacks and employ MFA. Strong authenticators include PKI where certificates are stored on a token protected by a password, passphrase, or biometric. Enforcing requirements in MA-04 is accomplished, in part, by other controls. The Cyber Centre publication User authentication guidance for information technology systems (ITSP.30.03) provides additional guidance on strong authentication and authenticators.

Related controls and activities: AC-02, AC-03, AC-06, AC-17, AC-17(400), AU-02, AU-03, IA-02, IA-04, IA-05, IA-08, MA-02, MA-05, PL-02, SA-400, SC-07, SC-10, SI-400.

Enhancements:

(01) **Non-local maintenance: Logging and review**

- a. Log [Assignment: organization-defined audit events] for non-local maintenance and diagnostic sessions
- b. Review the audit records of the maintenance and diagnostic sessions to detect anomalous behaviour

Discussion: Audit logging for non-local maintenance is enforced by AU-02. Audit events are defined in AU-02A.

Related controls and activities: AU-02, AU-06, AU-12.

(02) **Non-local maintenance: Document non-local maintenance**

Withdrawn: Incorporated into MA-01 and MA-04.

(03) **Non-local maintenance: Comparable security and sanitization**

- a. Require that non-local maintenance and diagnostic services be performed from a system that implements a security capability comparable to the capability implemented on the system being serviced
- b. Remove the component to be serviced from the system prior to non-local maintenance or diagnostic services; sanitize the component (for organizational information); and, after the service is performed, inspect and sanitize the component (for potentially malicious software) before reconnecting the component to the system

Discussion: Comparable security capability on systems, diagnostic tools, and equipment providing maintenance services implies that the implemented controls on those systems, tools, and equipment are at least as comprehensive as the controls on the system being serviced.

Related controls and activities: MP-06, SI-03, SI-07.

(04) **Non-local maintenance: Authentication and separation of maintenance sessions**

Protect non-local maintenance sessions by:

- a. employing [Assignment: organization-defined authenticators that are replay resistant]
- b. separating the maintenance sessions from other network sessions with the system by either
 - 1) physically separated communications paths
 - 2) logically separated communications paths

Discussion: Communications paths can be logically separated using encryption.

Related controls and activities: None.

(05) **Non-local maintenance: Approvals and notifications**

- a. Require the approval of each non-local maintenance session by [Assignment: organization-defined personnel or roles]
- b. Notify the following personnel or roles of the date and time of planned non-local maintenance: [Assignment: organization-defined personnel or roles].

Discussion: Notification may be performed by maintenance personnel. Approval of non-local maintenance is accomplished by personnel with sufficient information security and system knowledge to determine the appropriateness of the proposed maintenance.

Related controls and activities: None.

(06) **Non-local maintenance: Cryptographic protection**

Implement the following cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance and diagnostic communications: [Assignment: organization-defined cryptographic mechanisms].

Discussion: Failure to protect non-local maintenance and diagnostic communications can result in unauthorized individuals gaining access to organizational information. Unauthorized access during remote maintenance sessions

can result in a variety of hostile actions, including malicious code insertion, unauthorized changes to system parameters, and exfiltration of organizational information. Such actions can result in the loss or degradation of mission or business capabilities.

Related controls and activities: SC-08, SC-12, SC-13.

(07) **Non-local maintenance: Disconnect verification**

Verify session and network connection termination after the completion of non-local maintenance and diagnostic sessions.

Discussion: Verifying the termination of a connection once maintenance is completed ensures that connections established during non-local maintenance and diagnostic sessions have been terminated and are no longer available for use.

Related controls and activities: AC-12.

References:

- [User authentication guidance for information technology systems \(ITSP.30.031\)](#)
- [Identity, credential, and access management \(ICAM\) \(ITSAP.30.018\)](#)
- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)

MA-05 Maintenance personnel

Control:

- A. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel
- B. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations
- C. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations

Discussion: Maintenance personnel refers to individuals who perform hardware or software maintenance on organizational systems, while PE-02 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems. Technical competence of supervising individuals relates to the maintenance performed on the systems, while having required access authorizations refers to maintenance on and near the systems.

Individuals not previously identified as authorized maintenance personnel – such as information technology manufacturers, vendors, systems integrators, and consultants – may require privileged access to organizational systems, such as when they are required to conduct maintenance activities with little or no notice. Based on organizational assessments of risk, organizations may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for very limited time periods.

Information about maintenance personnel may be personal information and should be protected accordingly.

Related controls and activities: AC-02, AC-03, AC-05, AC-06, IA-02, IA-08, MA-04, MP-02, PE-02, PE-03, PS-07, RA-03, SA-400.

Enhancements:

(01) **Maintenance personnel: Individuals without appropriate access**

- a. Implement procedures for the use of maintenance personnel that lack appropriate security clearances, that include the following requirements

- 1) maintenance personnel who do not have the needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified
 - 2) prior to initiating maintenance or diagnostic activities by personnel who do not have the needed access authorizations, clearances, or formal access approvals, all volatile information storage components within the system are sanitized and all non-volatile storage media are removed or physically disconnected from the system and secured
- b. Develop and implement [Assignment: organization-defined alternate controls] in the event a system component cannot be sanitized, removed, or disconnected from the system

Discussion: Procedures for individuals who lack appropriate security clearances are intended to deny visual and electronic access to classified or protected information contained on organizational systems. Procedures for the use of maintenance personnel can be documented in security plans for the systems.

Related controls and activities: MP-06, PL-02.

(02) **Maintenance personnel: Security clearances for classified systems**

Verify that personnel performing maintenance and diagnostic activities on a system processing, storing, or transmitting classified information possess security clearances and formal access approvals for at least the highest classification level and for compartments of information on the system.

Discussion: Personnel who conduct maintenance on organizational systems may be exposed to classified information during the course of their maintenance activities. To mitigate the inherent risk of such exposure, organizations use maintenance personnel that are cleared (i.e., possess security clearances) to the classification level of the information stored on the system.

Related controls and activities: PS-03.

(03) **Maintenance personnel: Citizenship requirements for classified systems**

Verify that personnel performing maintenance and diagnostic activities on a system processing, storing, or transmitting classified information are Canadian citizens.

Discussion: Personnel who conduct maintenance on organizational systems may be exposed to classified information during the course of their maintenance activities. If access to classified information on organizational systems is restricted to Canadian citizens, the same restriction is applied to personnel performing maintenance on those systems.

Related controls and activities: PS-03.

(04) **Maintenance personnel: Foreign nationals**

Ensure that:

- a. foreign nationals with appropriate security clearances are used to conduct maintenance and diagnostic activities on classified systems only when the systems are jointly owned and operated by Canadian and foreign allied governments, or owned and operated solely by foreign allied governments
- b. approvals, consents, and detailed operational conditions regarding the use of foreign nationals to conduct maintenance and diagnostic activities on classified systems are fully documented within memoranda of agreement

Discussion: Personnel who conduct maintenance and diagnostic activities on organizational systems may be exposed to classified information. If non-Canadian citizens are permitted to perform maintenance and diagnostic activities on classified systems, then additional vetting is required to ensure agreements and restrictions are not being violated.

Related controls and activities: PS-03.

(05) **Maintenance personnel: Non-system maintenance**

Ensure that non-escorted personnel performing maintenance activities not directly associated with the system, but in the physical proximity of the system, have required access authorizations.

Discussion: Personnel who perform maintenance activities in other capacities not directly related to the system include physical plant personnel and custodial personnel.

Related controls and activities: None.

References: [PSPC Contract Security Manual, Chapter 6: Handling and safeguarding information and assets](#)

MA-06 Timely maintenance

Control: Obtain maintenance support and/or spare parts for [Assignment: organization-defined system components] within [Assignment: organization-defined time period] of failure.

Discussion: Organizations specify the system components that result in increased risk to organizational operations and assets, individuals, other organizations, or Canada when the functionality provided by those components is not operational. Organizational actions to obtain maintenance support include having appropriate contracts in place.

Related controls and activities: CM-08, CP-02, CP-07, RA-07, SA-15, SI-13, SR-02, SR-03, SR-04.

Enhancements:

(01) **Timely maintenance: Preventive maintenance**

Perform preventive maintenance on [Assignment: organization-defined system components] at [Assignment: organization-defined time intervals].

Discussion: Preventive maintenance includes proactive care and the servicing of system components to maintain organizational equipment and facilities in satisfactory operating condition. Such maintenance provides for the systematic inspection, tests, measurements, adjustments, parts replacement, detection, and correction of incipient failures either before they occur or before they develop into major defects.

The primary goal of preventive maintenance is to avoid or mitigate the consequences of equipment failures. Preventive maintenance is designed to preserve and restore equipment reliability by replacing worn components before they fail.

Methods of determining what preventive (or other) failure management policies to apply include: original equipment manufacturer recommendations; statistical failure records; expert opinion; maintenance that has already been conducted on similar equipment; requirements of codes, laws, or regulations within a jurisdiction; or measured values and performance indications.

Related controls and activities: None.

(02) **Timely maintenance: Predictive maintenance**

Perform predictive maintenance on [Assignment: organization-defined system components] at [Assignment: organization-defined time intervals].

Discussion: Predictive maintenance evaluates the condition of equipment by performing periodic or continuous (online) equipment condition monitoring. The goal of predictive maintenance is to perform maintenance at a scheduled time when the maintenance activity is most cost-effective and before the equipment loses performance within a threshold.

The predictive component of predictive maintenance stems from the objective of predicting the future trend of the equipment's condition. The predictive maintenance approach employs principles of statistical process control to

determine at what point in the future maintenance activities will be appropriate. Most predictive maintenance inspections are performed while equipment is in service, thus minimizing disruption of normal system operations. Predictive maintenance can result in substantial cost savings and higher system reliability.

Related controls and activities: None.

(03) **Timely maintenance: Automated support for predictive maintenance**

Transfer predictive maintenance data to a maintenance management system using [Assignment: organization-defined automated mechanisms].

Discussion: A computerized maintenance management system maintains a database of information about the maintenance operations of organizations and automates the processing of equipment condition data to trigger maintenance planning, execution, and reporting.

Related controls and activities: None.

References: None.

MA-07 Field maintenance

Control: Restrict or prohibit field maintenance on [Assignment: organization-defined systems or system components] to [Assignment: organization-defined trusted maintenance facilities].

Discussion: Field maintenance is the type of maintenance conducted on a system or system component after the system or component has been deployed to a specific site (i.e., an operational environment). In certain instances, field maintenance (i.e., local maintenance at the site) may not be executed with the same degree of rigour or with the same quality control checks as depot maintenance. For critical systems designated as such by the organization, it may be necessary to restrict or prohibit field maintenance at the local site and require that such maintenance be conducted in trusted facilities with additional controls.

Related controls and activities: MA-02, MA-04, MA-05.

Enhancements: None.

References: None.

Family: Media protection

The controls and activities in the Media protection (MP) family support the protection of system media throughout their lifecycle. They help limit access to information on system media to authorized users and sanitize or destroy system media before disposal or release for reuse.

MP-01 Media protection policy and procedures

Activity:

- A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]
 - 1. [Selection (1 or more): Organization-level; Mission/business process-level; System-level] media protection policy that
 - a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
 - b. is consistent with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines
 - 2. procedures to facilitate the implementation of the media protection policy and the associated media protection controls
- B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the media protection policy and procedures
- C. Review and update the current media protection
 - 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]
 - 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]

Discussion: Media protection policy and procedures address the controls in the MP family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of media protection policy and procedures.

In general, security and privacy program policies and procedures at the organization level are preferable and may remove the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations.

Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.

Events that may precipitate an update to media protection policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related controls and activities: PM-09, PS-08, SI-02, SI-12.

Enhancements: None.

References:

- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [TBS Directive on Security Management, Appendix C: Mandatory Procedures for Physical Security Control](#)
- [TBS Directive on Security Management, Appendix E: Mandatory Procedures for Information Management Security Control](#)
- [TBS Directive on Service and Digital, Appendix G: Standard on Enterprise Information Technology Service Common Configurations](#)
- Directive for the Control of COMSEC Material in the Government of Canada (ITSD-03A) (upon request to the Cyber Centre)

MP-02 Media access

Control: Restrict access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].

Discussion: System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), compact discs (CDs), and digital versatile discs (DVDs). Non-digital media includes paper and microfilm. An example of restricting access to non-digital media is denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers. An example of restricting access to digital media is limiting access to the design specifications stored on CDs in the media library to individuals on the system development team.

Related controls and activities: AC-19, AU-09, CP-02, CP-09, CP-10, MA-05, MP-04, MP-06, PE-02, PE-03, SC-12, SC-13, SC-34, SI-12.

Enhancements:

(01) Media access: Automated restricted access

Withdrawn: Incorporated into MP-04(02).

(02) Media access: Cryptographic protection

Withdrawn: Incorporated into SC-28(01).

References:

- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [TBS Directive on Security Management, Appendix C: Mandatory Procedures for Physical Security Control](#)
- [TBS Directive on Security Management, Appendix J: Standard on Security Categorization](#)
- [Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B information \(ITSP.40.111\)](#)

MP-03 Media marking

Control:

- Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information
- Exempt [Assignment: organization-defined types of system media] from marking if the media remain within [Assignment: organization-defined controlled areas]

Discussion: Security marking refers to the application or use of human-readable security attributes. Digital media includes diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), flash drives, CDs, and DVDs. Non-digital media includes paper and microfilm. Protected information is defined by TBS. The appropriate safeguarding and

dissemination requirements for protected and classified information is defined by the Cyber Centre and by PSPC Contract Security Program in Annex C, Chapter 6 of the Contract Security Manual. Security markings are generally not required for media that contains information determined by organizations to be in the public domain or to be publicly releasable. Some organizations may require markings for public information indicating that the information is publicly releasable. System media marking reflects applicable laws, Orders in Council, directives, policies, regulations, standards, and guidelines.

Related controls and activities: AC-16, CP-09, MP-05, PE-22, SA-400, SI-12.

Enhancements: None.

References:

- [TBS Directive on Security Management, Appendix C: Mandatory Procedures for Physical Security Control](#)
- [TBS Directive on Security Management, Appendix J: Standard on Security Categorization](#)
- [TBS Directive on Security Management, Appendix E: Mandatory Procedures for Information Management Security Control](#)
- [PSPC Contract Security Manual, Chapter 6: Handling and safeguarding information and assets](#)
- [PSPC Contract Security Manual, Annex C: Guidelines for safeguarding information and assets](#)
- [Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B information \(ITSP.40.111\)](#)
- [Security considerations for the use of removable media devices for Protected C and Classified Information \(ITSB-112\)](#)

MP-04 Media storage

Control:

- A. Physically control and securely store [Assignment: organization-defined types of digital and/or non-digital media] within [Assignment: organization-defined controlled areas]
- B. Protect system media types defined in MP-04A until the media are destroyed or sanitized using approved equipment, techniques, and procedures

Discussion: System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), CDs, and DVDs. Non-digital media includes paper and microfilm. Physically controlling stored media includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the library, and maintaining accountability for stored media. Secure storage includes a locked drawer, desk, or cabinet or a controlled media library.

The type of media storage is commensurate with the security category or classification of the information on the media. Controlled areas are spaces that provide physical and procedural controls to meet the requirements established for protecting information and systems. Fewer controls may be needed for media that contains information determined to be in the public domain, publicly releasable, or has limited adverse impacts on organizations, operations, or individuals if accessed by other than authorized personnel. In these situations, physical access controls provide adequate protection.

Related controls and activities: AC-19, CP-02, CP-06, CP-09, CP-10, MP-02, MP-07, PE-03, PL-02, SC-12, SC-13, SC-28, SC-34, SI-12.

Enhancements:

(01) **Media storage: Cryptographic protection**

Withdrawn: Incorporated into SC-28(01).

(02) **Media storage: Automated restricted access**

Restrict access to media storage areas and log access attempts and access granted using [Assignment: organization-defined automated mechanisms].

Discussion: Automated mechanisms include keypads, biometric readers, or card readers on the external entries to media storage areas.

Related controls and activities: AC-03, AU-02, AU-06, AU-09, AU-12, PE-03.

References:

- [RCMP GCPSP-001 Equipment Selection Guide for Paper Shredders](#)
- [IT media sanitization \(ITSP.40.006\)](#)
- [RCMP G13-01 Secure Storage Room Guide](#)
- [RCMP G13-02 Secure Demising Wall Guide](#)
- [TBS Directive on Service and Digital, Appendix G: Standard on Enterprise Information Technology Service Common Configurations](#)
- [Security considerations for the use of removable media devices for Protected C and Classified Information \(ITSB-112\)](#)

MP-05 Media transport

Control:

- A. Protect and control [Assignment: organization-defined types of system media] during transport outside of controlled areas using [Assignment: organization-defined controls]
- B. Maintain accountability for system media during transport outside of controlled areas
- C. Document activities associated with the transport of system media
- D. Restrict the activities associated with the transport of system media to authorized personnel

Discussion: System media includes digital and non-digital media. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state and magnetic), CDs, and DVDs. Non-digital media includes microfilm and paper. Controlled areas are spaces for which organizations provide physical or procedural controls to meet requirements established for protecting information and systems. Controls to protect media during transport include cryptography and locked containers.

Cryptographic mechanisms can provide confidentiality and integrity protections depending on the mechanisms implemented. Activities associated with media transport include releasing media for transport, ensuring that media enters the appropriate transport processes, and the actual transport.

Authorized transport and courier personnel may include individuals external to the organization. Maintaining accountability of media during transport includes restricting transport activities to authorized personnel and tracking and/or obtaining records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering.

Organizations should establish documentation requirements for activities associated with the transport of system media in accordance with organizational assessments of risk. Organizations maintain the flexibility to define record-keeping methods for the different types of media transport as part of a system of transport-related records.

Related controls and activities: AC-07, AC-19, CP-02, CP-09, MP-03, MP-04, PE-16, PL-02, SC-12, SC-13, SC-28, SC-34.

Enhancements:

(01) **Media transport: Protection outside of controlled areas**

Withdrawn: Incorporated into MP-05.

(02) **Media transport: Documentation of activities**

Withdrawn: Incorporated into MP-05.

(03) Media transport: Custodians

Employ an identified custodian during transport of system media outside of controlled areas.

Discussion: Identified custodians provide organizations with specific points of contact during the media transport process and facilitate individual accountability. Custodial responsibilities can be transferred from one individual to another if an unambiguous custodian is identified.

Related controls and activities: None.

(04) Media transport: Cryptographic protection

Withdrawn: Incorporated into SC-28(01).

References:

- [TBS Directive on Security Management, Appendix C: Mandatory Procedures for Physical Security Control](#)
- [TBS Directive on Service and Digital, Appendix G: Standard on Enterprise Information Technology Service Common Configurations](#)
- [RCMP GCPSG-007 Transport, Transmittal and Storage of Protected and Classified Material](#) (restricted to GC)
- [Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B information \(ITSP.40.111\)](#)
- Directive for the Control of COMSEC Material in the Government of Canada (ITSD-03A) (upon request to the Cyber Centre)

MP-06 Media sanitization**Control:**

- Sanitize [Assignment: organization-defined system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures]
- Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information

Discussion: Media sanitization applies to all digital and non-digital system media subject to disposal or reuse, whether the media is considered removable or not. Examples include digital media in scanners, copiers, printers, notebook computers, workstations, network components, mobile devices, and non-digital media (e.g., paper and microfilm). The sanitization process removes information from system media such that the information cannot be retrieved or reconstructed.

Sanitization techniques—including clearing, purging, cryptographic erase, de-identification of personal information, and destruction—prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods, recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Organizations use discretion on the employment of approved sanitization techniques and procedures for media that contains information deemed to be in the public domain or publicly releasable or information deemed to have no adverse impact on organizations or individuals if released for reuse or disposal.

Sanitization of non-digital media includes destruction, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing them from the document.

GC discussion: The sanitization requirements for protected and classified information are set by Cyber Centre- and RCMP-endorsed standards. Organizations can refer to the Cyber Centre guidance IT media sanitization (ITSP.40.006) and to the RCMP's Security Equipment Guide.

Related controls and activities : AC-03, AC-07, AU-11, MA-02, MA-03, MA-04, MA-05, PM-22, SA-400, SI-12, SI-18, SI-19, SR-11.

Enhancements:

(01) Media sanitization: Review, approve, track, document, and verify

Review, approve, track, document, and verify media sanitization and disposal actions.

Discussion: Organizations review and approve media to be sanitized to ensure compliance with records retention policies. Tracking and documenting actions include listing personnel who reviewed and approved sanitization and disposal actions, types of media sanitized, files stored on the media, sanitization methods used, date and time of the sanitization actions, personnel who performed the sanitization, verification actions taken and personnel who performed the verification, and the disposal actions taken. Organizations should verify that the sanitization of the media was effective prior to disposal.

Related controls and activities: None.

(02) Media sanitization: Equipment testing

Test sanitization equipment and procedures [Assignment: organization-defined frequency] to ensure that the intended sanitization is being achieved.

Discussion: Testing of sanitization equipment and procedures may be conducted by qualified and authorized external entities, including federal departments or agencies or external service providers.

Related controls and activities: None.

(03) Media sanitization: Non-destructive techniques

Apply non-destructive sanitization techniques to portable storage devices prior to connecting such devices to the system under the following circumstances: [Assignment: organization-defined circumstances requiring sanitization of portable storage devices].

Discussion: Portable storage devices include external or removable hard disk drives (e.g., solid state, magnetic), optical discs, magnetic or optical tapes, flash memory devices, flash memory cards, and other external or removable disks. Portable storage devices can be obtained from untrustworthy sources and may contain malicious code that can be inserted into or transferred to organizational systems through USB ports or other entry portals.

While scanning storage devices is recommended, sanitization provides additional assurance that such devices are free of malicious code. Organizations should consider non-destructive sanitization of portable storage devices when the devices are purchased from manufacturers or vendors prior to initial use or when organizations cannot maintain a positive chain of custody for the devices.

Related controls and activities: None.

(04) Media sanitization: Protected information

Withdrawn: Incorporated into MP-06.

(05) Media sanitization: Classified information

Withdrawn: Incorporated into MP-06.

(06) Media sanitization: Media destruction

Withdrawn: Incorporated into MP-06.

(07) Media sanitization: Dual authorization

Enforce dual authorization for the sanitization of [Assignment: organization-defined system media].

Discussion: Organizations employ dual authorization to help ensure that system media sanitization cannot occur unless 2 technically qualified individuals conduct the designated task. Individuals who sanitize system media possess sufficient skills and expertise to determine if the proposed sanitization reflects applicable federal and organizational standards, policies, and procedures. Dual authorization also helps to ensure that sanitization occurs as intended, protecting against errors and false claims of having performed the sanitization actions. Dual

authorization may also be known as two-person control. To reduce the risk of collusion, organizations should consider rotating dual authorization duties to other individuals.

Related controls and activities: AC-03, MP-02.

(08) **Media sanitization: Remote purging or wiping of information**

Provide the capability to purge or wipe information from [Assignment: organization-defined systems or system components] [Selection (1): remotely; under the following conditions: [Assignment: organization-defined conditions]].

Discussion: Remote purging or wiping of information protects information on organizational systems and system components if systems or components are obtained by unauthorized individuals. Remote purge or wipe commands require strong authentication to help mitigate the risk of unauthorized individuals purging or wiping the system, component, or device. The purge or wipe function can be implemented in a variety of ways, including by overwriting data or information multiple times or by destroying the key necessary to decrypt encrypted data.

Related controls and activities: None.

References:

- [IT media sanitization \(ITSP.40.006\)](#)
- [RCMP G1-001 Security Equipment Guide](#) (restricted to GC)
- [RCMP GCPSP-001 Equipment Selection Guide for Paper Shredders](#)
- [TBS Directive on Service and Digital, Appendix G: Standard on Enterprise Information Technology Service Common Configurations](#)
- Directive for the Control of COMSEC Material in the Government of Canada (ITSD-03A) (upon request to the Cyber Centre)

MP-07 Media use

Control:

- [Selection (1): Restrict; Prohibit] the use of [Assignment: organization-defined types of system media] on [Assignment: organization-defined systems or system components] using [Assignment: organization-defined controls]
- Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner

Discussion: System media includes both digital and non-digital media. Digital media includes diskettes, magnetic tapes, flash drives, CDs, DVDs, and removable hard disk drives. Non-digital media includes paper and microfilm. Media use protections also apply to mobile devices with information storage capabilities. In contrast to MP-02, which restricts user access to media, MP-07 restricts the use of certain types of media on systems, for example, restricting or prohibiting the use of flash drives or external hard disk drives.

Organizations use technical and non-technical controls to restrict the use of system media. Organizations may restrict the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports or disabling or removing the ability to insert, read, or write to such devices. Organizations may also limit the use of portable storage devices to only approved devices, including devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned.

Finally, organizations may restrict the use of portable storage devices based on the type of device, such as by prohibiting the use of writeable, portable storage devices and implementing this restriction by disabling or removing the capability to write to such devices. Requiring identifiable owners for storage devices reduces the risk of using such devices by allowing organizations to assign responsibility for addressing known vulnerabilities in the devices.

Related controls and activities: AC-19, AC-20, PL-04, PM-12, SC-34, SC-41.

Enhancements:**(01) Media use: Prohibit use without owner**

Withdrawn: Incorporated into MP-07.

(02) Media use: Prohibit use of sanitization-resistant media

Prohibit the use of sanitization-resistant media in organizational systems.

Discussion: Sanitization resistance refers to how resistant media are to non-destructive sanitization techniques with respect to the capability to purge information from media. Certain types of media do not support sanitization commands or, if supported, the interfaces are not supported in a standardized way across these devices. Sanitization-resistant media includes compact flash, embedded flash on boards and devices, solid state drives, and USB removable media.

Related controls and activities: MP-06.

References:

- [TBS Directive on Service and Digital, Appendix G: Standard on Enterprise Information Technology Service Common Configurations](#)

MP-08 Media downgrading

Control:

- Establish [Assignment: organization-defined system media downgrading process] that includes employing downgrading mechanisms with strength and integrity commensurate with the security category or classification of the information
- Verify that the system media downgrading process is commensurate with the security category and/or classification level of the information to be removed and the access authorizations of the potential recipients of the downgraded information
- Identify [Assignment: organization-defined system media requiring downgrading]
- Downgrade the identified system media using the established process

Discussion: Media downgrading applies to digital and non-digital media subject to release outside of the organization, whether the media is considered removable or not. When applied to system media, the downgrading process removes information from the media, typically by security category or classification level, such that the information cannot be retrieved or reconstructed. Downgrading of media includes redacting information to enable wider release and distribution. Downgrading ensures that empty space on the media is devoid of information.

Related controls and activities: SA-400.

Enhancements:**(01) Media downgrading: Documentation of process**

Document system media downgrading actions.

Discussion: Organizations can document the media downgrading process by providing information, such as the downgrading technique employed, the identification number of the downgraded media, and the identity of the individual that authorized and/or performed the downgrading action.

Related controls and activities: None.

(02) Media downgrading: Equipment testing

Test downgrading equipment and procedures [Assignment: organization-defined frequency] to ensure that downgrading actions are being achieved.

Discussion: None.

Related controls and activities: None.

(03) **Media downgrading: Protected information**

Downgrade system media containing protected information prior to public release.

Discussion: None.

GC discussion: The downgrading of protected information uses approved sanitization tools, techniques, and procedures.

Related controls and activities: None.

(04) **Media downgrading: Classified information**

Downgrade system media containing classified information prior to release to individuals without required access authorizations.

Discussion: None.

GC discussion: Downgrading of classified information uses approved sanitization tools, techniques, and procedures to transfer information confirmed to be unclassified from classified systems to unclassified media.

Related controls and activities: None.

References:

- [TBS Directive on Service and Digital, Appendix G: Standard on Enterprise Information Technology Service Common Configurations](#)
- [IT media sanitization \(ITSP.40.006\)](#)

Family: Physical and environmental protection

The controls and activities in the Physical and environmental protection (PE) family support the control of physical access to systems, equipment, and the respective operating environments to authorized individuals. They enable the protection of the physical plant and support infrastructure for systems, and the protection of systems against environmental hazards and provide appropriate environmental controls in facilities containing systems.

PE-01 Physical and environmental protection policy and procedures

Activity:

- A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]
 - 1. [Selection (1 or more): Organization-level; Mission/business process-level; System-level] physical and environmental protection policy that
 - a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
 - b. is consistent with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines
 - 2. procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls
- B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures
- C. Review and update the current physical and environmental protection
 - 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]
 - 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]

Discussion: Physical and environmental protection policy and procedures address the controls in the PE family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of physical and environmental protection policy and procedures.

In general, security and privacy program policies and procedures at the organization level are preferable and may remove the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations.

Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.

Events that may precipitate an update to physical and environmental protection policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related controls and activities: AT-03, PM-09, PS-08, SI-02, SI-12.

Enhancements: None.

References:

- [TBS Directive on Security Management, Appendix C: Mandatory Procedures for Physical Security Control](#)
- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [RCMP GCPSPG-006 Access Management Guide](#) (restricted to GC)

PE-02 Physical access authorizations

Control:

- Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides
- Issue authorization credentials for facility access
- Review the access list detailing authorized facility access by individuals [Assignment: organization-defined frequency]
- Remove individuals from the facility access list when access is no longer required

Discussion: Physical access authorizations apply to employees and visitors. Individuals with permanent physical access authorization credentials are not considered visitors. Authorization credentials include identification badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed consistent with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines. Physical access authorizations may not be necessary to access certain areas within facilities that are designated as publicly accessible.

Related controls and activities: AT-03, AU-09, IA-04, MA-05, MP-02, PE-03, PE-04, PE-05, PE-08, PM-12, PS-03, PS-04, PS-05, PS-06.

Enhancements:

(01) Physical access authorizations: Access by position or role

Authorize physical access to the facility where the system resides based on position or role.

Discussion: Role-based facility access includes access by authorized permanent and regular/routine maintenance personnel, duty officers, and emergency medical staff.

Related controls and activities: AC-02, AC-03, AC-06.

(02) Physical access authorizations: Two forms of identification

Require 2 forms of identification from the following forms of identification for visitor access to the facility where the system resides: [Assignment: organization-defined list of acceptable forms of identification].

Discussion: Examples of acceptable forms of identification include passports, federal, provincial, or territorial issued identification cards, and military identification cards. To gain access to facilities using automated mechanisms, organizations may use radio frequency identification (RFID) key cards, PINs, and biometrics. Organizations should recognize that these forms of identification are considered personal information and should be protected accordingly.

Related controls and activities: IA-02, IA-04, IA-05.

(03) Physical access authorizations: Restrict unescorted access

Restrict unescorted access to the facility where the system resides to personnel with [Selection (1 or more): security clearances for all information contained within the system; formal access authorizations for all information contained within the system; need for access to all information contained within the system; [Assignment: organization-defined physical access authorizations]].

Discussion: Individuals without required security clearances, access approvals, or need to know are escorted by individuals with appropriate physical access authorizations to ensure that information is not exposed or otherwise compromised.

Related controls and activities: PS-02, PS-06.

(400) **Physical access authorizations: Identification card requirements**

Ensure identification cards meet requirements prior to issuance.

Discussion: None.

GC discussion: The organization issues an identification card to all personnel, which as a minimum includes the name of the organization, the bearer's name and photo, a unique card number, and an expiry date. Identification cards may contain personal information and should be protected accordingly.

Related controls and activities: None.

References:

- [TBS Directive on Security Management, Appendix C: Mandatory Procedures for Physical Security Control](#)
- Directive for the Control of COMSEC Material in the Government of Canada (ITSD-03A) (upon request to the Cyber Centre)
- [RCMP GCPSPG-006 Access Management Guide](#) (restricted to GC)
- [TBS Policy on Privacy Protection](#)
- [TBS Directive on Privacy Practices](#)
- [RCMP GCPSPG-005 Security Inspections Guide](#) (restricted to GC)
- [RCMP G1-005 Preparation of Physical Security Briefs](#)
- [PSPC Contract Security Manual, Chapter 5: Facility protection](#)
- [PSPC Contract Security Manual, Annex B: Guidelines for facility protection](#)
- [Privacy Act](#)

PE-03 Physical access control

Control:

- A. Enforce physical access authorizations at [Assignment: organization-defined entry and exit points to the facility where the system resides] by
 1. verifying individual access authorizations before granting access to the facility
 2. controlling ingress and egress to the facility using [Selection (1 or more): [Assignment: organization-defined physical access control systems or devices]; guards]
- B. Maintain physical access audit logs for [Assignment: organization-defined entry or exit points]
- C. Control access to areas within the facility designated as publicly accessible by implementing the following controls: [Assignment: organization-defined physical access controls]
- D. Escort visitors and control visitor activity [Assignment: organization-defined circumstances requiring visitor escorts and control of visitor activity]
- E. Secure keys, access cards, combinations, safes, cipher locks, and other physical access devices
- F. Inventory [Assignment: organization-defined physical access devices] every [Assignment: organization-defined frequency]

- G. Change combinations and keys [Assignment: organization-defined frequency] and/or when keys are lost, or combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated
- AA. Remove the access card identifier from the access list or database [Assignment: organization-defined frequency] when the access card is lost, misplaced, stolen, or when the individual possessing the card is transferred or terminated

Discussion: Physical access control applies to employees and visitors. Individuals with permanent physical access authorizations are not considered visitors. Physical access controls for publicly accessible areas may include physical access control logs/records, guards, or physical access devices and barriers to prevent movement from publicly accessible areas to non-public areas. Organizations determine the types of guards needed, including professional security staff, system users, or administrative staff. Physical access devices include keys, locks, combinations, biometric readers, and card readers.

Physical access control systems comply with applicable laws, Orders in Council, directives, policies, regulations, standards, and guidelines. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural, automated, or some combination thereof. Physical access points can include facility access points, interior access points to systems that require supplemental access controls, or both. Components of systems may be in areas designated as publicly accessible with organizations controlling access to the components.

Related controls and activities: AT-03, AU-02, AU-06, AU-09, AU-13, CP-10, IA-03, IA-08, MA-05, MP-02, MP-04, PE-02, PE-04, PE-05, PE-08, PS-02, PS-03, PS-06, PS-07, RA-03, SC-28, SI-04, SR-03.

Enhancements:

(01) Physical access control: System access

Enforce physical access authorizations to the system in addition to the physical access controls for the facility at [Assignment: organization-defined physical spaces containing one or more components of the system].

Discussion: Control of physical access to the system provides additional physical security for those areas within facilities where there is a concentration of system components.

Related controls and activities: None.

(02) Physical access control: Facility and systems

Perform security checks [Assignment: organization-defined frequency] at the physical perimeter of the facility or system for exfiltration of information or removal of system components.

Discussion: Organizations determine the extent, frequency, and/or randomness of security checks to adequately mitigate risk associated with exfiltration.

Related controls and activities: AC-04, SC-07.

(03) Physical access control: Continuous guards

Employ guards to control [Assignment: organization-defined physical access points] to the facility where the system resides 24 hours per day, 7 days per week.

Discussion: Employing guards at selected physical access points to the facility provides a more rapid response capability for organizations. Guards also provide the opportunity for human surveillance in areas of the facility not covered by video surveillance.

Related controls and activities: CP-06, CP-07, PE-06.

(04) Physical access control: Lockable casings

Use lockable physical casings to protect [Assignment: organization-defined system components] from unauthorized physical access.

Discussion: The greatest risk from the use of portable devices—such as smart phones, tablets, and notebook computers—is theft. Organizations can employ lockable, physical casings to reduce or eliminate the risk of equipment theft or tampering. Such casings come in a variety of sizes, from units that protect a single notebook computer to full cabinets that can protect multiple servers, computers, and peripherals. Lockable physical casings can be used in conjunction with cable locks or lockdown plates to prevent the theft of the locked casing containing the computer equipment.

Related controls and activities: None.

(05) **Physical access control: Tamper protection**

Employ [Assignment: organization-defined anti-tamper technologies] to [Selection (1 or more): detect; prevent] physical tampering or alteration of [Assignment: organization-defined hardware components] within the system.

Discussion: Organizations can implement tamper detection and prevention in selected hardware components or implement tamper detection in some components and tamper prevention in other components. Detection and prevention activities can employ many types of anti-tamper technologies, including tamper-detection seals and anti-tamper coatings. Anti-tamper programs help to detect hardware alterations through counterfeiting and other supply chain-related risks.

Related controls and activities: SA-16, SR-09, SR-11.

(06) **Physical access control: Facility penetration testing**

Withdrawn: Incorporated into CA-08.

(07) **Physical access control: Physical barriers**

Limit access using physical barriers.

Discussion: Physical barriers include bollards, concrete slabs, jersey walls, and hydraulic active vehicle barriers.

Related controls and activities: None.

(08) **Physical access control: Access control vestibules**

Employ access control vestibules at [Assignment: organization-defined locations within the facility].

Discussion: An access control vestibule is part of a physical access control system that typically provides a space between 2 sets of interlocking doors. Vestibules are designed to prevent unauthorized individuals from following authorized individuals into facilities with controlled access. This activity, also known as piggybacking or tailgating, results in unauthorized access to the facility. Interlocking door controllers can be used to limit the number of individuals who enter controlled access points and to provide containment areas while authorization for physical access is verified.

Interlocking door controllers can be fully automated (i.e., controlling the opening and closing of the doors) or partially automated (i.e., using security guards to control the number of individuals entering the containment area).

Related controls and activities: None.

(400) **Physical access control: Security inspections**

Conduct security inspections in facilities where sensitive or valuable information or assets are handled or stored, or in facilities supporting critical services or activities.

Discussion: None.

GC discussion: Security inspections are conducted to verify compliance with departmental security practices. They must be conducted by authorized personnel and in accordance with defined processes and timelines. In emergency

or heightened threat situations, the frequency or depth of security inspections is increased to achieve a higher readiness level. Non-compliance shall be reported in accordance with defined processes to enable the implementation of corrective actions and, when applicable, to report to the responsible authorities.

Related controls and activities: None.

References:

- [PSPC Contract Security Manual](#)
- [TBS Directive on Security Management, Appendix C: Mandatory Procedures for Physical Security Control](#)
- [National Building Code of Canada 2020](#)
- [National Fire Code of Canada 2020](#)
- Directive for the control of COMSEC material in the Government of Canada (ITSD-03A) (upon request to the Cyber Centre)
- [RCMP GCPSPG-007 Transport, Transmittal and Storage of Protected and Classified Material](#) (restricted to GC)
- [RCMP GCPSPG-010 Operational Physical Security Guide](#) (restricted to GC)
- [RCMP GCPSPG-006 Access Management Guide](#) (restricted to GC)
- [RCMP G1-005 Preparation of Physical Security Briefs](#)
- [RCMP G13-01 Secure Storage Room Guide](#)
- [RCMP G13-02 Secure Demising Wall Guide](#)
- [RCMP G1-031 Physical Protection of Computer Servers](#)
- [PSPC Contract Security Manual, Chapter 5: Facility protection](#)
- [PSPC Contract Security Manual, Annex B: Guidelines for facility protection](#)
- [PSPC Contract Security Manual, Annex D: Information technology security inspection process](#)

PE-04 Access control for transmission

Control: Control physical access to [Assignment: organization-defined system distribution and transmission lines] within organizational facilities using [Assignment: organization-defined security controls].

Discussion: Security controls applied to system distribution and transmission lines prevent accidental damage, disruption, and physical tampering. Such controls may also be necessary to prevent eavesdropping or modification of unencrypted transmissions. Security controls used to control physical access to system distribution and transmission lines include disconnected or locked spare jacks, locked wiring closets, protection of cabling by conduit or cable trays, and wiretapping sensors.

Related controls and activities: AT-03, IA-04, MP-02, MP-04, PE-02, PE-03, PE-05, PE-09, SC-07, SC-08.

Enhancements: None.

References: [RCMP GCPSPG-006 Access Management Guide](#) (restricted to GC)

PE-05 Access control for output devices

Control: Control physical access to output from [Assignment: organization-defined output devices] to prevent unauthorized individuals from obtaining the output.

Discussion: Controlling physical access to output devices includes placing output devices in locked rooms or other secured areas with keypad or card reader access controls and allowing access to authorized individuals only, placing output devices in locations that can be monitored by personnel, installing monitor or screen filters, and using headphones. Examples of output devices include monitors, printers, scanners, audio devices, facsimile machines, and copiers.

Related controls and activities: PE-02, PE-03, PE-04, PE-18.

Enhancements:**(01) Access control for output devices: Access to output by authorized individuals**

Withdrawn: Incorporated into PE-05.

(02) Access control for output devices: Link to individual identity

Link individual identity to receipt of output from output devices.

Discussion: Methods for linking individual identity to the receipt of output from output devices include installing security functionality on facsimile machines, copiers, and printers. Such functionality allows organizations to implement authentication on output devices prior to the release of output to individuals.

Related controls and activities: None.

(03) Access control for output devices: Marking output devices

Withdrawn: Incorporated into PE-22.

References: RCMP [GCPSPG-015 Guide to the Application of Physical Security Zones](#) (restricted to GC)

PE-06 Monitoring physical access

Control:

- A. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents
- B. Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events]
- C. Coordinate results of reviews and investigations with the organizational incident response capability

Discussion: Physical access monitoring includes publicly accessible areas within organizational facilities. Examples of physical access monitoring include employing guards, video surveillance equipment (i.e., cameras), and sensor devices. Reviewing physical access logs can help identify suspicious activity, anomalous events, or potential threats. The reviews can be supported by audit logging controls, such as AU-02, if the access logs are part of an automated system. Organizational incident response capabilities include investigations of physical security incidents and responses to the incidents. Incidents include security violations or suspicious physical access activities. Suspicious physical access activities include accesses outside of normal work hours, repeated accesses to areas not normally accessed, accesses for unusual lengths of time, and out-of-sequence accesses.

Related controls and activities: AU-02, AU-06, AU-09, AU-12, CA-07, CP-10, IR-04, IR-08.

Enhancements:**(01) Monitoring physical access: Intrusion alarms and surveillance equipment**

Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.

Discussion: Physical intrusion alarms can be employed to alert security personnel when unauthorized access to the facility is attempted. Alarm systems work in conjunction with physical barriers, physical access control systems, and security guards by triggering a response when these other forms of security have been compromised or breached.

Physical intrusion alarms can include different types of sensor devices, such as motion sensors, contact sensors, and broken glass sensors. Surveillance equipment includes video cameras installed at strategic locations throughout the facility. In the event that surveillance videos are recorded, this may constitute personal information and should be protected appropriately.

Related controls and activities: None.

(02) Monitoring physical access: Automated intrusion recognition and response

Recognize [Assignment: organization-defined classes or types of intrusions] and initiate [Assignment: organization-defined response actions] using [Assignment: organization-defined automated mechanisms].

Discussion: Response actions can include notifying selected organizational personnel or law enforcement personnel. Automated mechanisms implemented to initiate response actions include system alert notifications, email and text messages, and activating door locking mechanisms. Physical access monitoring can be coordinated with intrusion detection systems and system monitoring capabilities to provide integrated threat coverage for the organization. Care should be taken to ensure the least amount of personal information is both collected and communicated for intrusion recognition and response.

Related controls and activities: SI-04.

(03) Monitoring physical access: Video surveillance

- a. Employ video surveillance of [Assignment: organization-defined operational areas]
- b. Review video recordings [Assignment: organization-defined frequency]
- c. Retain video recordings for [Assignment: organization-defined time period]

Discussion: Video surveillance focuses on recording activity in specified areas for the purposes of subsequent review, if circumstances so warrant. Video recordings are typically reviewed to detect anomalous events or incidents. Monitoring the surveillance video is not required, although organizations may choose to do so. A threat and risk assessment (TRA) will assist in determining specifics of video retention, storage, use, or release. Prior to installing closed circuit TV or video equipment (CCTV/CCVE), research into local laws and regulations should be considered. Video recordings may collect and store personal information and should be protected appropriately.

Related controls and activities: None.

(04) Monitoring physical access: Monitoring physical access to systems

Monitor physical access to the system in addition to the physical access monitoring of the facility at [Assignment: organization-defined physical spaces containing one or more components of the system].

Discussion: Monitoring physical access to systems provides additional monitoring for those areas within facilities where there is a concentration of system components, including server rooms, media storage areas, and communications centres. Physical access monitoring can be coordinated with intrusion detection systems and system monitoring capabilities to provide comprehensive and integrated threat coverage for the organization.

Related controls and activities: None.

References:

- [RCMP GCPSPG-006 Access Management Guide](#) (restricted to GC)
- [RCMP GCPSPG-010 Operational Physical Security Guide](#) (restricted to GC)
- [RCMP GCPSPG-019 Protection, Detection, Response, and Recovery Guide](#) (restricted to GC)
- [TBS Directive on Security Management, Appendix C: Mandatory Procedures for Physical Security Control](#)
- [Privacy Act](#)
- [TBS Policy on Privacy Protection](#)
- [TBS Directive on Privacy Practices](#)

PE-07 Visitor control

Withdrawn: Incorporated into PE-02 and PE-03.

PE-08 Visitor access records

Control:

- A. Maintain visitor access records to the facility where the system resides for [Assignment: organization-defined time period].
- B. Review visitor access records [Assignment: organization-defined frequency].
- C. Report anomalies in visitor access records to [Assignment: organization-defined personnel].

Discussion: Visitor access records include the names and organizations of individuals visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purpose of visits, and the names and organizations of individuals visited. Access record reviews determine if access authorizations are current and are still required to support organizational mission and business functions. Access records are not required for publicly accessible areas. Visitor signatures and identification, along with (at times) the purpose of the visit may be considered personal information and should be protected accordingly. Organizations should contact their appropriate privacy senior official or executive for information.

GC discussion: Where appropriate, access records can include the entry and exit of specific facilities, zones, or sensitive areas. These activities are recorded in accordance with departmental security practices and with records retention and disposition schedules.

Related controls and activities: PE-02, PE-03, PE-06.

Enhancements:

(01) Visitor access records: Automated records maintenance and review

Maintain and review visitor access records using [Assignment: organization-defined automated mechanisms].

Discussion: Visitor access records may be stored and maintained in a database that is accessible by organizational personnel with a documented need to know. Automated access to such records facilitates record reviews on a regular basis to determine if access authorizations are current and still required to support organizational mission and business functions. This database should be reviewed periodically for compliance to the organization's approved retention schedule.

Related controls and activities: None.

(02) Visitor access records: Physical access records

Withdrawn: Incorporated into PE-02.

(03) Visitor access records: Limit personal information elements

Limit personal information contained in visitor access records to the following elements identified in the privacy risk assessment: [Assignment: organization-defined elements].

Discussion: Organizations may have requirements that specify the contents of visitor access records. Care should be taken to ensure the least amount of personal information is collected and stored for visitor access records when such information is not needed for operational purposes. This will help reduce the level of privacy risk created by such a system.

Related controls and activities: RA-03, SA-08.

References:

- [TBS Directive on Security Management, Appendix C: Mandatory Procedures for Physical Security Control](#)
- [Privacy Act](#)
- [TBS Policy on Privacy Protection](#)
- [TBS Directive on Privacy Practices](#)

PE-09 Power equipment and cabling

Control: Protect power equipment and power cabling for the system from damage and destruction.

Discussion: Organizations determine the types of protection necessary for the power equipment and cabling employed at different locations that are both internal and external to organizational facilities and environments of operation. Types of power equipment and cabling include internal cabling and uninterruptible power sources in offices or data centres, generators and power cabling outside of buildings, and power sources for self-contained components such as satellites, vehicles, and other deployable systems.

Related controls and activities: PE-04.

Enhancements:

(01) **Power equipment and cabling: Redundant cabling**

Employ redundant power cabling paths that are physically separated by [Assignment: organization-defined distance].

Discussion: Physically separate and redundant power cables ensure that power continues to flow in the event that one of the cables is cut or otherwise damaged.

Related controls and activities: None.

(02) **Power equipment and cabling: Automatic voltage controls**

Employ automatic voltage controls for [Assignment: organization-defined critical system components].

Discussion: Automatic voltage controls can monitor and control voltage. Such controls include voltage regulators, voltage conditioners, and voltage stabilizers.

Related controls and activities: None.

References: None.

PE-10 Emergency shutoff

Control:

- A. Provide the capability of shutting off power to [Assignment: organization-defined system or individual system components] in emergency situations
- B. Place emergency shutoff switches or devices in [Assignment: organization-defined location by system or system component] to facilitate access for authorized personnel
- C. Protect emergency power shutoff capability from unauthorized activation

Discussion: Emergency power shutoff primarily applies to organizational facilities that contain concentrations of system resources, including data centres, mainframe computer rooms, server rooms, and areas with computer-controlled machinery.

Related controls and activities: PE-15.

Enhancements:

(01) **Emergency shutoff: Accidental and unauthorized activation**

Withdrawn: Incorporated into PE-10.

References: None.

PE-11 Emergency power

Control: Provide an uninterruptible power supply to facilitate [Selection (1 or more): an orderly shutdown of the system; transition of the system to long-term alternate power] in the event of a primary power source loss.

Discussion: An uninterruptible power supply (UPS) is an electrical system or mechanism that provides emergency power when there is a failure of the main power source. A UPS is typically used to protect computers, data centres, telecommunication equipment, or other electrical equipment where an unexpected power disruption could cause injuries, fatalities, serious mission or business disruption, or loss of data or information. A UPS differs from an emergency power system or backup generator in that the UPS provides near-instantaneous protection from unanticipated power interruptions from the main power source by providing energy stored in batteries, supercapacitors, or flywheels. The battery duration of a UPS is relatively short but provides sufficient time to start a standby power source, such as a backup generator, or to properly shut down the system.

Related controls and activities: AT-03, CP-02, CP-07.

Enhancements:

(01) Emergency Power: Alternate power supply – minimal operational capability

Provide an alternate power supply for the system that is activated [Selection (1): manually; automatically] and that can maintain minimally required operational capability in the event of an extended loss of the primary power source.

Discussion: Provision of an alternate power supply with minimal operating capability can be satisfied by accessing a secondary commercial power supply or other external power supply.

Related controls and activities: None.

(02) Emergency power: Alternate power supply – self-contained

Provide an alternate power supply for the system that is activated [Selection (1): manually; automatically] and that is:

- a. self-contained
- b. not reliant on external power generation
- c. capable of maintaining [Selection (1): minimally required operational capability; full operational capability] in the event of an extended loss of the primary power source

Discussion: The provision of a long-term, self-contained power supply can be satisfied by using one or more generators with sufficient capacity to meet the needs of the organization.

Related controls and activities: None.

References:

- [RCMP GCPSP-010 Operational Physical Security Guide](#) (restricted to GC)

PE-12 Emergency lighting

Control: Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

Discussion: The provision of emergency lighting applies primarily to organizational facilities that contain concentrations of system resources, including data centres, server rooms, and mainframe computer rooms. Emergency lighting provisions for the system are described in the contingency plan for the organization. If emergency lighting for the system fails or cannot be provided, organizations consider alternate processing sites for power-related contingencies.

Related controls and activities: CP-02, CP-07.

Enhancements:**(01) Emergency lighting: Essential mission and business functions**

Provide emergency lighting for all areas within the facility supporting essential mission and business functions.

Discussion: Organizations define their essential missions and functions.

Related controls and activities: None.

References: [RCMP GCPSPG-004 Security Lighting Considerations Guide](#)

PE-13 Fire protection

Control: Employ and maintain fire detection and suppression systems that are supported by an independent energy source.

Discussion: The provision of fire detection and suppression systems applies primarily to organizational facilities that contain concentrations of system resources, including data centres, server rooms, and mainframe computer rooms. Fire detection and suppression systems that may require an independent energy source include sprinkler systems and smoke detectors. An independent energy source is an energy source, such as a microgrid, that is separate or can be separated from the energy sources providing power for the other parts of the facility.

Related controls and activities: AT-03.

Enhancements:**(01) Fire protection: Detection systems – automatic activation and notification**

Employ fire detection systems that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders] in the event of a fire.

Discussion: Organizations can identify personnel, roles, and emergency responders if individuals on the notification list need to have access authorizations or clearances (e.g., to enter to facilities where access is restricted due to the classification or impact level of information within the facility). Notification mechanisms may require independent energy sources to ensure that the notification capability is not adversely affected by the fire.

Related controls and activities: None.

(02) Fire protection: Suppression systems – automatic activation and notification

- a. Employ fire suppression systems that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders]
- b. Employ an automatic fire suppression capability when the facility is not staffed on a continuous basis

Discussion: Organizations can identify specific personnel, roles, and emergency responders if individuals on the notification list need to have appropriate access authorizations and/or clearances (e.g., to enter to facilities where access is restricted due to the impact level or classification of information within the facility). Notification mechanisms may require independent energy sources to ensure that the notification capability is not adversely affected by the fire.

Related controls and activities: None.

(03) Fire protection: Automatic fire suppression

Withdrawn: Incorporated into PE-13(02).

(04) Fire protection: Inspections

Ensure that the facility undergoes [Assignment: organization-defined frequency] fire protection inspections by authorized and qualified inspectors and that identified deficiencies are resolved within [Assignment: organization-defined time period].

Discussion: Authorized and qualified personnel within the jurisdiction of the organization include provincial and municipal fire inspectors and fire marshals. Organizations provide escorts during inspections in situations where the systems that reside within the facilities contain sensitive information.

Related controls and activities: None.

(400) **Fire protection: Emergency services**

Ensure that firefighting water capacity and effective response times of emergency services are considered when developing safeguarding strategies.

Discussion: Firefighting water capacity and the effective response times of firefighters and police need to be considered during the development of safeguarding strategies, based on the principles of protection, detection, and response. It applies to site selection, facilities, and assets. If emergency response times are inadequate, alternative or additional measures for life safety and asset protection may be required.

Related controls and activities: None.

References:

- [RCMP GCPSG-010 Operational Physical Security Guide](#) (restricted to GC)
- [National Fire Code of Canada 2020](#)

PE-14 Environmental controls

Control:

- Maintain [Selection (1 or more): temperature; humidity; pressure; radiation; [Assignment: organization-defined environmental control]] levels within the facility where the system resides at [Assignment: organization-defined acceptable levels]
- Monitor environmental control levels [Assignment: organization-defined frequency]

Discussion: The provision of environmental controls applies primarily to organizational facilities that contain concentrations of system resources (e.g., data centres, mainframe computer rooms, and server rooms). Insufficient environmental controls, especially in very harsh environments, can have a significant adverse impact on the availability of systems and system components that are needed to support organizational mission and business functions.

Related controls and activities: AT-03, CP-02.

Enhancements:

(01) **Environmental controls: Automatic controls**

Employ the following automatic environmental controls in the facility to prevent potentially harmful fluctuations to the system: [Assignment: organization-defined automatic environmental controls].

Discussion: The implementation of automatic environmental controls provides an immediate response to environmental conditions that can damage, degrade, or destroy organizational systems or systems components.

Related controls and activities: None.

(02) **Environmental controls: Monitoring with alarms and notifications**

Employ environmental control monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment to [Assignment: organization-defined personnel or roles].

Discussion: The alarm or notification may be an audible alarm or a visual message in real time to personnel or roles defined by the organization. Such alarms and notifications can help minimize harm to individuals and damage to organizational assets by facilitating a timely incident response.

Related controls and activities: None.

References: None.

PE-15 Water damage protection

Control: Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

Discussion: The provision of water damage protection primarily applies to organizational facilities that contain concentrations of system resources, including data centres, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern without affecting entire organizations.

Related controls and activities: AT-03, PE-10.

Enhancements:

(01) Water damage protection: Automation support

Detect the presence of water near the system and alert [Assignment: organization-defined personnel or roles] using [Assignment: organization-defined automated mechanisms].

Discussion: Automated mechanisms include notification systems, water detection sensors, and alarms.

Related controls and activities: None.

References: None.

PE-16 Delivery and removal

Control:

- A. Authorize and control [Assignment: organization-defined types of system components] entering and exiting the facility
- B. Maintain records of the system components

Discussion: Enforcing authorizations for entry and exit of system components may require restricting access to delivery areas and isolating the areas from the system and media libraries.

Related controls and activities: CM-03, CM-08, MA-02, MA-03, MP-05, PE-20, SR-02, SR-03, SR-04, SR-06.

Enhancements: None.

References: [RCMP GCPSPG-006 Access Management Guide](#) (restricted to GC)

PE-17 Alternate work site

Control:

- A. Determine and document the [Assignment: organization-defined alternate work sites] allowed for use by employees
- B. Employ the following controls at alternate work sites: [Assignment: organization-defined controls]
- C. Assess the effectiveness of controls at alternate work sites
- D. Provide a means for employees to communicate with information security and privacy personnel in case of incidents

Discussion: Alternate work sites include government facilities or the private residences of employees. While distinct from alternative processing sites, alternate work sites can provide readily available alternate locations during contingency

operations. Organizations can define different sets of controls for specific alternate work sites or types of sites depending on the work-related activities conducted at the sites. Implementing and assessing the effectiveness of organization-defined controls and providing a means to communicate incidents at alternate work sites supports the contingency planning activities of organizations.

Related controls and activities: AC-17, AC-18, CP-07.

Enhancements: None.

References: [RCMP GCPSPG-008 Physical Security Considerations for Remote and Telework Environments](#)

PE-18 Location of system components

Control: Position system components within the facility to minimize potential damage from [Assignment: organization-defined physical and environmental hazards] and to minimize the opportunity for unauthorized access.

Discussion: Physical and environmental hazards include floods, tsunamis, fires, tornadoes, earthquakes, hurricanes, terrorism, vandalism, electromagnetic pulse (EMP), electrical interference, and other forms of incoming electromagnetic radiation. Organizations consider the location of entry points where unauthorized individuals, while not being granted access, might nonetheless be near systems. Such proximity can increase the risk of unauthorized access to organizational communications using wireless packet sniffers, microphones, or unauthorized disclosure of information.

Related controls and activities: CP-02, PE-05, PE-19, PE-20, RA-03.

Enhancements:

(01) **Location of system components: Facility site**

Withdrawn: Moved to PE-23.

References:

- Criteria for the design, fabrication, supply, installation and acceptance testing of walk-in, radio-frequency-shielded enclosures (ITSG-02) (upon request to the Cyber Centre)
- [RCMP GCPSPG-015 Guide to the Application of Physical Security Zones](#) (restricted to GC)

PE-19 Information leakage

Control: Protect the system from information leakage due to electromagnetic signals emanations.

Discussion: Information leakage is the intentional or unintentional release of data or information to an untrusted environment from electromagnetic signals emanations. The security categories or classifications of systems (with respect to confidentiality), organizational security policies, and risk tolerance guide the selection of controls employed to protect systems against information leakage due to electromagnetic signals emanations.

Related controls and activities: AC-18, PE-18, PE-20.

Enhancements:

(01) **Information leakage: National emissions policies and procedures**

Protect system components, associated data communications, and networks in accordance with national emissions security (EMSEC) policies and procedures based on the security category or classification of the information.

Discussion: EMSEC policies include the former TEMPEST policies.

Related controls and activities: None.

References:

- Criteria for the design, fabrication, supply, installation and acceptance testing of walk-in, radio-frequency-shielded enclosures (ITSG-02) (upon request to the Cyber Centre)
- [Canadian Industrial TEMPEST program \(CITP\)](#)
- Emission security (EMSEC) guidance (ITSG-11A) (Protected A)
- Directives for the Application of Communications Security in the Government of Canada (ITSD-01A) (upon request to the Cyber Centre)

PE-20 Asset monitoring and tracking

Control: Employ [Assignment: organization-defined asset location technologies] to track and monitor the location and movement of [Assignment: organization-defined assets] within [Assignment: organization-defined controlled areas].

Discussion: Asset location technologies can help ensure that critical assets—including vehicles, equipment, and system components—remain in authorized locations. Organizations consult with the appropriate privacy senior officials or executives or their legal services regarding the deployment and use of asset location technologies to address potential privacy concerns.

GC discussion: Location tracking of GC employees using GC assets in the exercise of their duties is not considered personal information. While this information may be sensitive, protected, or classified depending on the nature of their duties, it would not be considered personal information if it was created while the employee was exercising their official duties. In the case where an employee decides to use their GC asset (e.g., vehicle, cell phone) for personal purposes, it might be considered personal information, but also an inappropriate use of GC assets. In all cases, a notice given to employees that their GC assets are being tracked and monitored would mitigate privacy concerns regarding the creation of personal information associated with an improper use of such assets.

Related controls and activities: CM-08, PE-16, PM-08.

Enhancements: None.

References:

- [Privacy Act](#)
- [TBS Policy on Privacy Protection](#)
- [TBS Directive on Privacy Practices](#)

PE-21 Electromagnetic pulse protection

Control: Employ [Assignment: organization-defined protective measures] against electromagnetic pulse (EMP) damage for [Assignment: organization-defined systems and system components].

Discussion: An EMP is a short, intense burst of electromagnetic energy that is spread over a range of frequencies. Such energy bursts may be natural or man-made. EMP interference may be disruptive or damaging to electronic equipment. Protective measures used to mitigate EMP risk include shielding, surge suppressors, ferro-resonant transformers, and earth grounding. EMP protection may be especially significant for systems and applications that are part of Canadian critical infrastructure.

Related controls and activities: PE-18, PE-19.

Enhancements: None.

References: None.

PE-22 Component marking

Control: Mark [Assignment: organization-defined system hardware components] indicating the impact level or classification level of the information permitted to be processed, stored, or transmitted by the hardware component.

Discussion: Hardware components that may require marking include input and output devices. Input devices include desktop and notebook computers, keyboards, tablets, and smartphones. Output devices include printers, monitors/video displays, facsimile machines, scanners, copiers, and audio devices. Permissions controlling output to the output devices are addressed in AC-03 or AC-04. Components are marked to indicate the impact level or classification level of the system to which the devices are connected, or the impact level or classification level of the information permitted to be output.

Security marking refers to the use of human-readable security attributes. Security labeling refers to the use of security attributes for internal system data structures. Security marking is generally not required for hardware components that process, store, or transmit information determined by organizations to be in the public domain or to be publicly releasable. However, organizations may require markings for hardware components that process, store, or transmit public information in order to indicate that such information is publicly releasable. Marking of system hardware components reflects applicable laws, Orders in Council, directives, policies, regulations, and standards.

Related controls and activities: AC-03, AC-04, AC-16, MP-03.

Enhancements: None.

References:

- [TBS Directive on Security Management, Appendix E: Mandatory Procedures for Information Management Security Control](#)
- [TBS Directive on Security Management, Appendix J: Standard on Security Categorization](#)
- [PSPC Contract Security Manuel, Annex C: Guidelines for safeguarding information and assets](#)

PE-23 Facility location

Control:

- Plan the location or site of the facility where the system resides considering physical and environmental hazards
- For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy

Discussion: Physical and environmental hazards include floods, tsunamis, fires, tornadoes, earthquakes, hurricanes, terrorism, vandalism, an EMP, electrical interference, and other forms of incoming electromagnetic radiation. Land and environmental surveys can help inform the optimal site location(s) for facilities to reduce as many environmental threats as practicable. Where such threats cannot be avoided, such surveys will identify what, if any, mitigation factors to employ to minimize damage to assets and disruption to services. The location of system components within the facility is addressed in PE-18.

Related controls and activities: CP-02, PE-18, PE-19, PM-08, PM-09, RA-03.

Enhancements: None.

References: None.

PE-400 Remote and telework environments

Control:

- Assess physical security of remote or telework environments

- B. Apply appropriate protection and storage requirements for information and assets
- C. Use approved security equipment and electronic devices in accordance with the categorization of material

Discussion: None.

GC discussion: Security considerations should be addressed in remote or telework locations for GC departments, agencies and employees. Remote/telework can increase the likelihood of compromise of an organization's sensitive information. Information can be targeted by threat actors through different methods such as physical access to information and devices, theft of information or devices, eavesdropping during meetings and telephone conversations, and overviewing of information and devices.

When working in a location other than the designated work site, employees should assess physical security and apply appropriate protection and storage requirements for GC information and assets. A risk assessment needs to be completed for all remote and telework situations and associated work solutions.

Protected A and B material may be processed and stored at remote and telework locations outside a designated GC workplace when physical protections are employed. The processing of Secret and Top Secret (TS) information originating from allies is only permitted in the appropriate zone of a designated GC security zone. TS Sensitive compartmented information (SCI) cannot be processed, stored, or discussed in a telework environment. It is recommended to prevent or limit the use of hard-copy material as much as practicable.

Employees should be provided equipment that supports and promotes secure processing, storage, and transport of GC information. Employees should complete appropriate security awareness training as a condition to being granted their remote/telework request. Appropriate security controls need to be available and in place.

Tracking data for employees on remote/telework agreements should be maintained and should include the names, locations, issued equipment, and assets, as well as registries of information taken to the remote/telework location, when appropriate. Employees are responsible for understanding and implementing all remote/telework security control measures that contribute to the secure processing of GC information at their location.

Related controls and activities: AT-02, PE-17, PE-23, RA-02, RA-03.

Enhancements:

(01) Remote and telework environments: Physical information and assets storage

Store physical information and assets in accordance with RCMP guidance and departmentally established security practices.

Discussion: None.

GC discussion: Effort should be made to limit the need to process or store hard-copy documents of any categorization in locations outside a GC controlled facility. The RCMP does not recommend that Confidential and Secret information or assets be processed in remote/telework environments, but in cases where it cannot be avoided, requirements set out in the RCMP G1-001 Security Equipment Guide should be followed.

The processing and storage of Protected C or Top Secret information outside approved GC facilities is considered an extremely high risk and is not recommended by the RCMP. If unavoidable, departmental physical security shall perform a full site security assessment, including a complete Threat and Risk Assessment (TRA). All security controls required for High Secure Zones in GC facilities should be used as a minimum standard for location fit-up.

Related controls and activities: RA-02, RA-03.

(02) Remote and telework environments: International remote/telework

Allow requests for remote/telework from international locations only under exceptional circumstances.

Discussion: None.

GC discussion: This enhancement does not apply to already assigned positions of employees working abroad as part of their regular operational duties, such as those attached to Canadian Embassies and High Commissions or

military deployments. The RCMP does not recommend allowing remote/telework from international locations. Departments that may allow international remote/telework should develop a process with considerations given for all security controls, risk assessments, approvals, and briefings.

Requests for international remote/telework should only be considered under exceptional circumstances; be limited to a specific defined period of time; require a complete TRA for the employee, country, and city of work; and require additional approval from Deputy Head, department Chief Security Officer (CSO), Chief Human Resources Officer (CHRO) and Chief Information Officer (CIO) as well as Shared Services Canada (SSC).

International remote/telework carries increased security risks for the individual and the GC, since the Vienna Convention on Diplomatic Relations (1963) would not apply to those GC employees. As such, these employees are subject to all local and state laws and are not afforded diplomatic protections for information, assets, or property, including GC information and assets. Additionally, it carries increased physical security risks, and, in some countries, physical security controls may be cost prohibitive or difficult to maintain without a departmental security presence.

Related controls and activities: RA-03.

References:

- [RCMP GCPSP-008 Physical Security Considerations for Remote and Telework Environments](#)
- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [TBS Directive on Security Management, Appendix J: Standard on Security Categorization](#)
- [RCMP GCPSP-007 Transport, Transmittal and Storage of Protected and Classified Material](#) (restricted to GC)
- [TBS Directive on Telework](#)
- [CSE-RCMP Harmonized Threat and Risk Assessment Methodology \(TRA-1\)](#)
- [RCMP G1-001 Security Equipment Guide](#) (restricted to GC)

PE-401 Security operations centre

Control: Establish and maintain a Security Operations Centre (SOC) to protect the organization's people, property, assets, and information, through physical and technical surveillance and monitoring.

Discussion: A SOC combines people, processes, and technology to deliver operational and other security services to organizations, including the protection of people, property, assets, and information. The SOC usually provides the facilities to support security personnel in the monitoring, surveillance, display, control, and management of security-related events, including insider threats. The SOC enables system operators to collect the information related to the physical or cyber environment, to analyze it, to detect and assess alerts notifications, and to dispatch the appropriate personnel to properly respond to events. A SOC increases situational awareness of the organization's environment, enabling effective decision-making and response during an event.

The SOC can assist multidisciplinary teams, including physical security, IT and operational technology (OT) security, analysts, engineers, architects, and other service providers. Indeed, the convergence of IT and OT instigates new requirements to assess the risk posed by both information and physical security. For example, the proper functioning of control systems, such as those seen in building automation that can control temperature, lightning, access, etc., could be impacted if the software/application was compromised.

IR-04(14) provides information on a SOC meant to protect an organization's technical infrastructure, which is comprised of systems and networks.

Related controls and activities: IR-04.

Enhancements: None.

References:

- [RCMP GCPSPG-003 Security Operations Centre Design Considerations Guide](#)
- [Best practices for setting up a security operations centre \(SOC\) \(ITSAP.00.500\)](#)
- [RCMP GCPSPG-019 Protection, Detection, Response, and Recovery Guide](#) (restricted to GC)

Family: Planning

The controls and activities in the Planning (PL) family deal with the development, documentation, update and implementation of security and privacy plans for organizational systems. These plans describe the security and privacy controls in place or planned for the systems, and the rules of behaviour for individuals accessing the systems.

PL-01 Planning policy and procedures

Activity:

- A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]
 1. [Selection (1 or more): Organization-level; Mission/business process-level; System-level] planning policy that
 - a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
 - b. is consistent with applicable laws, jurisprudence, Orders in Council, directives, regulations, policies, standards, and guidelines
 2. procedures to facilitate the implementation of the planning policy and the associated planning controls
- B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the planning policy and procedures
- C. Review and update the current planning
 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]
 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]

Discussion: Planning policy and procedures for the controls in the PL family are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Planning policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on their development.

Security and privacy program policies and procedures at the organization level are preferable and may remove the need for mission-level or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations.

Procedures can be established for security and privacy programs, for mission/business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.

Events that may precipitate an update to planning policy and procedures include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in laws, jurisprudence, Orders in Council, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related controls and activities: PM-09, PS-08, SI-02, SI-12.

Enhancements: None.

References:

- [TBS Policy on Privacy Protection](#)
- [TBS Directive on Privacy Practices](#)
- [TBS Government of Canada Enterprise Architecture Framework](#)

- [TBS Policy on Service and Digital](#)
- [TBS Directive on Service and Digital](#)
- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)

PL-02 System security and privacy plans

Activity:

- A. Develop security and privacy plans for the system that
 1. are consistent with the organization's enterprise architecture
 2. explicitly define the constituent system components
 3. describe the operational context of the system in terms of mission and business processes
 4. identify the individuals that fulfill system roles and responsibilities
 5. identify the information types processed, stored, and transmitted by the system
 6. provide the security categorization of the system, including supporting rationale
 7. describe any specific threats to the system that are of concern to the organization
 8. provide the results of a privacy risk assessment for systems handling personal information
 9. describe the operational environment for the system and any dependencies on or connections to other systems or system components
 10. provide an overview of the security and privacy requirements for the system
 11. identify any relevant control baselines or overlays, if applicable
 12. describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions
 13. include risk determinations for security and privacy architecture and design decisions
 14. include security- and privacy-related activities affecting the system that require planning and coordination with [Assignment: organization-defined individuals or groups]
 15. are reviewed and approved by the authorizing official or designated representative prior to plan implementation
 400. document the business purposes for the processing of personal information
 401. define retention and disposition standards for personal information stored within the system
- B. Distribute copies of the plans and communicate subsequent changes to the plans to [Assignment: organization-defined personnel or roles]
- C. Review the plans [Assignment: organization-defined frequency]
- D. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments
- E. Protect the plans from unauthorized disclosure and modification

Discussion: System security and privacy plans are scoped to the system and system components within the defined authorization boundary and contain an overview of the security and privacy requirements for the system and the controls selected to satisfy the requirements. The plans describe the intended application of each selected control in the context of the system with a sufficient level of detail to correctly implement the control and to subsequently assess the effectiveness of the control.

The control documentation describes how system-specific and hybrid controls are implemented and the plans and expectations regarding the functionality of the system. System security and privacy plans can also be used in the design and development of systems in support of lifecycle-based security and privacy engineering processes.

System security and privacy plans are living documents that are updated and adapted throughout the system development lifecycle (e.g., during capability determination, analysis of alternatives, requests for proposal, and design reviews). Section

2.1 describes the different types of requirements that are relevant to organizations during the system development lifecycle and the relationship between requirements and controls.

Organizations may develop a single, integrated security and privacy plan or maintain separate plans. Security and privacy plans relate security and privacy requirements to a set of controls and control enhancements. The plans describe how the controls and control enhancements meet the security and privacy requirements but do not provide detailed, technical descriptions of the design or implementation of the controls and control enhancements. Security and privacy plans contain sufficient information (including specifications of control parameter values for selection and assignment operations explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, other organizations, and Canada if the plan is implemented.

Security and privacy plans do not need to be single documents. The plans can be a collection of various documents, including documents that already exist. Effective security and privacy plans make extensive use of references to policies, procedures, and additional documents, including design and implementation specifications, where more detailed information can be obtained. The use of references helps reduce the documentation associated with security and privacy programs and maintains the security- and privacy-related information in other established management and operational areas, including enterprise architecture, system development lifecycle, systems engineering, and acquisition. Security and privacy plans do not need to contain detailed contingency plans, incident response plans, or privacy breach processes but can instead provide (explicitly or by reference) sufficient information to define what needs to be accomplished by those plans.

Security- and privacy-related activities that may require coordination and planning with other individuals or groups within the organization include assessments, audits, inspections, hardware and software maintenance, acquisition and supply chain risk management, patch management, and contingency plan testing. Planning and coordination include emergency and non-emergency (i.e., planned or non-urgent unplanned) situations. The process defined by organizations to plan and coordinate security- and privacy-related activities can also be included in other documents, as appropriate.

Related controls and activities: AC-02, AC-06, AC-14, AC-17, AC-20, CA-02, CA-03, CA-07, CM-09, CM-13, CP-02, CP-04, IR-04, IR-08, MA-04, MA-05, MP-04, MP-05, PL-07, PL-08, PL-10, PL-11, PM-01, PM-07, PM-08, PM-09, PM-10, PM-11, RA-03, RA-08, RA-09, SA-05, SA-17, SA-22, SI-12, SR-02, SR-04.

Enhancements:

(01) **System security and privacy plans: Concept of operations**

Withdrawn: Incorporated into PL-07.

(02) **System security and privacy plans: Functional architecture**

Withdrawn: Incorporated into PL-08.

(03) **System security and privacy plans: Plan and coordinate with other organizational entities**

Withdrawn: Incorporated into PL-02.

References:

- [TBS Policy on Service and Digital](#)
- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)

PL-03 System security plan update

Withdrawn: Incorporated into PL-02.

PL-04 Rules of behaviour

Activity:

- A. Establish and provide to individuals requiring access to the system the rules that describe their responsibilities and expected behaviour for information and system usage, security, and privacy
- B. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behaviour, before authorizing access to information and the system
- C. Review and update the rules of behaviour [Assignment: organization-defined frequency]
- D. Require individuals who have acknowledged a previous version of the rules of behaviour to read and re-acknowledge [Selection (1 or more): [Assignment: organization-defined frequency]; when the rules are revised or updated]

Discussion: Rules of behaviour represent a type of access agreement for organizational users. Other types of access agreements include non-disclosure agreements, conflict of interest agreements, and acceptable use agreements (see PS-06). Organizations should consider rules of behaviour based on individual user roles and responsibilities and differentiate between rules that apply to privileged users and rules that apply to general users.

Establishing rules of behaviour for some types of non-organizational users, including individuals who receive information from federal systems, is often not feasible given the large number of such users and the limited nature of their interactions with the systems. Rules of behaviour for organizational and non-organizational users can also be established in AC-08. The related controls and activities section provides a list of controls that are relevant to organizational rules of behaviour. PL-04B, the documented acknowledgment portion of the control, may be satisfied by the literacy training and awareness and role-based training programs conducted by organizations if such training includes rules of behaviour. Documented acknowledgments for rules of behaviour include electronic or physical signatures and electronic agreement check boxes or radio buttons.

GC discussion: The expectations for rules of behaviour for external system users or recipients of information contained within governmental systems can be captured in an information sharing agreement or arrangement.

Related controls and activities: AC-02, AC-06, AC-08, AC-09, AC-17, AC-18, AC-19, AC-20, AT-02, AT-03, CM-11, IA-02, IA-04, IA-05, MP-07, PS-06, PS-08, SA-05, SI-12.

Enhancements:

(01) Rules of behaviour: Social media and external site/application usage restrictions

Include in the rules of behaviour restrictions on:

- a. use of social media, social networking sites, and external sites/applications
- b. posting organizational information on public websites
- c. use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications

Discussion: Social media, social networking, and external site/application usage restrictions address rules of behaviour related to the use of social media, social networking, and external sites when organizational personnel are using such sites for official duties or in the conduct of official business, when organizational information is involved in social media and social networking transactions, and when personnel access social media and networking sites from organizational systems. Organizations should also address specific rules that prevent unauthorized entities from obtaining non-public organizational information from social media and networking sites either directly or through inference. Non-public information includes personal information and system account information.

Related controls and activities: AC-22, AU-13.

References:

- [TBS Policy on Service and Digital](#)
- [TBS Directive on Service and Digital, Appendix A: Examples of Acceptable Network and Device Use](#)
- [TBS Directive on Service and Digital, Appendix B: Examples of Unacceptable Network and Device Use](#)
- [TBS Privacy Implementation Notice 2021-01: Privacy Requirements for Official Social Media Accounts](#)
- [Security considerations when using social media in your organization \(ITSM.10.066\)](#)
- [Use of personal social media in the workplace \(ITSAP.00.066\)](#)

PL-05 Privacy impact assessment

Withdrawn: Incorporated into RA-08.

PL-06 Security-related activity planning

Withdrawn: Incorporated into PL-02.

PL-07 Concept of operations

Activity:

- A. Develop a Concept of Operations (CONOPS) for the system describing how the organization intends to operate the system from the perspective of information security and privacy
- B. Review and update the CONOPS [Assignment: organization-defined frequency]

Discussion: The CONOPS may be included in the security or privacy plans for the system or in other system development lifecycle documents. The CONOPS is a living document that requires updating throughout the system development lifecycle. For example, during system design reviews, the CONOPS is checked to ensure that it remains consistent with the design for controls, the system architecture, and the operational procedures. Changes to the CONOPS are reflected in ongoing updates to the security and privacy plans, security and privacy architectures, and other organizational documents, such as procurement specifications, system development lifecycle documents, and systems engineering documents.

Related controls and activities: PL-02, SA-02, SI-12.

Enhancements: None.

References:

- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)

PL-08 Security and privacy architecture

Activity:

- A. Develop security and privacy architectures for the system that describe
 1. the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information
 2. the requirements and approach to be taken for handling personal information to minimize any privacy risk to individuals
 3. how the architectures are integrated into and support the enterprise architecture
 4. any assumptions about, and dependencies on, external systems and services

- B. Review and update the architectures [Assignment: organization-defined frequency] to reflect changes in the enterprise architecture
- C. Reflect planned architecture changes in security and privacy plans, CONOPS, criticality analysis, organizational procedures, and procurements and acquisitions

Discussion: The security and privacy architectures at the system level are consistent with the organization-wide security and privacy architectures described in PM-07, which are integral to and developed as part of the enterprise architecture. The architectures include an architectural description, the allocation of security and privacy functionality (including controls), security- and privacy-related information for external interfaces, information being exchanged across the interfaces, personal information data flow, and the protection mechanisms associated with each interface. The architectures can also include other information, such as user roles and the access privileges assigned to each role; security and privacy requirements; types of information processed, stored, and transmitted by the system; supply chain risk management requirements; restoration priorities of information and system services; and other protection needs.

It is important to follow relevant guidance on the use of security architectures as part of the system development lifecycle process. The Cyber Centre recommends the use of the systems security engineering concepts described in System lifecycle cyber security and privacy risk management activities (ITSP.10.037). Security and privacy architectures are reviewed and updated throughout the system development lifecycle, from analysis of alternatives through review of the proposed architecture in contract proposals to the design reviews before and during implementation (e.g., during preliminary design reviews and critical design reviews).

In today's modern computing architectures, it is becoming less common for organizations to control all information resources. There may be key dependencies on external information services and service providers. Describing such dependencies in the security and privacy architectures is necessary for developing a comprehensive mission and business protection strategy.

Establishing, developing, documenting, and maintaining under configuration control a baseline configuration for organizational systems is critical to implementing and maintaining effective architectures. The development of the architectures is coordinated with the office of the departmental CIO, the senior official in the department's security governance, and the appropriate privacy senior official or executive to ensure that the controls needed to support security and privacy requirements are identified and effectively implemented.

In many circumstances, there may be no distinction between the security and privacy architecture for a system. In other circumstances, security objectives may be adequately satisfied, but privacy objectives may only be partially satisfied by the security requirements. In these cases, consideration of the privacy requirements needed to achieve satisfaction will result in a distinct privacy architecture. The documentation, however, may simply reflect the combined architectures.

PL-08 is primarily directed at organizations to ensure that architectures are developed for the system and, moreover, that the architectures are integrated with or tightly coupled to the enterprise architecture. In contrast, SA-17 is primarily directed at the external IT product and system developers and integrators. SA-17, which is complementary to PL-08, is selected when organizations outsource the development of systems or components to external entities and when there is a need to demonstrate consistency with the organization's enterprise architecture and security and privacy architectures.

Related controls and activities: CM-02, CM-06, PL-02, PL-07, PL-09, PM-05, PM-07, RA-09, SA-03, SA-05, SA-08, SA-17, SC-07.

Enhancements:

(01) Security and privacy architectures: Defence in depth

Design the security and privacy architectures for the system using a defence-in-depth approach that:

- a. allocates [Assignment: organization-defined controls] to [Assignment: organization-defined locations and architectural layers]
- b. ensures that the allocated controls operate in a coordinated and mutually reinforcing manner

Discussion: Organizations strategically allocate security and privacy controls in the security and privacy architectures so that adversaries must overcome multiple controls to achieve their objective. Requiring adversaries to defeat multiple controls makes it more difficult to attack information resources by increasing the work factor of the adversary; it also increases the likelihood of detection. The coordination of allocated controls is essential to ensure that an attack that involves one control does not create adverse, unintended consequences by interfering with other controls. Unintended consequences can include system lock-out and cascading alarms.

The placement of controls in systems and organizations is an important activity that requires thoughtful analysis. The value of organizational assets is an important consideration in providing additional layering. Defence-in-depth architectural approaches include modularity and layering (see SA-08(03)), separation of system and user functionality (see SC-02), and security function isolation (see SC-03).

Related controls and activities: SC-02, SC-03, SC-29, SC-36.

(02) Security and privacy architectures: Supplier diversity

Require that [Assignment: organization-defined controls] allocated to [Assignment: organization-defined locations and architectural layers] are obtained from different suppliers.

Discussion: IT products have different strengths and weaknesses. Providing a broad spectrum of products complements the individual offerings. For example, vendors offering malicious code protection typically update their products at different times, often developing solutions for known viruses, Trojans, or worms based on their priorities and development schedules. By deploying different products at different locations, there is an increased likelihood that at least one of the products will detect the malicious code. With respect to privacy, vendors may offer products that track personal information in systems. Products may use different tracking methods. Using multiple products may result in more assurance that personal information is inventoried.

Related controls and activities: SC-29, SR-3.

References:

- [TBS Directive on Service and Digital](#)
- [TBS Government of Canada Enterprise Architecture Framework](#)
- [TBS Policy on Privacy Protection](#)
- [TBS Directive on Privacy Practices](#)
- [Guidance on defence in depth for cloud-based services \(ITSP.50.104\)](#)
- System lifecycle cyber security and privacy risk management activities (ITSP.10.037)

PL-09 Central management

Control: Centrally manage [Assignment: organization-defined controls and related processes].

Discussion: Central management refers to organization-wide management and implementation of selected controls and processes. This includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed controls and processes. As the central management of controls is generally associated with the concept of common (inherited) controls, such management promotes and facilitates standardization of control implementations and management and the judicious use of organizational resources. Centrally managed controls and processes may also meet independence requirements for assessments in support of initial and ongoing authorizations to operate and as part of organizational continuous monitoring.

Automated tools (e.g., security information and event management tools or enterprise security monitoring and management tools) can improve the accuracy, consistency, and availability of information associated with centrally managed controls and processes. Automation can also provide data aggregation and data correlation capabilities, alerting mechanisms, and dashboards to support risk-based decision-making within the organization. Some central management or enterprise security monitoring tools can collect or create personal behavioural information about system users. This information should be

protected as personal information. For insight, organizations should seek advice and guidance from the organization's appropriate privacy senior officials or executives.

As part of the control selection processes, organizations should determine the controls that may be suitable for central management based on resources and capabilities. It is not always possible to centrally manage every aspect of a control. In such cases, the control can be treated as a hybrid control with the control managed and implemented centrally or at the system level. The controls and control enhancements that are candidates for full or partial central management include but are not limited to: AC-02(01), AC-02(02), AC-02(03), AC-02(04), AC-04(all), AC-17(01), AC-17(02), AC-17(03), AC-17(09), AC-18(01), AC-18(03), AC-18(04), AC-18(05), AC-19(04), AC-22, AC-23, AT-02(01), AT-02(02), AT-03(01), AT-03(02), AT-03(03), AT-04, AU-03, AU-06(01), AU-06(03), AU-06(05), AU-06(06), AU-06(09), AU-07(01), AU-07(02), AU-11, AU-13, AU-16, CA-02(01), CA-02(02), CA-02(03), CA-03(01), CA-03(02), CA-03(03), CA-07(01), CA-09, CM-02(02), CM-03(01), CM-03(04), CM-04, CM-06, CM-06(01), CM-07(02), CM-07(04), CM-07(05), CM-08(all), CM-09(01), CM-10, CM-11, CP-07(all), CP-08(all), SC-43, SI-02, SI-03, SI-04(all), SI-07, SI-08.

Related controls and activities: PL-08, PM-09.

Enhancements: None.

References: None.

PL-10 Baseline selection

Activity: Select a control baseline for the system.

Discussion: Control baselines are predefined sets of controls specifically assembled to address the protection needs of a group, organization, or community of interest. Controls are chosen for baselines to either satisfy mandates imposed by laws, Orders in Council, directives, regulations, policies, standards, and guidelines or address threats common to all users of the baseline under the assumptions specific to the baseline.

Baselines represent a starting point for the protection of individuals' privacy, information, and information systems with subsequent tailoring actions to manage risk in accordance with mission, business, or other constraints (see PL-11). Recommended control baselines are provided in Security and privacy controls and assurance activities catalogue – Baseline profiles (ITSP.10.033-01) for Protected B, Medium Integrity, Medium Availability (PBMM) and Cloud profiles.

The selection of a control baseline is determined by the needs of stakeholders. Stakeholders need to consider mission and business requirements as well as mandates imposed by applicable laws, Orders in Council, directives, policies, regulations, standards, and guidelines. The requirements recommend organizations to select one of the control baselines after the reviewing the information types and the information that is processed, stored, and transmitted on the system; analyzing the potential adverse impact of the loss or compromise of the information or system on the organization's operations and assets, individuals, other organizations, or Canada; and considering the results from system and organizational risk assessments.

GC discussion: The control baselines in Security and privacy controls and assurance activities catalogue – Baseline profiles (ITSP.10.033-01) are compliant with TBS policies, directives, standards, and guidelines. For guidance on control baselines for national security systems, contact contact@cyber.gc.ca.

Related controls and activities: PL-02, PL-11, RA-02, RA-03, SA-08.

Enhancements: None.

References:

- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [TBS Government of Canada Security Control Profile for Cloud-based GC Services](#)

- [TBS Directive on Service and Digital, Appendix G: Standard on Enterprise Information Technology Service Common Configurations](#)
- [TBS Directive on Service and Digital, Appendix J: Standard on Systems that Manage Information and Data](#)
- [Baseline Security Requirements for Network Security Zones \(ITSP.80.022\)](#)
- Directive for the Control of COMSEC Material in the Government of Canada (ITSD-03A) (upon request to the Cyber Centre)
- [Baseline cyber security controls for small and medium organizations](#)
- [Introduction to the baseline controls](#)
- Security and privacy controls and assurance activities catalogue – Baseline profiles (ITSP.10.033-01)

PL-11 Baseline tailoring

Activity: Tailor the selected control baseline by applying specified tailoring actions.

Discussion: The concept of tailoring allows organizations to specialize or customize a set of baseline controls by applying a defined set of tailoring actions. Tailoring actions facilitate such specialization and customization by allowing organizations to develop security and privacy plans that reflect their specific mission and business functions, the environments where their systems operate, the threats and vulnerabilities that can affect their systems, and any other conditions or situations that can impact their mission or business success. Tailoring guidance is provided in the Cyber security and privacy risk management: A lifecycle approach series.

Tailoring a control baseline is accomplished by identifying and designating common controls, applying scoping considerations, selecting compensating controls, assigning values to control parameters, supplementing the control baseline with additional controls as needed, and providing information for control implementation. The general tailoring actions in the Cyber security and privacy risk management: A lifecycle approach series can be supplemented with additional actions based on the needs of organizations.

Tailoring actions can be applied to the baselines provided in Security and privacy controls and assurance activities catalogue – Baseline profiles (ITSP.10.033-01) in accordance with the security and privacy requirements from the *Privacy Act*, PIPEDA, and TBS policies and directives. Alternatively, other communities of interest adopting different control baselines can apply the tailoring actions in Cyber security and privacy risk management: A lifecycle approach series to specialize or customize the controls that represent the specific needs and concerns of those entities.

Related controls and activities: PL-10, RA-02, RA-03, RA-09, SA-08.

Enhancements: None.

References:

- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [TBS Government of Canada Security Control Profile for Cloud-based GC Services](#)
- [TBS Directive on Service and Digital, Appendix G: Standard on Enterprise Information Technology Service Common Configurations](#)
- [Baseline security requirements for network security zones \(ITSP.80.022\)](#)
- Directive for the Control of COMSEC Material in the Government of Canada (ITSD-03A) (upon request to the Cyber Centre)
- [Baseline cyber security controls for small and medium organizations](#)
- [Introduction to the baseline controls](#)
- Security and privacy controls and assurance activities catalogue – Baseline profiles (ITSP.10.033-01)

Family: Program management

TBS, through its policy suite, requires GC departments and agencies to develop, implement, and provide oversight for organization-wide information security and privacy programs to help ensure the confidentiality, integrity, and availability of GC information processed, stored, and transmitted by GC information systems and to protect individual privacy. The program management (PM) controls and activities described in this section are implemented at the organization level and not directed at individual information systems.

PM-01 Information security program plan

Activity:

- A. Develop and disseminate an organization-wide information security program plan that
 1. provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements
 2. includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance
 3. reflects the coordination among organizational entities responsible for information security
 4. is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and Canada
- B. Review and update the organization-wide information security program plan [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]
- C. Protect the information security program plan from unauthorized disclosure and modification

Discussion: An information security program plan is a formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements. An information security program plan can be represented in a single document or sets of documents. Privacy program plans and supply chain risk management plans are addressed separately in PM-18 and SR-02, respectively.

An information security program plan documents implementation details about program management and common controls. The plan provides sufficient information about the controls (including specification of parameters for assignment and selection operations, explicitly or by reference) to enable implementations that are unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended. Updates to information security program plans include organizational changes, and problems identified during plan implementation or control assessments.

Program management controls may be implemented at the organization, mission, or business process level, and are essential for managing the organization's information security program. Program management controls are distinct from common, system-specific, and hybrid controls because program management controls are independent of any particular system. Together, the individual system security plans and the organization-wide information security program plan provide complete coverage for the security controls employed within the organization.

Common controls available for inheritance by organizational systems are documented in an appendix to the organization's information security program plan unless the controls are included in a separate security plan for a system. The organization-wide information security program plan indicates which separate security plans contain descriptions of common controls.

Events that may precipitate an update to the information security program plan include, but are not limited to, organization-wide assessment or audit findings, security incidents or breaches, or changes in laws, Orders in Council, directives, regulations, policies, standards, and guidelines.

Related controls and activities: PL-02, PM-18, PM-30, RA-09, SI-02, SI-12, SR-02.

Enhancements: None.

References:

- [Privacy Act](#)
- [TBS Policy on Privacy Protection](#)
- [TBS Policy on Government Security](#)
- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [TBS Guide to Integrated Risk Management](#)

PM-02 Information security program leadership role

Control: Appoint a senior official in the department's security governance with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

Discussion: The senior official in the department's security governance is an organizational official. For federal departments and agencies (as defined by applicable laws, Orders in Council, regulations, directives, policies, and standards), this official is the senior agency information security officer. Organizations may also refer to this official as the senior information security officer or chief information security officer.

Related controls and activities: None.

Enhancements: None.

References:

- [TBS Policy on Government Security](#)
- [TBS Directive on Security Management](#)

PM-03 Information security and privacy resources

Control:

- A. Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement
- B. Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, Orders in Council, directives, policies, regulations, standards
- C. Make the planned information security and privacy resources available for expenditure

Discussion: Organizations consider establishing champions for information security and privacy and, as part of including the necessary resources, assign specialized expertise and resources as needed. Organizations may designate and empower a group to manage and provide oversight for the information security and privacy aspects of the capital planning and investment control process.

Related controls and activities: PM-04, SA-02.

Enhancements: None

References:

- [TBS Directive on Privacy Practices](#)
- [TBS Guideline on Service and Digital](#)
- [TBS Directive on Security Management: Appendix F: Mandatory Procedures for Security in Contracts and Other Arrangements Control](#)

PM-04 Plan of action and milestones process

Activity:

- A. Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems
 1. are developed and maintained
 2. document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and Canada
 3. are reported in accordance with established reporting requirements
- B. Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions

Discussion: Organizations develop plans of action and milestones with an organization-wide perspective, prioritizing risk response actions and ensuring consistency with the goals and objectives of the organization. Plan of action and milestones updates are based on findings from control assessments and continuous monitoring activities. There can be multiple plans of action and milestones corresponding to the information system level, mission/business process level, and organizational/governance level. While plans of action and milestones are required for federal organizations, other types of organizations can help reduce risk by documenting and tracking planned remediations. Specific guidance on plans of action and milestones at the system level is provided in CA-05.

GC discussion: The plan of action and milestones is a key organizational document and is subject to reporting requirements established by the TBS.

Related controls and activities: CA-05, CA-07, PM-03, RA-07, SI-12.

Enhancements: None.

References: [TBS Framework for the Management of Risk](#)

PM-05 System and program inventory

Control: Develop and update [Assignment: organization-defined frequency] an inventory of organizational systems and programs.

Discussion: System inventory refers to an organization-wide inventory of systems, not system components as described in CM-08.

Related controls and activities: None.

Enhancements:

(01) **System and program inventory: Inventory of personal information**

Establish, maintain, and update [Assignment: organization-defined frequency] an inventory of all systems, programs, applications, and projects that process personal information.

Discussion: An inventory of systems, programs, applications, and projects that handle personal information supports the mapping of data actions, requiring the confirmation of lawful authority for collecting and maintaining accurate personal information, and for limiting the handling of personal information unless it relates directly to an operating program or activity of the organization. Organizations may use this inventory to ensure that systems only handle the personal information required for an institution's operating programs and services, in compliance with approved retention standards.

GC discussion: For GC organizations, personal information intended to be used to make administrative decisions should also be reflected in PIBs. These PIBs can be either institution-specific or standard and should comprehensively reflect every element of personal information. PIBs will also describe the legislative authority for the collection, permissible uses and disclosures of the information, and the retention and disposition standards. They may also describe requirements for individuals who are seeking access to their personal information.

Related controls and activities: AC-03, CM-08, CM-12, CM-13, PL-08, PM-22, PT-03, PT-05, SI-12, SI-18.

References:

- [Privacy Act](#)
- [TBS Policy on Privacy Protection](#)
- [TBS Directive on Privacy Practices](#)
- [GC Info Source: Online Publishing Requirements](#)

PM-06 Measures of performance

Activity: Develop, monitor, and report on the results of information security and privacy measures of performance.

Discussion: Measures of performance are outcome-based metrics used by an organization to measure the effectiveness or efficiency of the information security and privacy programs and the controls employed in support of the program. To facilitate security and privacy risk management, organizations consider aligning measures of performance with the organizational risk tolerance as defined in the risk management strategy.

Cyber security performance metrics could include the volume of security breaches, attainment of Cyber Security Readiness Goals (CRGs), robustness, post-incident change implementation, and security investments versus budget for lawsuits, class actions, public relations, and incident recovery. Some factors to consider when assessing privacy measures of performance include the volume of breaches, metrics related to well-founded complaints to the OPC, and the completion of privacy assessment tools for organizational programs and services.

Related controls and activities: CA-07, PM-09.

Enhancements: None.

References:

- [Privacy Act](#)
- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [TBS Directive on Security Management: Appendix E: Mandatory Procedures for Information Management Security Control](#)

PM-07 Enterprise architecture

Activity: Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations and assets, individuals, other organizations, and Canada.

Discussion: The integration of security and privacy requirements and controls into the enterprise architecture helps to ensure that security and privacy considerations are addressed throughout the system development lifecycle and are explicitly related to the organization's mission and business processes. The process of integrating security and privacy requirements also embeds into the enterprise architecture and the organization's security and privacy architectures consistent with the organizational risk management strategy.

For PM-07, security and privacy architectures are developed at a system-of-systems level, representing all organizational systems. For PL-08, the security and privacy architectures are developed at a level that represents an individual system. The system-level architectures are consistent with the security and privacy architectures defined for the organization. Security and privacy requirements and control integration are most effectively accomplished through the rigorous application of the Cyber Centre Cyber security and privacy risk management: A lifecycle approach series, together with supporting security standards and guidelines.

GC discussion: For GC departments and agencies, security and privacy requirements and control integration are most effectively accomplished by rigorously applying, to the departmental architecture, the Cyber Security and Privacy Risk Management: A Lifecycle Approach series, together with the supporting privacy policy suite requirements issued by TBS and considering the requirements set by legislation, regulations, and jurisprudence.

Related controls and activities: AU-06, PL-02, PL-08, PM-11, RA-02, SA-03, SA-08, SA-17.

Enhancements:

(01) Enterprise architecture: Offloading

Offload [Assignment: organization-defined non-essential functions or services] to other systems, system components, or an external provider.

Discussion: Not every function or service that a system provides is essential to organizational mission or business functions. Printing or copying is an example of a non-essential but supporting service for an organization. Whenever feasible, such supportive but non-essential functions or services are not co-located with the functions or services that support essential mission or business functions. Maintaining such functions on the same system or system component increases the attack surface of the organization's mission-essential functions or services. Moving supportive but non-essential functions to a non-critical system, system component, or external provider can also increase efficiency by putting those functions or services under the control of individuals or providers who are SMEs in the functions or services. If an external provider has access to personal information, it is important to ensure privacy controls and activities are reflected in associated contract vehicles.

Related controls and activities: SA-08.

References:

- [TBS Government of Canada Enterprise Architecture Framework](#)
- Organizational cyber security and privacy risk management activities (ITSP.10.036)
- System lifecycle cyber security and privacy risk management activities (ITSP.10.037)
- [Privacy Act](#)
- [TBS Policy on Privacy Protection](#)
- [TBS Directive on Privacy Practices](#)

PM-08 Critical infrastructure plan

Activity: Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

Discussion: Protection strategies are based on the prioritization of critical assets and resources. The requirement and guidance for defining critical infrastructure and key resources and for preparing an associated critical infrastructure

protection plan are found in applicable laws, jurisprudence, Orders in Council, directives, policies, regulations, standards, and guidelines.

Related controls and activities: CP-02, CP-04, PE-18, PL-02, PM-09, PM-11, PM-18, RA-03, SI-12.

Enhancements: None.

References: [Public Safety Canada Risk Management Guide for Critical Infrastructure Sectors](#)

PM-09 Risk management strategy

Activity:

- A. Develop a comprehensive strategy to manage the
 1. security risks to organizational operations and assets, individuals, other organizations, and Canada associated with the operation and use of organizational systems
 2. privacy risks to individuals resulting from the authorized handling of personal information
- B. Implement the risk management strategy consistently across the organization
- C. Review and update the risk management strategy [Assignment: organization-defined frequency] or as required, to address organizational changes

Discussion: An organization-wide risk management strategy includes an expression of the security and privacy risk tolerance for the organization, security and privacy risk mitigation strategies, acceptable risk assessment methodologies, a process for evaluating security and privacy risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time.

The senior accountable official for risk management (head of department or designated official) aligns information security management processes with strategic, operational, and budgetary planning processes. The risk executive function, led by the senior accountable official for risk management, can facilitate consistent application of the risk management strategy across the organization.

The risk management strategy can be informed by security and privacy risk-related inputs from other sources, both internal and external to the organization, to ensure that the strategy is broad and comprehensive. The supply chain risk management strategy described in PM-30 can also provide useful inputs to the organization-wide risk management strategy.

Related controls and activities: AC-01, AU-01, AT-01, CA-01, CA-02, CA-05, CA-06, CA-07, CM-01, CP-01, IA-01, IR-01, MA-01, MP-01, PE-01, PL-01, PL-02, PM-02, PM-08, PM-18, PM-28, PM-30, PS-01, PT-01, PT-02, PT-03, RA-01, RA-03, RA-09, SA-01, SA-04, SC-01, SC-38, SI-01, SI-12, SR-01, SR-02.

Enhancements: None.

References:

- [TBS Framework for the Management of Risk](#)
- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [TBS Directive on Service and Digital](#)
- [TBS Guideline on Service and Digital](#)
- [TBS Directive on Privacy Practices, Appendix C: Standard on Privacy Impact Assessment](#)
- [TBS Directive on Privacy Practices](#)

PM-10 Authorization process

Control:

- A. Manage the security and privacy state of organizational systems and the environments in which those systems operate through authorization processes
- B. Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process
- C. Integrate the authorization processes into an organization-wide risk management program

Discussion: Authorization processes for organizational systems and environments of operation require the implementation of an organization-wide risk management process and associated security and privacy standards and guidelines. Specific roles for risk management processes include a risk executive (function) and designated authorizing officials for each organizational system and common control provider. The authorization processes for the organization are integrated with continuous monitoring processes to facilitate ongoing understanding and acceptance of security and privacy risks to organizational operations, organizational assets, individuals, other organizations, and Canada.

Related controls and activities: CA-06, CA-07, PL-02.

Enhancements: None.

References:

- [TBS Framework for the Management of Risk](#)
- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [TBS Guideline on Service and Digital](#)

PM-11 Mission and business process definition

Activity:

- A. Define organizational mission and business processes with consideration for information security and privacy protection and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and Canada
- B. Determine information protection and personal information handling needs arising from the defined mission and business processes
- C. Review and revise the mission and business processes [Assignment: organization-defined frequency]

Discussion: Protection needs are technology-independent capabilities that are required to counter threats to organizations, individuals, systems, and Canada from the compromise of information (i.e., loss of confidentiality, integrity, availability, or privacy). Information protection and personal information handling needs are derived from the mission and business needs defined by organizational stakeholders, the mission and business processes designed to meet those needs, and the organizational risk management strategy.

Information protection and personal information handling needs determine the required controls for the organization and the systems. Inherent to defining protection and personal information handling needs is an understanding of the adverse impact that could result if a compromise or breach of information occurs. The categorization process is used to make such potential impact determinations.

Privacy risks to individuals can arise from the compromise of personal information, but they can also arise as unintended consequences or a by-product of the handling of personal information at any stage of the information lifecycle. PIAs are used to identify potential injuries that may arise from the handling of personal information. These impact assessments enable the selection of the required controls. Mission and business process definitions and the associated protection requirements are documented in accordance with organizational policies and procedures.

Related controls and activities: CP-02, PL-02, PM-07, PM-08, RA-02, RA-03, RA-09, SA-02.

Enhancements: None.

References:

- [TBS Directive on Security Management](#)
- [TBS Guideline on Service and Digital](#)
- [TBS Policy on Privacy Protection](#)
- [TBS Directive on Privacy Practices](#)
- [TBS Directive on Privacy Practices, Appendix C: Standard on Privacy Impact Assessment](#)

PM-12 Insider threat program

Control: Implement an insider threat program that includes a cross-discipline insider threat incident handling team.

Discussion: Insider threat programs can leverage the existence of incident handling teams that organizations may already have in place, such as computer security incident response teams. Human resources records are especially important in this effort, as there is compelling evidence to show that some types of insider crimes are often preceded by nontechnical behaviours in the workplace, including ongoing patterns of disgruntled behaviour and conflicts with coworkers and other colleagues. These precursors can guide organizational officials in more focused, targeted monitoring efforts.

However, the use of human resource records could raise significant concerns for privacy and compliance with the Charter of Rights and Freedoms. The participation of a legal team, including consultation with the appropriate privacy senior official or executive, ensures that monitoring activities are performed in accordance with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines.

GC discussion: In addition, there are specific notice requirements when monitoring GC electronic networks and devices. These additional requirements are reflected in the Policy, Directive and Guidelines on Service and Digital.

Related controls and activities: AC-06, AT-02, AU-06, AU-07, AU-10, AU-12, AU-13, CA-07, IA-04, IR-04, MP-07, PE-02, PM-16, PS-03, PS-04, PS-05, PS-07, PS-08, SC-07, SC-38, SI-04, PM-14.

Enhancements: None.

References:

- [TBS Policy on Service and Digital](#)
- [TBS Directive on Service and Digital](#)
- [TBS Guideline on Service and Digital](#)

PM-13 Security and privacy workforce

Activity: Establish a security and privacy workforce development and improvement program.

Discussion: Security and privacy workforce development and improvement programs include defining the knowledge, skills, and abilities needed to perform security and privacy duties and tasks; developing role-based training programs for individuals assigned security and privacy roles and responsibilities; and providing standards and guidelines for measuring and building individual qualifications for incumbents and applicants for security- and privacy-related positions. Such workforce development and improvement programs can also include security and privacy career paths to encourage security and privacy professionals to advance in the field and fill positions with greater responsibility.

The programs encourage organizations to fill security- and privacy-related positions with qualified personnel. Security and privacy workforce development and improvement programs are complementary to organizational security awareness and training programs and focus on developing and institutionalizing the core security and privacy capabilities of personnel needed to protect organizational operations, assets, and individuals. A capable workforce means that employees have the necessary resources, tools, relationships, training, education, and supervisory support to enable them to apply knowledge and skills in their day-to-day work.

GC discussion: The [TBS Guideline on Service and Digital](#) provides non-exhaustive lists of desired knowledge and skills, as well as additional training resources.

Related controls and activities: AT-02, AT-03.

Enhancements: None.

References:

- [TBS Policy on Service and Digital](#)
- [TBS Directive on Service and Digital](#)
- [TBS Guideline on Service and Digital](#)

PM-14 Testing, training, and monitoring

Activity:

- A. Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems
 1. are developed and maintained
 2. continue to be executed
- B. Review testing, training, and monitoring plans for consistency with the organizational security and privacy risk management strategy and organization-wide priorities for risk response actions

Discussion: A process for organization-wide security and privacy testing, training, and monitoring helps ensure that organizations provide oversight for testing, training, and monitoring activities and that those activities are coordinated. With the growing importance of continuous monitoring programs, the implementation of information security and privacy across the 3 levels of the risk management hierarchy and the widespread use of common controls, organizations coordinate and consolidate the testing and monitoring activities that are routinely conducted as part of ongoing assessments supporting a variety of controls. Security and privacy training activities, while focused on individual systems and specific roles, require coordination across all organizational elements. Testing, training, and monitoring plans and activities are informed by current threat and vulnerability assessments.

Related controls and activities: AT-02, AT-03, CA-07, CP-04, IR-03, PM-12, SI-04.

Enhancements: None.

References:

- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [TBS Directive on Security Management, Appendix D: Mandatory Procedures for Business Continuity Management Control](#)
- [TBS Directive on Security Management, Appendix E: Mandatory Procedures for Information Management Security Control](#)
- [TBS Directive on Security Management, Appendix H: Mandatory Procedures for Security Awareness and Training Control](#)

PM-15 Security and privacy groups and associations

Activity: Establish and institutionalize contact with selected groups and associations within the security and privacy communities to:

- A. facilitate ongoing security and privacy education and training for organizational personnel

- B. maintain currency with recommended security and privacy practices, techniques, and technologies
- C. share current security and privacy information, including threats, vulnerabilities, and incidents

Discussion: Ongoing contact with security and privacy groups and associations is important in an environment of rapidly changing technologies and threats. Groups and associations include special interest groups, professional associations, forums, news groups, users' groups, and peer groups of security and privacy professionals in similar organizations. Organizations select security and privacy groups and associations based on mission and business functions. Organizations share threat, vulnerability, and incident information, as well as contextual insights, compliance techniques, and privacy problems consistent with applicable laws, Orders in Council, directives, policies, regulations, standards, and guidelines.

Related controls and activities: SA-11, SI-05.

Enhancements: None.

References: None.

PM-16 Threat awareness program

Control: Implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.

Discussion: Because of the constantly changing and increasing sophistication of adversaries, especially the advanced persistent threat (APT), it may be more likely that adversaries can successfully breach or compromise organizational systems. One of the best techniques to address this concern is for organizations to share threat information, including threat events (i.e., tactics, techniques, and procedures) that organizations have experienced, mitigations that organizations have found are effective against certain types of threats, and threat intelligence (i.e., indications and warnings about threats). Threat information sharing may be bilateral or multilateral. Bilateral threat sharing includes government-to-commercial and government-to-government cooperatives. Multilateral threat sharing includes organizations taking part in threat-sharing consortia. Threat information may require special agreements and protection, or it may be freely shared.

Related controls and activities: IR-04, PM-12.

Enhancements:

(01) Threat awareness program: Automated means for sharing threat intelligence

Employ automated mechanisms to maximize the effectiveness of sharing threat intelligence information.

Discussion: To maximize the effectiveness of monitoring, it is important to know what threat observables and indicators the sensors need to be searching for. By using well-established frameworks, services, and automated tools, organizations improve their ability to rapidly share and feed the relevant threat detection signatures into monitoring tools.

Related controls and activities: None.

References:

- [TBS Directive on Security Management, Appendix I: Standard on Security Event Reporting](#)
- [TBS Government of Canada Cyber Security Event Management Plan \(GC CSEMP\)](#)

PM-17 Protecting controlled information on outsourced external systems

Control:

- A. Establish policy and procedures to ensure that requirements for the protection of controlled information that is processed, stored, or transmitted on external systems, are implemented in accordance with applicable laws, Orders in Council, directives, policies, regulations, and standards

- B.** Review and update the policy and procedures [Assignment: organization-defined frequency]

Discussion: None.

GC discussion: Controlled information (CI) includes Protected A, Protected B and controlled goods information that is not classified. Protected information is defined by the TBS Directive on Security Management, Appendix J: Standard on Security Categorization along with the safeguarding and dissemination requirements for such information and is codified in the TBS Policy on Privacy Protection. The policy prescribes the specific use and conditions to be implemented in accordance with organizational procedures, including via its contracting processes. Chapter 6 of the PSPC Contract Security Manual is dedicated to the handling and safeguarding of information and assets and is used in conjunction with Annex C – Guidelines for safeguarding information and assets. Requirements related to information sharing agreements or arrangements are documented in TBS' Guidance on Preparing Information Sharing Agreements Involving Personal Information.

Related controls and activities: CA-06, PM-10.

Enhancements: None.

References:

- [TBS Directive on Security Management, Appendix J: Standard on Security Categorization](#)
- [TBS Policy on Privacy Protection](#)
- [PSPC Contract Security Manual, Chapter 6: Handling and safeguarding information and assets](#)
- [PSPC Contract Security Manual, Annex C: Guidelines for safeguarding information and assets](#)

PM-18 Privacy program plan

Activity:

- A.** Develop and disseminate an organization-wide privacy program plan that provides an overview of the organization's privacy program, and
1. includes a description of the structure of the service delivery program for privacy and the resources dedicated to the privacy program
 2. provides an overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements
 3. includes the role of the appropriate privacy senior official or executive, describes the formal delegation of authority from the Deputy Head, and identifies and assigns the roles of other privacy officials and staff and their responsibilities
 4. describes management commitment, compliance requirements, and the strategic goals and objectives of the privacy program
 5. reflects coordination among organizational entities responsible for the different aspects of privacy
 6. is approved by a senior official with responsibility and accountability for the privacy risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and Canada
- B.** Update the plan [Assignment: organization-defined frequency] and address changes in the application of federal privacy laws based on jurisprudence and policy and organizational changes and problems identified during plan implementation or privacy control assessments
- AA.** Ensure the privacy program plan is communicated and made available to personnel responsible for implementing the plan

Discussion: A privacy program plan is a formal document that provides an overview of an organization's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the appropriate privacy senior official or executive and other privacy officials and staff, the strategic goals and objectives of

the privacy program, and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks. Privacy program plans can be represented in single documents or compilations of documents.

The appropriate privacy senior official or executive is responsible for designating which privacy controls the organization will treat as program management, common, system-specific, and hybrid controls. Privacy program plans provide sufficient information about the privacy program management and common controls (including the specification of parameters and assignment and selection operations explicitly or by reference) to enable control implementations that are unambiguously compliant with the intent of the plans and a determination of the risk incurred if the plans are implemented as intended.

Program management controls are generally implemented at the organization level and are essential for managing the organization's privacy program. Program management controls are distinct from common, system-specific, and hybrid controls because program management controls are independent of any particular information system. Together, the privacy plans for individual systems and the organization-wide privacy program plan provide complete coverage for the privacy controls employed within the organization.

Common controls are documented in an appendix to the organization's privacy program plan unless the controls are included in a separate privacy plan for a system. The organization-wide privacy program plan indicates which separate privacy plans contain descriptions of privacy controls.

Related controls and activities: PM-08, PM-09, PM-19.

Enhancements: None.

References:

- [TBS Policy on Privacy Protection](#)
- [TBS Directive on Privacy Practices](#)
- [OPC Guidance document: Getting Accountability Right with a Privacy Management Program](#)
- [OPC Privacy Guide for Businesses](#)

PM-19 Privacy program leadership role

Control: Appoint an appropriate privacy senior official or executive with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the organization-wide privacy program.

Discussion: The privacy officer is an organizational official.

GC discussion: For GC departments and agencies—as defined by applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines—this official is appointed by the head of an institution as the appropriate privacy senior official or executive. Organizations may also refer to this appropriate privacy senior official or executive as the CPO. The appropriate privacy senior official or executive also has roles on the data governance committee (see PM-23) and the committee on data and information (see PM-24).

Related controls and activities: PM-18, PM-20, PM-23, PM-24, PM-27.

Enhancements: None.

References:

- [Privacy Act](#)
- [TBS Policy on Privacy Protection](#)
- [TBS Directive on Privacy Practices](#)

PM-20 Communication of key privacy services

Control: Maintain a central resource webpage on the organization's principal public website that serves as a central source of information about the organization's privacy services and that:

- A. ensures that the public has access to a list of programs and services that collect and use personal information via Info Source
- B. ensures that organizational privacy policies, practices and resources are published in the Annual Report to Parliament on the Administration of the *Privacy Act*
- C. communicates publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices
- AA. includes summaries of completed PIAs
- BB. includes direction to individuals about how to file a request to access their personal information, how to file a formal records correction and how to file a formal complaint, if they choose to do so

Discussion: None.

GC discussion: For federal departments and agencies, the central webpage with respect to privacy legislation is located at <https://laws-lois.justice.gc.ca/>. Individual federal departments and agencies typically include contact information for CPO, summaries of PIAs, publications such as the Annual Report to Parliament on the Administration of the *Privacy Act*, program activity summaries such as Info Source, and instructions for individuals seeking to file requests to access or correct their personal information as well as complaint procedures.

Related controls and activities: AC-03, PM-19, PT-05, PT-06, PT-07, RA-08.

Enhancements:

(01) **Communication of key privacy services: Privacy policies on websites, applications, and digital services**

Develop and post privacy policies on all external-facing websites, mobile applications, and other digital services, if the privacy of websites visitors could be affected. Ensure that policies:

- a. are written in plain language and organized in a way that is easy to understand and navigate
- b. provide information needed by the public to make an informed decision about whether and how to interact with the organization
- c. are updated whenever the organization makes a substantive change to the practices it describes and includes a time/date stamp to inform the public of the date of the most recent changes

Discussion: Organizations post privacy policies on all external-facing websites, mobile applications, and other digital services if the privacy of website visitors could be affected. Organizations post a link to the relevant privacy policy on any known, major entry points to the website, application, or digital service. Organizations may be subject to applicable laws, directives, regulations, or policies that require the provision of specific information to the public. Organizational personnel consult with the appropriate privacy senior official or executive and legal counsel regarding such requirements.

Related controls and activities: None.

References:

- [Privacy Act](#)
- [TBS Policy on Privacy Protection](#)

PM-21 Maintain a record of disclosures

Control:

- A. Establish procedures for and maintain a record of disclosures of, personal information, including the
 - 1. date and details of the disclosure
 - 2. position and address, or other contact information of the individual or organization to which the disclosure was made
- B. Keep a record of disclosures for the length of the time the personal information is maintained or as required by the organization's information management standards
- C. Make the record of disclosure available to the individual to whom the personal information relates, upon request, unless the disclosure meets the exemptions cited in the *Privacy Act*
- AA. Establish a contract, information sharing agreement or information sharing arrangement to document appropriate safeguards prior to any disclosure of personal information to another federal program or to another public or private sector entity

Discussion: The purpose of records of disclosures is to allow individuals to learn to whom their personal information has been disclosed, to provide a basis for subsequently advising recipients of any corrected or annotated personal information, and to provide an audit trail for subsequent reviews of organizational compliance with conditions for disclosures.

PIPEDA generally requires organizations to obtain an individual's consent before they disclose their personal information. Personal information is either allowed or prohibited to be disclosed depending on the purposes for doing so, as stated in subsection 5(3).

Organizations can use any system for keeping records of disclosures, if they can construct from such a system, a document listing of all disclosures along with the required information. Automated mechanisms can be used by organizations to determine when personal information is disclosed, including commercial services that provide notifications and alerts. Keeping records of disclosures may also be used to help organizations verify compliance with applicable privacy statutes and policies governing the disclosure or dissemination of information and dissemination restrictions.

GC discussion: For GC departments and agencies, keeping records of disclosures is required by applicable legislations, policies, and directives. Institutions should consult with their appropriate privacy senior official or executive, legal counsel and information management officials on this requirement and be aware of the statutory exceptions and TBS guidance relating to the provision.

Related controls and activities: AC-03, AU-02, PT-02.

Enhancements: None.

References:

- [TBS Policy on Privacy Protection](#)
- [TBS Directive on Privacy Practices](#)
- [Privacy Act](#)
- [Privacy Regulations SOR/83-508](#)
- [PIPEDA](#)
- [TBS Guidance on Preparing Information Sharing Agreements Involving Personal Information](#)

PM-22 Personal information quality management

Control: Develop and document organization-wide policies and procedures for:

- A. reviewing for the accuracy, relevance, timeliness, and completeness of personal information across the information lifecycle
- B. implementing records correction process that facilitates correcting or deleting inaccurate or outdated personal information
- C. implementing records correction process that facilitates disseminating notice of corrected personal information when the incorrect information has been disclosed previously
- AA. ensuring that collection procedures adhere to the requirements of applicable legislation
- BB. documenting any changes or modifications to the information, including the date and sources of the information change

Discussion: Personal information quality management includes steps that organizations take to confirm the accuracy and relevance of personal information throughout the information lifecycle. The personal information lifecycle includes the creation, collection, use, correction, retention, disclosure, and disposition of personal information.

Organizational policies and procedures for personal information quality management are important because inaccurate or outdated personal information maintained by organizations may cause problems for individuals. Organizations consider the quality of personal information involved in business functions where inaccurate information may result in adverse decisions or the denial of benefits and services, or where the disclosure of the information may cause stigmatization.

In certain circumstances, incorrect personal information can cause problems for individuals that outweigh the benefits of organizations maintaining the personal information. Organizations should consider creating policies and procedures for the removal of such personal information.

The appropriate privacy senior official or executive ensures that practical means and mechanisms exist and are accessible for individuals or their authorized representatives to seek the correction or deletion of personal information. Processes for correcting or deleting data are clearly defined and publicly available.

Organizations use discretion in determining whether data is to be deleted or corrected based on the scope of requests, the changes sought, and the impact of the changes. Additionally, processes include the provision of responses to individuals of decisions to deny requests for correction or deletion. The responses should include the reasons for the decisions, a means to record individual objections to the decisions, and a means to file a complaint with the OPC if the individual wishes to pursue the matter further.

Organizations notify individuals or their designated representatives when their personal information is corrected or deleted to provide transparency and confirm the completed action. Due to the complexity of data flows and storage, other entities may need to be informed of the correction or deletion. Notice supports the consistent correction and deletion of personal information across the data ecosystem.

GC discussion: Organizations have an obligation to ensure the accuracy of personal information used in a decision-making process. This obligation includes steps to confirm the accuracy of personal information throughout the information lifecycle. Subsection 6(2) of the *Privacy Act* requires a government institution to take all reasonable steps to ensure that the collected personal information is accurate, up-to-date and as complete as possible.

The Directive on Privacy Practices provides additional details such as collecting information directly from the individual unless the individual authorizes otherwise or for reasons permitted by subsection 5(1) of the *Privacy Act*; collecting information from reliable sources; and validating and verifying the information before using the information for a decision-making process, if appropriate. When validating the accuracy of personal information, identify the relevant PIB description the source or technique used, including any data matching, where appropriate.

Organizations ensure that individuals are given the opportunity, whenever possible, to correct inaccurate personal information before any decision is made that could have an impact on them. Organizational policies and procedures to ensure accuracy of personal information are important to ensure the integrity of any administrative decisions made using that information. Inaccurate information may result in adverse decisions or the denial of benefits and services.

Organizations need to balance the necessity of holding information versus the invasiveness to the individual. One aspect to consider is the impact of a potential compromise of the information. Organizations should work with Information Management officials to determine an appropriate retention schedule for the personal information.

Organizations publish retention standards in their PIBs to ensure transparency. When information is deleted in accordance with the retention standard, organizations may choose to inform individuals of the completed action.

Related controls and activities: PM-23, SI-18.

Enhancements: None.

References:

- [Privacy Act](#)
- [Privacy Regulations SOR/83-508](#)
- [TBS Directive on Privacy Practices](#)
- [TBS Directive on Personal Information Requests and Correction of Personal Information](#)
- [TBS Guidance on Preparing Information Sharing Agreements Involving Personal Information](#)

PM-23 Data governance committee

Activity: Establish a data governance committee consisting of [Assignment: organization-defined roles] with [Assignment: organization-defined responsibilities].

Discussion: A data governance committee can help ensure that the organization has coherent policies and the ability to balance the utility of data with security and privacy requirements. The data governance committee establishes policies, procedures, and standards that facilitate data governance so that data, including personal information, is effectively managed and maintained in accordance with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidance.

Responsibilities can include developing and implementing guidelines that support data modeling, quality, integrity, and the de-identification needs of personal information across the information lifecycle. The data governance committee may oversee the reviewing and approving of applications to release data outside of the organization, the archiving of applications and the released data, and post-release monitoring to ensure that the assumptions made as part of the data release continue to be valid.

The data governance committee may also oversee the use of data, including personal information, in technologies such as advanced analytics, automation and artificial intelligence, perform statistical analyses to identify and mitigate systemic bias in institutional systems and data, analyze the de-identification techniques to ensure ongoing effectiveness, and ensure appropriate accountability mechanisms are in place, updated, understood, and followed.

Members typically include the CIO, the CSO, and appropriate privacy senior official or executive such as a CPO.

Related controls and activities: AT-02, AT-03, PM-19, PM-22, PM-24, PT-07, SI-04, SI-19.

Enhancements: None.

References: None.

PM-24 Data integrity board

Activity: Establish a data integrity board to:

- A. review proposals to conduct or participate in a matching program
- B. conduct an annual review of all matching programs in which the organization has participated

Discussion: None.

GC discussion: A data integrity board is the board of senior officials designated by the head of a GC department or agency and is responsible for, among other things, reviewing the organization's proposals to conduct or participate in a matching program and conducting an annual review of all matching programs in which the agency has participated. As a general matter, a matching program is a computerized comparison of records subject to the *Privacy Act* or PIPEDA from 2 or more automated systems of records or an automated system of records and automated records maintained by a non-federal organization (or agent thereof).

GC departments and agencies can establish an assistant deputy minister committee on data and information (ADM CDI) to review proposals on all uses of data by the institution, up to and including automation, advanced analytics, and artificial intelligence. At a minimum, the ADM CDI includes the chief data officer (CDO), CIO, CSO, and the appropriate privacy senior official or executive.

Related controls and activities: AC-04, PM-19, PM-23, PT-02, PT-08.

Enhancements: None.

References:

- [TBS Guideline on Service and Digital](#)
- [Privacy Act](#)
- [PIPEDA](#)

PM-25 Minimization of personal information used in testing, training, and research

Control:

- A. Develop, document, and implement policies and procedures that address the use of personal information for internal testing, training, and research
- B. Limit or minimize the amount of personal information used for internal testing, training, and research purposes
- C. Authorize the use of personal information in internal testing, training, and research when the required result cannot be achieved without the use of the personal information
- D. Review and update policies and procedures [Assignment: organization-defined frequency]
- AA. Restrict the disclosure of datasets containing personal information to external contractors, wherever possible

Discussion: The use of personal information in testing, training, and research increases the risk of unauthorized uses and disclosures of such information. Organizations consult with the appropriate privacy senior official or executive and/or legal counsel to ensure that the use of personal information in testing, training, and research is compatible with the original purpose for which it was collected. When possible, organizations use placeholder (de-identified or anonymized) data to avoid exposure of personal information when conducting testing, training, and research. If the use of personal information cannot be avoided in these environments, then the testing, training or research environments become subject to the same control requirements as the original environment.

GC discussion: GC departments and agencies consult with the appropriate privacy senior official or executive and/or legal counsel to ensure that the use of personal information in testing, training, and research is compatible with the original purpose for which it was collected or permissible under subsection 8(2) of the *Privacy Act*. Information-sharing agreements for research and statistical purposes are provided for in subsection 8(2)(j) of the *Privacy Act*. For the use of personal information in training activities, organizations may rely on training as a consistent use of the information, in accordance with subsection 8(2)(a) of the *Privacy Act*.

When organizations collect personal information for the express purpose of research or program evaluation, institutions should ensure that the collected personal information is reflected in any privacy notice, PIAs, and PIBs relevant to the program.

Related controls and activities: PM-23, PT-03, SA-03, SA-08, SI-12.

Enhancements: None.

References:

- [TBS Directive on Privacy Practices, Appendix C: Standard on Privacy Impact Assessment](#)
- [Privacy Act](#)
- [PIPEDA](#)
- [TBS Privacy Implementation Notice 2020-03: Protecting privacy when releasing information about a small number of individuals](#)

PM-26 Complaint management

Control: Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational security and privacy practices that includes:

- mechanisms that are easy to use and readily accessible by the public
- all information necessary for successfully filing complaints
- tracking mechanisms to ensure all complaints received are reviewed and addressed within [Assignment: organization-defined time period]
- acknowledgment of receipt of complaints, concerns, or questions from individuals within [Assignment: organization-defined time period]
- response, with discretion, to complaints, concerns, or questions from individuals within [Assignment: organization-defined time period]

Discussion: Complaints, concerns, and questions from individuals can serve as valuable sources of input to organizations and ultimately improve operational models, uses of technology, data collection practices, and controls. Mechanisms that can be used by the public include telephone hotline, email, or web-based forms. The information necessary for successfully filing complaints includes contact information for the appropriate privacy senior official or executive or other official designated to receive complaints. Privacy complaints may also include personal information, which is handled in accordance with relevant policies and processes. Under certain circumstances, the OPC can initiate its own investigation or complaint.

GC discussion: GC departments and agencies are required to implement a process that acknowledges individuals' rights to file a complaint related to the collection, retention, or disposal of personal information; the use or disclosure of personal information; and their rights of access to their personal information. Organizations should inform individuals of their right to complain about the handling of their personal information, including both organization contacts and the OPC complaint resolution contact.

When informed of a formal privacy complaint and/or investigation by the OPC, organizations should be prepared to provide a clear description of the relevant facts and circumstances related to the complaint, copies of any documentation relevant to the matter under investigation, a clear statement of the organization's position concerning the allegations, and specifics of any action taken to date, or planned to be taken.

GC departments and agencies should review trends to assess opportunities to proactively improve privacy practices and report complaint volumes and trends in the organization's Annual Report to Parliament for the *Privacy Act*.

Related controls and activities: IR-07, IR-09, PM-22, SI-18.

Enhancements: None.

References:

- [TBS Policy on Privacy Protection](#)
- [TBS Directive on Privacy Practices](#)

- [TBS Directive on Personal Information Requests and Correction of Personal Information](#)
- [Privacy Act](#)
- [PIPEDA](#)

PM-27 Privacy reporting

Activity:

- A. Develop [Assignment: organization-defined privacy reports] and disseminate to
 1. [Assignment: organization-defined oversight bodies] to demonstrate accountability with statutory, regulatory, and policy privacy mandates
 2. [Assignment: organization-defined officials] and other personnel with responsibility for monitoring privacy program compliance
- B. Review and update privacy reports [Assignment: organization-defined frequency]
- AA. Federal departments and agencies are required to report details related to the administration of the *Privacy Act* to both Parliament and TBS, as per section 72 of the *Privacy Act*

Discussion: None.

GC discussion: Organizations promote accountability and transparency in organizational privacy operations through internal and external reporting. Reporting can also help organizations to determine progress in meeting privacy compliance requirements and privacy controls, compare performance across the federal government, discover vulnerabilities, identify gaps in policy and implementation, and identify models for success. TBS is responsible for the operational policies, directives, and guidelines relating to the *Privacy Act* and its regulations.

For GC departments and agencies, annual privacy reports are prepared by the head of each institution, reporting on the administration of the *Privacy Act*. The appropriate privacy senior official or executive consults with legal counsel, where appropriate, to ensure that organizations meet all applicable privacy reporting requirements.

The Privacy Commissioner of Canada is an Agent of Parliament with the duty of protecting and promoting privacy rights and is responsible for reporting annually to Parliament on activities. The Privacy Commissioner can also report at any time on any important matter within the scope of the Commissioner's powers, duties and functions.

Related controls and activities: IR-09, PM-19.

Enhancements: None.

References:

- [TBS Policy on Privacy Protection](#)
- [TBS Directive on Privacy Practices](#)
- [Privacy Act](#)

PM-28 Risk framing

Activity:

- A. Identify and document
 1. assumptions affecting risk assessments, risk responses, and risk monitoring
 2. constraints affecting risk assessments, risk responses, and risk monitoring
 3. priorities and trade-offs considered by the organization for managing risk
 4. organizational risk tolerance

- B. Distribute the results of risk framing activities to [Assignment: organization-defined personnel]
- C. Review and update risk framing considerations [Assignment: organization-defined frequency]

Discussion: Risk framing is most effective when conducted at the organization level and in consultation with stakeholders throughout the organization including mission, business, and system owners. The assumptions, constraints, risk tolerance, priorities, and trade-offs identified as part of the risk framing process inform the risk management strategy, which in turn informs the conduct of risk assessment, risk response, and risk monitoring activities. Risk framing results are shared with organizational personnel, including mission and business owners, information owners or stewards, system owners, authorizing officials, the senior agency information security officer, the appropriate privacy senior official or executive, and the senior accountable official for risk management.

Related controls and activities: CA-07, PM-09, RA-03, RA-07.

Enhancements: None.

References:

- [TBS Framework for the Management of Risk](#)
- [TBS Guide to Integrated Risk Management](#)
- [CSE-RCMP Harmonized Threat and Risk Assessment Methodology \(TRA-1\)](#)

PM-29 Risk management program leadership roles

Control:

- A. Appoint a senior accountable official for risk management to align organizational information security and privacy management processes with strategic, operational, and budgetary planning processes
- B. Establish a risk executive (function) to view and analyze risk from an organization-wide perspective and ensure management of risk is consistent across the organization

Discussion: The senior accountable official for risk management leads the risk executive (function) in organization-wide risk management activities.

Related controls and activities: PM-02, PM-19.

Enhancements: None.

References:

- [TBS Framework for the Management of Risk](#)
- [TBS Guide to Integrated Risk Management](#)

PM-30 Supply chain risk management strategy

Activity:

- A. Develop an organization-wide strategy for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services
- B. Implement the supply chain risk management strategy consistently across the organization
- C. Review and update the supply chain risk management strategy on [Assignment: organization-defined frequency] or as required, to address organizational changes

Discussion: An organization-wide supply chain risk management strategy includes an unambiguous expression of the supply chain risk appetite and tolerance for the organization, acceptable supply chain risk mitigation strategies or controls, a

process for consistently evaluating and monitoring supply chain risk, approaches for implementing and communicating the supply chain risk management strategy, and the associated roles and responsibilities.

Supply chain risk management includes considerations of the security and privacy risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services. The supply chain risk management strategy can be incorporated into the organization's overarching risk management strategy and can guide and inform supply chain policies and system-level supply chain risk management plans.

In addition, the use of a risk executive function can facilitate a consistent, organization-wide application of the supply chain risk management strategy. The supply chain risk management strategy is implemented at the organization and mission/business levels, whereas the supply chain risk management plan (see SR-02) is implemented at the system level.

Related controls and activities: CM-10, PM-09, SR-01, SR-02, SR-03, SR-04, SR-05, SR-06, SR-07, SR-08, SR-09, SR-11.

Enhancements:

(01) **Supply chain risk management strategy: Suppliers of critical or mission-essential items**

Identify, prioritize, and assess suppliers of critical or mission-essential technologies, products, and services.

Discussion: The identification and prioritization of suppliers of critical or mission-essential technologies, products, and services is paramount to the mission/business success of organizations. The assessment of suppliers is conducted using supplier reviews (see SR-06) and supply chain risk assessment processes (see RA-03(01)). An analysis of supply chain risk can help an organization identify systems or components for which additional supply chain risk mitigations are required.

Related controls and activities: RA-03, SR-06.

References:

- [Cyber supply chain: An approach to assessing risk \(ITSAP.10.070\)](#)
- [Supply chain security for small and medium-sized organizations \(ITSAP.00.070\)](#)
- [Public Safety Canada Risk Management Guide for Critical Infrastructure Sectors](#)
- [ISO 27036-1 Cybersecurity – Supplier relationships—Part 1: Overview and concepts](#)
- [ISO 27036-2 Cybersecurity – Supplier relationships—Part 2: Requirements](#)
- [ISO 20243-1 Information technology – Open Trusted Technology Provider™ Standard \(O-TTPS\)—Part 1: Requirements and recommendations for mitigating maliciously tainted and counterfeit products](#)

PM-31 Continuous monitoring strategy

Activity: Develop an organization-wide continuous monitoring strategy and implement continuous monitoring programs that include:

- A. the establishment of the following organization-wide metrics to be monitored: [Assignment: organization-defined metrics]
- B. the establishment of [Assignment: organization-defined monitoring frequencies] and [Assignment: organization-defined assessment frequencies] for control effectiveness
- C. ongoing monitoring of organizationally-defined metrics in accordance with the continuous monitoring strategy
- D. correlation and analysis of information generated by control assessments and monitoring
- E. response actions to address results of the analysis of control assessment and monitoring information
- F. reporting on the security and privacy status of organizational systems to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency]

Discussion: Continuous monitoring at the organization level facilitates ongoing awareness of the security and privacy posture across the organization to support organizational risk management decisions. The terms “continuous” and

“ongoing” imply that organizations assess and monitor their controls and risks at a frequency sufficient to support risk-based decisions.

Different types of controls may require different monitoring frequencies. The results of continuous monitoring guide and inform risk response actions by organizations. Continuous monitoring programs allow organizations to maintain the authorizations of systems and common controls in highly dynamic environments of operation with changing mission and business needs, threats, vulnerabilities, and technologies.

Having access to security- and privacy-related information on a continuing basis through reports and dashboards gives organizational officials the capacity to make effective, timely, and informed risk management decisions, including ongoing authorization decisions. To further facilitate security and privacy risk management, organizations consider aligning organization-defined monitoring metrics with organizational risk tolerance as defined in the risk management strategy.

Monitoring requirements, including the need for monitoring, may be referenced in other controls and control enhancements such as, AC-02G, AC-02(07), AC-02(12)a, AC-02(07)b, AC-02(07)c, AC-17(01), AT-04A, AU-13, AU-13(01), AU-13(02), CA-07, CM-03F, CM-06D, CM-11C, IR-05, MA-02B, MA-03A, MA-04A, PE-03D, PE-06, PE-14B, PE-16, PE-20, PM-06, PM-23, PS-07E, SA-09C, SC-05(03)b, SC-07A, SC-07(24)b, SC-18B, SC-43B, SI-04.

Related controls and activities: AC-02, AC-06, AC-17, AT-04, AU-06, AU-13, CA-02, CA-05, CA-06, CA-07, CM-03, CM-04, CM-06, CM-11, IA-05, IR-05, MA-02, MA-03, MA-04, PE-03, PE-06, PE-14, PE-16, PE-20, PL-02, PM-04, PM-06, PM-09, PM-10, PM-12, PM-14, PM-23, PM-28, PS-07, PT-07, RA-03, RA-05, RA-07, SA-09, SA-11, SC-05, SC-07, SC-18, SC-38, SC-43, SI-03, SI-04, SI-12, SR-02, SR-04.

Enhancements: None.

References:

- [TBS Directive on Security Management](#)
- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [TBS Directive on Security Management, Appendix E: Mandatory Procedures for Information Management Security Control](#)

PM-32 Purposing

Control: Analyze [Assignment: organization-defined systems or systems components] supporting mission essential services or functions to ensure that the information resources are being used consistent with their intended purpose.

Discussion: Systems are designed to support a specific mission or business function. However, over time, systems and system components may be used to support services and functions that are outside of the scope of the intended mission or business functions. This can result in exposing information resources to unintended environments and uses that can significantly increase threat exposure. In doing so, the systems are more vulnerable to compromise, which can ultimately impact the services and functions for which they were intended. This is especially impactful for mission-essential services and functions. By analyzing resource use, organizations can identify such potential exposures.

Related controls and activities: CA-07, PL-02, RA-03, RA-09.

Enhancements: None.

References: None.

Family: Personnel security

The controls and activities in the Personnel security (PS) family support the procedures required to ensure that all personnel who have access to systems have the necessary authorizations as well as the appropriate security screening levels. They ensure that organizational information and systems are protected during and after personnel actions such as terminations and transfers.

PS-01 Personnel security policy and procedures

Activity:

- A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]
 - 1. [Selection (1 or more): Organization-level; Mission/business process-level; System-level] personnel security policy that
 - a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
 - b. is consistent with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines
 - 2. procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls
- B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the personnel security policy and procedures
- C. Review and update the current personnel security
 - 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]
 - 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]

Discussion: Personnel security policy and procedures for the controls in the PS family are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on their development.

In general, security and privacy program policies and procedures at the organization level are preferable and may remove the need for mission-level or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations.

Procedures can be established for security and privacy programs, for mission/business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.

Events that may precipitate an update to personnel security policy and procedures include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related controls and activities: PM-09, PS-08, SI-02, SI-12.

Enhancements: None.

References:

- [TBS Standard on Security Screening](#)
- [TBS Directive on Security Management, Appendix A: Mandatory Procedures for Security Screening Control](#)
- [TBS Directive on Security Management: Appendix F: Mandatory Procedures for Security in Contracts and Other Arrangements Control](#)
- [PSPC Contract Security Manual](#)

PS-02 Position security analysis

Control:

- Determine the security screening requirements of all organizational positions
- Establish screening criteria for individuals filling those positions
- Review and update position security screening requirement [Assignment: organization-defined frequency]

Discussion: Security screening requirements reflect TBS policy and guidance. Proper position designation is the foundation of an effective and consistent suitability and personnel security program. The criteria for determining security screening requirements are established in accordance with the Position Analysis Tool and guidance issued by TBS. The level of security screening and access permissions are determined by the duties to be performed, the sensitivity of information, assets, or facilities to be accessed, the level of authority or control exercised by the position, and the degree of injury that could result from compromise of sensitive information, assets, or facilities to be accessed. The results of the position security analysis determine what level of inquiries, verifications, and assessments are conducted for a position.

Related controls and activities: AC-05, AT-03, PE-02, PE-03, PL-02, PS-03, PS-06, SA-05, SA-21, SI-12.

Enhancements: None.

References:

- [TBS Standard on Security Screening](#)
- [TBS Standard on Security Screening, Appendix B: Security Screening Model and Criteria](#)

PS-03 Personnel screening

Control:

- Screen individuals prior to authorizing access to the system
- Rescreen individuals in accordance with [Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of rescreening]

Discussion: Personnel screening and rescreening activities reflect applicable laws, Orders in Council, directives, regulations, policies, standards, guidelines, and specific criteria established for the risk designations of assigned positions. Examples of personnel screening include background investigations and agency checks. Organizations may define different rescreening conditions and frequencies for personnel accessing systems based on types of information processed, stored, or transmitted by the systems.

Related controls and activities: AC-02, IA-04, MA-05, PE-02, PM-12, PS-02, PS-06, PS-07, SA-21.

Enhancements:

(01) Personnel screening: Classified information

Verify that individuals accessing a system that processes, stores, or transmits classified information are cleared and indoctrinated to the highest classification level of the information to which they have access on the system.

Discussion: None.

GC discussion: Classified information is the most sensitive information that the GC processes, stores, or transmits. It is imperative that individuals have the requisite security clearances and system access authorizations prior to gaining access to such information. Access authorizations are enforced by system access controls (see AC-03) and flow controls (see AC-04).

Related controls and activities: AC-03, AC-04.

(02) **Personnel screening: Formal indoctrination**

Verify that individuals accessing a system that processes, stores, or transmits types of classified information that require formal indoctrination are formally indoctrinated for all the relevant types of information to which they have access on the system.

Discussion: None.

GC discussion: Types of classified information that require formal indoctrination include Special Access Program (SAP), Restricted Data (RD), and SCI.

Related controls and activities: AC-03, AC-04.

(03) **Personnel screening: Information requiring special protective measures**

Verify that individuals accessing a system that processes, stores, or transmits information requiring special protection:

- a. have valid access authorizations that are demonstrated by assigned official government duties
- b. satisfy [Assignment: organization-defined additional personnel screening criteria]

Discussion: None.

GC discussion: Organizational information that requires special protection includes protected information. Personnel security criteria include position sensitivity background screening requirements.

Related controls and activities: None.

(04) **Personnel screening: Citizenship requirements**

Verify that individuals accessing a system that processes, stores, or transmits [Assignment: organization-defined information types] meet [Assignment: organization-defined citizenship requirements].

Discussion: None.

Related controls and activities: None.

References:

- [TBS Policy on Government Security](#)
- [PSPC Contract Security Manual](#)
- [TBS Directive on Security Management, Appendix A: Mandatory Procedures for Security Screening Control](#)
- [TBS Standard on Security Screening](#)
- [TBS Standard on Security Screening, Appendix B: Security Screening Model and Criteria](#)
- [TBS Operational Standard for the Security of Information Act](#)
- [Security of Information Act](#)

PS-04 Personnel termination

Control: Upon termination of individual employment:

- A. disable system access within [Assignment: organization-defined time period]
- B. terminate or revoke any authenticators and credentials associated with the individual

- C. conduct exit interviews that include a discussion of [Assignment: organization-defined information security topics]
- D. retrieve all security-related, organizational system-related property
- E. retain access to organizational information and systems formerly controlled by the terminated individual

Discussion: System property includes hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for system-related property. Security topics at exit interviews include reminding individuals of non-disclosure agreements and potential limitations on future employment. Exit interviews may not always be possible for some individuals, including in cases related to the unavailability of supervisors, illnesses, or job abandonment.

The timely execution of termination actions is essential for individuals who have been terminated for cause. In certain situations, organizations should consider disabling the system accounts of individuals who are being terminated prior to the individuals being notified.

GC discussion: Exit interviews are important for individuals with security clearances. CSOs or delegated officials, in consultation with human resources advisors, must develop procedures and ensure that debriefings and reclamations are scheduled and conducted as a component of the overall termination process. The Security Screening Certificate and Screening Form is used to record that termination procedures have been completed.

Related controls and activities: AC-02, IA-04, PE-02, PM-12, PS-06, PS-07.

Enhancements:

(01) Personnel termination: Post-employment requirements

- a. Notify terminated individuals of applicable, legally binding, post-employment requirements for the protection of organizational information
- b. Require terminated individuals to sign an acknowledgment of post-employment requirements as part of the organizational termination process

Discussion: None.

GC discussion: In accordance with the TBS standard, terminated individuals shall receive a formal debriefing to remind them of their continuing responsibilities to maintain the confidentiality of the sensitive information to which they have had access.

Related controls and activities: None.

(02) Personnel termination: Automated actions

Use [Assignment: organization-defined automated mechanisms] to [Selection (1 or more): notify [Assignment: organization-defined personnel or roles] of individual termination actions; disable access to system resources].

Discussion: In organizations with many employees, not all personnel who need to know about termination actions receive the appropriate notifications, or if such notifications are received, they may not occur in a timely manner.

Automated mechanisms can be used to send automatic alerts or notifications to organizational personnel or roles when individuals are terminated. Such automatic alerts or notifications can be conveyed in a variety of ways, including via telephone, email, text message, or websites. Automated mechanisms can also be employed to quickly and thoroughly disable access to system resources after an employee is terminated.

Related controls and activities: None.

(400) Personnel termination: Permanently bound to secrecy

Forward data on the form *Record of a Person in a Scheduled Department or Agency Under the Security of Information Act* (SOIA) to the Canadian Security Intelligence Service (CSIS).

Discussion: None.

GC discussion: As part of the departmental security exit process, if the departing member or employee has not already been entered into the CSIS central registry, the scheduled department should proceed by forwarding the data to CSIS. A departing person who was not previously designated as a person permanently bound to secrecy during the course of their employment can be designated as such upon termination, if it is assessed that it is in the interest of national security. If a decision is made to recommend to the deputy head that a former member or employee be designated, procedures for designation by notice shall be followed.

Related controls and activities: None.

References:

- [TBS Policy on Government Security](#)
- [TBS Standard on Security Screening](#)
- [TBS Standard on Security Screening, Appendix B: Security Screening Model and Criteria](#)
- [TBS Standard on Security Screening, Appendix F: Aftercare](#)
- [TBS Operational Standard for the Security of Information Act](#)
- [Security of Information Act \(SOIA\)](#)
- [TBS Directive on Security Management, Appendix A: Mandatory Procedures for Security Screening Control](#)
- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [TBS Directive on Security Management, Appendix C: Mandatory Procedures for Physical Security Control](#)

PS-05 Personnel transfer

Control:

- A. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization
- B. Initiate [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action]
- C. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer
- D. Notify [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period]

Discussion: Personnel transfer applies when reassignments or transfers of individuals are permanent or of such extended duration as to make the actions warranted. Organizations define actions appropriate for the types of reassignments or transfers, whether permanent or extended. Actions that may be required for personnel transfers or reassignments to other positions within organizations include returning old and issuing new keys, identification cards, and building passes; closing system accounts and establishing new accounts; changing system access authorizations (i.e., privileges); and providing access to official records to which individuals had access at previous work locations and in previous system accounts.

Related controls and activities: AC-02, IA-04, PE-02, PM-12, PS-04, PS-07.

Enhancements:

(400) Personnel transfer: Security clearance

- a. Accept the security status or clearance of the individual when the required one is at the same or lesser level previously granted
- b. Redo the security screening when
 - 1) the results are over 5 years old

- 2) there is evidence to suggest that the security screening was not done in accordance with the TBS Standard on Security Screening
- 3) there is a security waiver attached to the status or clearance
- 4) law enforcement inquiries or security assessments results have been removed from the individual's file
- 5) there is adverse information in the individual's file that may pose a security risk to the receiving department or agency

Discussion: None.

GC discussion: When enhanced screening is required for the new position, security screening will be reviewed accordingly. There may be a need to conduct additional inquiries, verification, or assessments to comply with the status or clearance requirements.

Related controls and activities: PS-03.

References:

- [TBS Standard on Security Screening](#)
- [TBS Standard on Security Screening, Appendix F: Aftercare](#)
- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [TBS Directive on Security Management, Appendix C: Mandatory Procedures for Physical Security Control](#)

PS-06 Access agreements

Control:

- A. Develop and document access agreements for organizational systems
- B. Review and update the access agreements [Assignment: organization-defined frequency]
- C. Verify that individuals requiring access to organizational information and systems
 1. sign appropriate access agreements prior to being granted access
 2. re-sign access agreements to maintain access to organizational systems when access agreements have been updated or [Assignment: organization-defined frequency]

Discussion: Access agreements include non-disclosure agreements, acceptable use agreements, rules of behaviour, and conflict-of-interest agreements. Signed access agreements include an acknowledgment that individuals have read, understand, and agree to abide by the constraints associated with organizational systems to which access is authorized. Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy.

Related controls and activities: AC-17, PE-02, PL-04, PS-02, PS-03, PS-06, PS-07, PS-08, SA-21, SI-12.

Enhancements:

(01) Access agreements: Information requiring special protection

Withdrawn: incorporated into PS-03.

(02) Access agreements: Classified information requiring special protection

Verify that access to classified information requiring special protection is granted only to individuals who:

- a. have a valid access authorization that is demonstrated by assigned official government duties
- b. satisfy associated personnel security criteria
- c. have read, understood, and signed a non-disclosure agreement

Discussion: None.

GC discussion: Classified information that requires special protection includes collateral information, SAP information, and SCI. Personnel security criteria reflect applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines.

Related controls and activities: None.

(03) **Access agreements: Post-employment requirements**

- a. Notify individuals of applicable, legally binding, post-employment requirements for protection of organizational information
- b. Require individuals to sign an acknowledgment of these requirements, if applicable, as part of granting initial access to covered information

Discussion: Organizations comply with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines regarding matters of post-employment requirements on terminated individuals.

Related controls and activities: PS-04.

References: [TBS Standard on Security Screening, Appendix F: Aftercare](#)

PS-07 External personnel security

Control:

- A. Establish personnel security requirements, including security roles and responsibilities for external providers
- B. Require external providers to comply with personnel security policies and procedures established by the organization
- C. Document personnel security requirements
- D. Require external providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within [Assignment: organization-defined time period]
- E. Monitor provider compliance with personnel security requirements
- F. The organization ensures security screening of private-sector organizations and individuals who have access to Protected and Classified information, assets, and facilities in accordance with the TBS Standard on Security Screening
- G. The organization explicitly defines government oversight and end-user roles and responsibilities relative to third-party-provided services in accordance with the TBS Directive on Security Management: Appendix F: Mandatory Procedures for Security in Contracts and Other Arrangements Control

Discussion: External provider refers to organizations other than the organization operating or acquiring the system. External providers include service bureaus, contractors, and other organizations that provide system development, IT services, testing or assessment services, outsourced applications, and network/security management. Organizations explicitly include personnel security requirements in acquisition-related documents. External providers may have personnel working at organizational facilities with credentials, badges, or system privileges issued by organizations.

Notifications of external personnel changes ensure the appropriate termination of privileges and credentials. Organizations define the transfers and terminations deemed reportable by security-related characteristics that include functions, roles, and the nature of credentials or privileges associated with transferred or terminated individuals.

Related controls and activities: AT-02, AT-03, MA-05, PE-03, PS-02, PS-03, PS-04, PS-05, PS-06, SA-05, SA-09, SA-21.

Enhancements: None.

References:

- [TBS Standard on Security Screening](#)
- [TBS Directive on Security Management: Appendix F: Mandatory Procedures for Security in Contracts and Other Arrangements Control](#)

PS-08 Personnel sanctions

Control:

- Employ a formal sanctions process for individuals who fail to comply with established information security and privacy policies and procedures
- Notify [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction

Discussion: None.

GC discussion: Organizational sanctions reflect applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines. Sanctions processes are described in access agreements and can be included as part of general personnel policies for organizations and/or specified in security and privacy policies. Organizations should consult with TBS regarding matters of employee sanctions.

Related controls and activities: PL-04, PM-12, PS-06, PT-01.

Enhancements: None.

References: [TBS Guidelines for Discipline](#)

PS-09 Position descriptions

Activity: Incorporate security and privacy roles and responsibilities into organizational position descriptions.

Discussion: Specifying security and privacy roles in individual organizational position descriptions helps clarify the security or privacy responsibilities associated with the roles and the role-based security and privacy training requirements for the roles.

Related controls and activities: None.

Enhancements: None.

References: [TBS Directive on Classification, Appendix B: Standard on Classification](#)

Family: Personal information handling and transparency

The controls and activities in the Personal information handling and transparency (PT) family support the confidentiality and integrity of personal information and its lawful handling as per Canadian privacy laws.

The controls in this family loosely correspond to the ones in NIST SP 800-53 Rev.5, but the privacy laws in Canada are significantly different from those in the United-States, hence the control and activity statements and discussions are not directly aligned.

PT-01 Personal information handling and transparency policy and procedures

Activity:

- A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]
 - 1. [Selection (1 or more): organization-level; mission/business process-level; system-level] privacy policy and personal information handling procedures that
 - a. addresses objectives, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance obligations
 - b. is consistent with applicable laws, jurisprudence, directives, regulations, policies, directives, standards, and guidelines
 - 2. procedures to facilitate the implementation of the privacy policy and procedures for personal information handling and the associated personal information handling and transparency controls
- B. Delegate responsibility to [Assignment: organization-defined official] to develop, document, and communicate personal information handling and transparency policy and procedures
- C. Review and update personal information handling and transparency
 - 1. privacy policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]
 - 2. personal information handling procedures, including transparency requirements [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]

Discussion: Privacy policies and personal information handling procedures, including transparency requirements, address the controls in the PT family that are implemented within systems or that are specific to program activities and to the organization. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of policies that document or affect personal information handling and procedures.

Security and privacy policies and procedures at the organization level are required and augment program activity or system-specific personal information handling procedures. The privacy policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations.

Procedures can be established at the organizational level, for program activities or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.

Events that may precipitate an update to an organization privacy policy and personal information handling and transparency procedures include assessment or audit findings, breaches, or changes in applicable laws, jurisprudence, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related controls and activities: PM-18, PM-20, PM-27, SI-02.

Enhancements: None.

References:

- [TBS Policy on Privacy Protection](#)
- [TBS Directive on Privacy Practices](#)

PT-02 Authority to collect and use personal information

Control:

- Determine and document the [Assignment: organization-defined authority] that permits the [Assignment: organization-defined collection and use] of personal information
- Restrict the [Assignment: organization-defined collection and use] of personal information to only that which is authorized

Discussion: The collection and use of personal information is an operation or set of operations that the information system or organization performs with respect to personal information across the information lifecycle. Handling includes but is not limited to creation, collection, use, correction, modification, retention, disclosure, and disposal. Handling operations may also include accessing, logging, creating/generating, and transforming, as well as statistical and analysis techniques, such as data mining and advanced analytics. Handling is commonly required by service suppliers to provide the service.

Organizations take steps to ensure that personal information is only handled for authorized purposes, including training organizational personnel on the authorized handling of personal information and monitoring and auditing organizational use of personal information.

GC discussion: Federal institutions are subject to laws or Orders in Council that provide the institution's authority to establish program activities that collect and use personal information. Institutions must handle the personal information under their control in accordance with the requirements of the *Privacy Act* and related TBS policies and directives.

Appropriate privacy senior officials should consult with the appropriate privacy practitioner or executive and legal counsel regarding their authority and the appropriate handling requirements, particularly if the authorities are complex in nature. While handling of personal information is legally permissible, privacy risks may still arise.

PIAs, combined with other risk assessments, can identify the privacy impacts associated with the handling of personal information and support solutions to manage such risks. The Cyber Centre publication Organizational cyber security and privacy risk management activities (ITSP.10.036) provides an integrated approach to mitigating security and privacy risks through the system development lifecycle.

When handling personal information, federal institutions must follow the *Privacy Act*, its regulations, and related TBS policies and directives. Some organizations may also be subject to additional legislation that dictates handling requirements for personal information. With few exceptions, institutions must notify individuals of the purpose for collecting their information and how it will be used and disclosed. This notice should be given at the point of collection.

If personal information is used in a decision-making process or stored in a manner designated to be retrieved by the individual's identity, institutions should further document the personal information elements that are collected or created (including the legal authority), and how they may be disclosed in PIBs. In addition, these program activities must conduct a PIA, which will serve as an input to the risk assessment. Privacy risks should be identified before the start of the program or activity. A summary of the PIA must be posted online. Additional accountability and governance steps must be taken prior to sharing personal information or contracting out services that involve personal information such as information sharing agreements or arrangements, contracts, and memoranda of understanding.

Related controls and activities: AC-02, AC-03, CM-13, IR-09, PM-09, PM-19, PM-24, PT-01, PT-03, PT-05, PT-06, RA-03, RA-08, SI-12, SI-18.

Enhancements:

(01) Authority to collect and use personal information: Data tagging

Attach data tags containing [Assignment: organization-defined authorized handling] to [Assignment: organization-defined elements of personal information].

Discussion: Data tags support the tracking and enforcement of authorized handling by conveying the types of handling that are authorized, along with the relevant elements of personal information throughout the system. Data tags may also support the use of automated tools.

Related controls and activities: AC-16, CA-06, CM-12, PM-05, PM-22, PT-04, SC-16, SC-43, SI-10, SI-15, SI-19.

(02) Authority to collect and use personal information: Automation

Manage enforcement of the authorized handling of personal information using [Assignment: organization-defined automated mechanisms].

Discussion: Automated mechanisms augment verification that only authorized handling is occurring.

Related controls and activities: CA-06, CM-12, PM-05, PM-22, PT-04, SC-16, SC-43, SI-10, SI-15, SI-19.

References:

- [TBS Policy on Privacy Protection](#)
- [TBS Directive on Privacy Practices](#)
- [TBS Directive on Privacy Practices, Appendix C: Standard on Privacy Impact Assessment](#)
- [TBS Guidance on Preparing Information Sharing Agreements Involving Personal Information](#)
- Organizational cyber security and privacy risk management activities (ITSP.10.036)

PT-03 Personal information handling uses and disclosures

Control:

- A. Identify and document the [Assignment: organization-defined use(s) and disclosure(s)] associated with collections of personal information
- B. Describe the purpose(s) of collection in the privacy notices and policies of the program activity or organization
- C. Restrict the [Assignment: organization-defined use(s) and disclosure(s)] of personal information to only that which is compatible with the identified purpose(s) or permissible under the *Privacy Act*
- D. Monitor changes in handling personal information and implement [Assignment: organization-defined mechanisms] to ensure that any changes are made in accordance with [Assignment: identified legislative requirements]
- AA. Update the PIB and notify the OPC and TBS of the new use or disclosure

Discussion: Identifying and documenting the purpose of collection provides organizations with a basis for understanding how personal information may then be handled. The term “handling” refers to any process involving personal information in the information lifecycle, including collection, creation, correction, modification, use, retention, disclosure, and disposal. Identifying and documenting the primary purpose of collection, along with consistent uses or permissible secondary uses or disclosures, enables information custodians and operators of the system and individuals whose information is handled by the system to understand how the information will be used. This enables individuals to make informed decisions about their engagement with information systems and organizations and to manage their privacy interests.

Organizations should take steps to help ensure that personal information is used or disclosed only for the identified purpose. Organizational personnel should receive training and the organizational handling of personal information should be monitored and audited.

GC discussion: Once the primary purpose of collection has been identified, the purpose is described in the activity or service privacy notices, policies, and any related privacy compliance documentation, including PIAs, PIBs, PIPEDA or *Privacy Act* requirements, and applicable legislation.

Organizations must monitor for changes in personal information handling. Organizational personnel should consult with the appropriate privacy senior official or executive and legal counsel to ensure that any new uses or disclosures that arise are compatible with the purpose for which the information was collected and are consistent with that purpose or a permissible use or disclosure in accordance with the *Privacy Act*. If the use or disclosure is not permissible, consent may be required.

Related controls and activities: AC-02, AC-03, AT-03, CM-13, IR-09, PM-09, PM-25, PT-02, PT-05, PT-06, PT-07, RA-08, SC-43, SI-12, SI-18.

Enhancements:

(01) **Personal information handling uses and disclosures: Data tagging**

Attach data tags containing the following purposes to [Assignment: organization-defined elements of personal information]: [Assignment: organization-defined handling purposes].

Discussion: Data tags support the tracking of handling purposes by conveying the purposes along with the relevant elements of personal information throughout the system. By conveying the handling purposes in a data tag along with the personal information as the information transits a system, a system owner or operator can identify whether a change in handling would be compatible with the identified and documented purposes. Data tags may also support the use of automated tools.

Related controls and activities: CA-06, CM-12, PM-05, PM-22, SC-16, SC-43, SI-10, SI-15, SI-19.

(02) **Personal information handling uses and disclosures: Automation**

Track handling purposes of personal information using [Assignment: organization-defined automated mechanisms].

Discussion: Automated mechanisms augment tracking of the handling purposes.

Related controls and activities: CA-06, CM-12, PM-05, PM-22, SC-16, SC-43, SI-10, SI-15, SI-19.

References:

- [Privacy Act](#)
- [TBS Policy on Privacy Protection](#)
- [TBS Directive on Privacy Practices](#)
- [TBS Directive on Privacy Practices, Appendix C: Standard on Privacy Impact Assessment](#)

PT-04 Consent

Control:

- A. Ensure that consent is obtained in writing or is otherwise adequately documented, including information such as the date and time of consent
- B. In the federal government, implement [Assignment: organization-defined tools or mechanisms] for individuals to provide informed consent to the secondary uses or indirect collection of their personal information. Consent must include
 1. the purpose of the consent
 2. the specific personal information elements involved
 3. in the case of indirect collection, the sources that will be asked to provide the information, as well as the reason for making the collection indirectly

4. uses or disclosures that are not consistent with the original purpose of the collection and for which consent is being sought
 5. any consequences that may result from withholding consent
 6. any alternatives to providing consent
- C. In the private sector, implement [Assignment: organization-defined tools or mechanisms] for individuals to provide meaningful consent to the collection, use and disclosure of their personal information

Discussion: Organizations should also consider any demographic or contextual factors that may influence the understanding or behaviour of individuals with respect to the use of their personal information by the organization. When soliciting consent from individuals, organizations should consider the appropriate mechanism for obtaining consent, including the type of consent (e.g., opt-in, opt-out), how to properly authenticate and identity-proof individuals, and how to obtain consent through electronic means.

Consent should require a positive action on behalf of the individual and should not be considered implied. In addition, organizations must consider providing a mechanism for individuals to revoke consent once it has been provided, as appropriate. In the event that consent is revoked, individuals may be entitled to assurance that their personal information has been deleted from the collection database. Organizations should consider usability factors, such as using plain language and avoiding technical jargon, to help individuals understand the risks being accepted when providing consent.

Private-sector organizations are required to obtain meaningful consent for the collection, use, and disclosure of personal information. Consent is considered meaningful when individuals are provided with clear information explaining what organizations are doing with their information. An organization must identify and document the purposes for which it seeks to collect personal information at or before the time of collection. There may be exceptions where consent is not required.

GC discussion: While consent is appropriate in the private sector, it is only required in the GC if personal information will be used for a secondary purpose or may be appropriate if information will be collected indirectly. Federal institutions only require that the personal information collected has a direct connection to an operating program or service, commonly referred to as requiring legislative authority. The original use of personal information is the purpose that was communicated to the individual when the personal information was collected and is directly related to an operating program or activity of the institution. A use of the information that is not consistent with the original purpose is considered to be a secondary purpose.

Consent for secondary uses allows individuals to control the circumstances in which their personal information can be used. Consent may be required by applicable laws, directives, regulations, policies, standards, or guidelines. When selecting consent as a control, organizations should consider whether individuals have the capacity to provide informed consent.

Before collecting personal information, federal government organizations should make sure that they have parliamentary authority for the program or activity for which the information will be collected. Obtaining an individual's consent for the collection or use of personal information does not replace or establish authority for the collection of that information.

Related controls and activities: AC-16, PT-02, PT-05.

Enhancements:

(01) **Consent: Tailored consent Government of Canada**

Provide [Assignment: organization-defined mechanisms] to allow individuals to tailor handling permissions to selected elements of personal information.

Discussion: None.

GC discussion: Not all secondary uses will require all of the personal information that was collected for the primary purpose. In such cases, tailored consent should be considered. Organizations should inform individuals of their personal information that will be applied to the secondary use. For example, collecting the name, contact information, and financial information for a primary purpose and a secondary use of the name and contact information for proactive communication would require tailored consent. More tailored consent may help reduce

privacy risk, increase individual satisfaction, and avoid adverse behaviours, such as abandonment of the product or service.

Related controls and activities: PT-02.

(02) **Consent: Timely consent**

Present [Assignment: organization-defined consent mechanisms] to individuals at [Assignment: organization-defined frequency] and in conjunction with [Assignment: organization-defined personal information handling].

Discussion: Timely consent enables individuals to understand how their personal information will be handled at the time or in conjunction with specific types of data handling when such participation may be most useful to the individual. Individual assumptions about how personal information is being processed might not be accurate or reliable if time has passed since the individual last gave consent or if the type of handling creates significant privacy risk. Organizations should use discretion to determine when to request consent and may use supporting information on demographics, focus groups, or surveys to learn more about individuals' privacy interests and concerns.

Related controls and activities: PT-02.

(03) **Consent: Revocation**

Implement [Assignment: organization-defined tools or mechanisms] for individuals to revoke consent to the handling of their personal information.

Discussion: Revocation of consent enables individuals to exercise control over their initial consent decision when circumstances change. Organizations should consider usability factors in enabling easy-to-use revocation capabilities.

Related controls and activities: PT-02.

(400) **Consent: Tailored consent private sector**

Provide [Assignment: organization-defined mechanisms] to allow individuals to tailor handling permissions to selected elements of personal information.

Discussion: While some handling of personal information may be necessary for the basic functionality of the product or service, other handling may not be necessary. In such cases, tailored consent should be considered. Organizations should inform individuals of their personal information that will be used for the secondary use. Tailored consent allows individuals to select how personal information elements may be handled. More tailored consent may help reduce privacy risk, increase individual satisfaction, and avoid adverse behaviours, such as abandonment of the product or service.

Related controls and activities: PT-02.

References:

- [TBS Directive on Privacy Practices](#)
- [Privacy Act](#)
- [PIPEDA](#)

PT-05 Privacy notice

Control: Provide notice to individuals about the collection of their personal information that includes:

- A. the legal authority for the collection of personal information
- B. any legal or administrative consequences of refusing to provide the personal information
- C. the rights of access to, correction, and protection of personal information
- D. a warning that system usage may be monitored, recorded, and subject to audit and includes

1. a statement explaining the regular monitoring practices of electronic networks
 2. a statement that electronic networks will be monitored for work-related purposes
 3. a statement that special monitoring may be permitted without notice in instances where illegal or other unacceptable use is suspected
- E. an explanation of how the information will be used
- F. the right to file a complaint with the Privacy Commissioner of Canada regarding the institution's handling of the individual's personal information
- G. the relevant PIB reference, if applicable

Discussion: None.

GC discussion: Privacy notices ensure individuals are informed about how their personal information is being collected or used by the organization. Organizations should use privacy notices to inform individuals about how, under what authority, and for what purpose their personal information is processed, as well as other information such as the choices individuals might have with respect to that handling and other parties with whom information is shared. Laws, Orders in Council, directives, regulations, or policies may require that privacy notices include specific elements or be provided in specific formats.

GC personnel should consult with the appropriate privacy senior official or executive and legal counsel regarding when and where to provide privacy notices, as well as elements to include in privacy notices and required formats. In circumstances where laws or government-wide policies do not require privacy notices, organizational policies and determinations may require privacy notices and may serve as a source of the elements to include in privacy notices.

To help individuals understand how their information is being used, organizations should write materials in plain language and avoid technical jargon.

Related controls and activities: PM-20, PM-22, PT-02, PT-03, PT-04, PT-07, RA-03, SC-42, SI-18.

Enhancements:

(01) Privacy notice: Timely privacy notice statements

Present notice of personal information handling to individuals at the time that the individual provides personal information.

Discussion: None.

GC discussion: Privacy notice statements inform individuals of how organizations process their personal information at a time when such notices may be most useful to the individuals. Individual assumptions about how personal information will be used or disclosed might not be accurate or reliable if time has passed since the organization last presented notice or if the circumstances under which the individual was last provided notice have changed. Periodic communication of a privacy notice statement can remind individuals about uses or disclosures of their personal information. Organizations should use discretion to determine when to communicate privacy notice reminders and may use supporting information on user demographics, focus groups, or surveys to learn about users' privacy interests and concerns.

Related controls and activities: PM-21.

(02) Privacy notice: Privacy notice statements

Include privacy notice statements on forms that collect information that will be maintained in a PIB.

Discussion: None.

GC discussion: If a federal department or agency asks individuals to supply information, the department or agency is required to provide a privacy notice statement on the form used to collect the information. The department or agency provides a privacy notice statement in such circumstances, regardless of whether the information will be

collected on a paper or electronic form, on a website, on a mobile application, over the telephone, or through some other medium.

Privacy notice statements provide formal notice to individuals of the legislative authority under which the collection of the information is conducted; whether providing the information is mandatory or voluntary; the principal purpose(s) for which the information is to be used; the published consistent uses to which the information is subject; the effects on the individual, if any, of not providing all or any part of the information requested; and an appropriate citation and link to the relevant PIB.

Federal department and agency personnel should consult with the appropriate privacy senior official or executive and legal counsel regarding the notice provisions of the *Privacy Act*.

Related controls and activities: PT-06.

References:

- [TBS Policy on Service and Digital](#)
- [TBS Directive on Service and Digital](#)
- [Privacy Act](#)
- [TBS Directive on Privacy Practices](#)

PT-06 Personal information banks

Control: Program activities that collect personal information must register and publish a PIB if that information has been used, is being used, or is available for use for an administrative purpose or if it is organized or intended to be retrieved by the name of an individual or by an identifying number, symbol or other particular assigned to an individual. [Assignment: organization-defined roles or personnel] are responsible for:

- A. registering or submitting new or significantly modified PIBs in accordance with TBS Directive on Privacy Practices, using the Personal Information Bank Submission form provided by TBS
- B. publishing PIBs on the relevant institution's Info Source webpage and updating this information once a year
- C. keeping PIBs accurate, up-to-date, and scoped in accordance with policy

Discussion: None.

GC discussion: The *Privacy Act* requires that federal departments and agencies listed in Schedule III of the Act publish a collection of PIBs in their annual Info Source publication. Generally, a PIB is required when a GC department or agency collects personal information for an administrative purpose or if the personal information is retrievable by an individual's name, identifying number, symbol, or other identifier.

Institution-specific PIBs describe personal information collected in support of institution-specific programs or services. Standard PIBs describe information about members of the public, as well as current and former federal employees, contained in records created, collected, and maintained by most government institutions in support of common internal services. Central PIBs describe personal information that is held by one government department on behalf of other government departments. Finally, exempt banks, which are institution-specific, and their content can be withheld by the Head of the institution.

The PIB describes the legislative authority for the collection, the class of individuals affected, the personal information data elements collected, all uses of the information, consistent disclosures, retention expectations, and additional details about the system as described in TBS guidelines.

Related controls and activities: AC-03, PM-20, PT-02, PT-03, PT-04, PT-05.

Enhancements:**(01) Personal information banks: Consistent uses and disclosures**

Review all consistent uses published in the PIB at [Assignment: organization-defined frequency] to ensure continued accuracy, and to ensure that consistent uses continue to be compatible with the purpose for which the information was collected.

Discussion: None.

GC discussion: The *Privacy Act* requires federal departments and agencies to describe each consistent use of the records as documented in the PIB. A consistent use has a reasonable and direct connection to the original purpose(s) for which the information was obtained. Personal information, as referenced in a PIB, can be disclosed without the consent of the individual in specific circumstances. One such circumstance is a disclosure for a purpose for which the information was obtained or compiled by the institution for a use consistent with that purpose. There are other permissible disclosures as documented in the subsection 8(2) of the *Privacy Act*.

Related controls and activities: None.

(02) Personal information banks: Exempt banks

Review all PIBs that were designated as exempt banks under section 18 of the *Privacy Act* [Assignment: organization-defined frequency] to ensure they remain appropriate and necessary in accordance with law.

Discussion: None.

GC discussion: The *Privacy Act* includes provisions that allow federal departments and agencies to claim exemptions to TBS from certain requirements. A PIB qualifies for exemption when more than half of the information in each file contained in the bank qualifies for an exemption under section 21 or 22 of the *Privacy Act*. The described files consist predominantly of personal information that relates to international affairs, defence, and law enforcement and investigation. Exempt PIBs still require registration with TBS.

Related controls and activities: None.

References:

- [Privacy Act](#)
- [TBS Policy on Privacy Protection](#)
- [TBS Directive on Privacy Practices](#)

PT-07 Particularly sensitive personal information

Control: Apply [Assignment: organization-defined handling conditions] for particularly sensitive personal information.

Discussion: Organizations should apply any conditions or protections that may be necessary for particularly sensitive personal information. These conditions may be required by laws, Orders in Council, directives, regulations, policies, standards, or guidelines. The requirements may also come from the results of privacy risk assessments that factor in contextual changes that may result in an organizational determination that a particular category of personal information is particularly sensitive or raises particular privacy risks. Organizations should consult with the appropriate privacy senior official or executive and legal counsel regarding any protections that may be necessary.

Related controls and activities: IR-09, PT-02, PT-03, PT-05, PT-06, RA-03.

Enhancements:**(01) Particularly sensitive personal information: Social insurance numbers**

When a program or activity collects, uses, or discloses social insurance numbers (SINs):

- ensure there is express authority for the collection and use of the SIN

- b. provide notice, at the point of collection, regarding the authority to collect as well as the anticipated use or disclosures of the SIN
- c. ensure the collection and use of SIN is included in the associated PIB, if appropriate

Discussion: None.

GC discussion: GC policy establishes specific requirements for organizations' handling of some categories of particularly sensitive personal information such as SINs. The SIN is a confidential number that should not be used as identification or provided for non-governmental purposes. Organizations should take steps to eliminate unnecessary uses of SINs and other sensitive information and should observe any particular requirements that apply.

The collection and use of the SIN by government institutions should only be for the authorized and lawful purposes outlined in Appendix A of the TBS Directive on Social Insurance Number. The directive provides direction to government institutions on how the SIN can be collected, used, and disclosed. It also outlines the methods to establish policy authority for a new collection or new consistent use of the SIN.

Related controls and activities: IA-04.

(02) **Particularly sensitive personal information: Canadian Charter of Rights and Freedoms**

Restrict the handling of information describing how any individual exercises rights guaranteed by the Canadian Charter of Rights and Freedoms unless there is lawful authority or if it is within the scope of an authorized law-enforcement activity.

Discussion: None.

GC discussion: Organizations should exercise caution when considering the collection of data elements protected under the Canadian Charter of Rights and Freedoms to ensure there is lawful authority for the handling of that personal information. Organizations should consult with the appropriate privacy senior official or executive and legal counsel.

Related controls and activities: None.

(400) **Particularly sensitive personal information: Private sector**

When collecting, using, or disclosing particularly sensitive personal information, private sector organizations should:

- a. determine the form of consent to use, considering the sensitivity of information
- b. protect personal information with [Assignment: organization-defined tools or mechanisms] appropriate to the sensitivity of information

Discussion: Under PIPEDA, any personal information can be sensitive depending on the context. However, certain types of personal information will generally be considered sensitive because of the specific risks to individuals associated with the collection, use, or disclosure of these categories of information. Information that will generally be considered sensitive and require a higher degree of protection includes health and financial data, ethnic and racial origin, political opinions, genetic and biometric data, information about an individual's sex life or sexual orientation, and religious or philosophical beliefs.

Whether personal information is considered sensitive under PIPEDA will vary depending on the facts of each case. Context is important when determining whether personal information would be considered sensitive.

Related controls and activities: IA-04, PT-04.

References:

- [Privacy Act](#)
- [TBS Directive on Privacy Practices](#)
- [TBS Directive on Social Insurance Number](#)

- [OPC Interpretation Bulletin: Sensitive Information](#)
- [PIPEDA](#)
- [Canadian Charter of Rights and Freedoms](#)

PT-08 Data matching requirements

Control: When a program activity seeks to collect, use, or disclose personal information for the purpose of conducting a data matching activity:

- A. ensure the authority exists to collect, use, or disclose the personal information for the purpose of data matching
- B. develop and enter into an information sharing agreement or information sharing arrangement for the purpose of data matching
- C. verify that the [Selection (1): notice to the individual; consent obtained from the individual] identifies that the information will be used for data matching activities
- D. verify that the associated PIB identifies that the information will be used for data matching activities

Discussion: None.

GC discussion: Data matching is defined as an activity involving the comparison of personal information from different sources, including sources within the same government institution, for administrative or non-administrative purposes. The data-matching activity that is established can be systematic or recurring. The data-matching activity can also be conducted on a periodic basis when deemed necessary. Data matching includes the disclosure or sharing of personal information with another organization for data-matching purposes.

Related controls and activities: AC-21, PT-02, PT-03, PT-05, PT-06, PT-07, SI-18.

Enhancements: None.

References: [TBS Policy on Privacy Protection](#)

Family: Risk assessment

The controls and activities in the Risk assessment (RA) family deal with the periodic conduct of risk assessments, including PIAs, resulting from the operation of organizational systems and associated handling, storage, or transmission of data and information.

RA-01 Risk assessment policy and procedures

Activity:

- A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]
 - 1. [Selection (1 or more): organization-level; Mission/business process-level; System-level] risk assessment policy that
 - a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
 - b. is consistent with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines
 - 2. procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls
- B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the risk assessment policy and procedures
- C. Review and update the current risk assessment
 - 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]
 - 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]

Discussion: Risk assessment policy and procedures address the controls in the RA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of risk assessment policy and procedures.

Security and privacy program policies and procedures at the organization level are preferable in that they may remove the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or can be represented by multiple policies reflecting the complex nature of organizations.

Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.

Events that may precipitate an update to risk assessment policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, Orders in Council, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related controls and activities: PM-09, PS-08, SA-400, SI-02, SI-12.

Enhancements:

(400) Risk assessment policy and procedures: Privacy impact assessments

Develop a PIA process and associated procedures that:

- a. is established by Heads of GC institutions

- b. considers the responsibility within the institution for establishing PIBs
- c. is commensurate with the severity of potential injuries related to the privacy invasiveness of the institution's programs or activities
- d. ensures the PIA is completed by the appropriate privacy senior official or executive holding responsibility within the institution for new or substantially modified programs or activities

Discussion: None.

GC discussion: Following the establishment of the PIA by the Head of the institution, the appropriate privacy senior officials or executives are responsible for adhering to the process in RA-08 for the completion of the PIA.

Related controls and activities: RA-08.

References:

- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [CSE-RCMP Harmonized Threat and Risk Assessment Methodology \(TRA-1\)](#)
- [TBS Directive on Privacy Practices, Appendix C: Standard on Privacy Impact Assessment](#)

RA-02 Security categorization

Activity:

- A. Categorize the system and information it processes, stores, and transmits
- B. Document the security categorization results, including supporting rationale, in the security plan for the system
- C. Verify that the authorizing official or authorizing official's designated representative reviews and approves the security categorization decision

Discussion: Security categories describe the potential adverse impacts or negative consequences to organizational operations, organizational assets, and individuals if organizational information and systems are compromised through a loss of confidentiality, integrity, or availability. Security categorization is also a type of asset loss characterization in systems security engineering processes that is carried out throughout the system development lifecycle. Organizations can use privacy risk assessments or PIAs to better understand the potential adverse effects on individuals.

Security categorization processes facilitate the development of inventories of information assets and, along with CM-08, mappings to specific system components where information is handled, stored, or transmitted. The security categorization process is revisited throughout the system development lifecycle to ensure that the security categories remain accurate and relevant. Organizational cyber security and privacy risk management activities (ITSP.10.036) provides guidance on security categorization.

GC discussion: Organizations should conduct the security categorization process as an organization-wide activity with the direct involvement of chief information officers, senior officials in the department's security governance, appropriate privacy senior officials or executives, system owners, mission and business owners, and information owners or stewards. Organizations should consider the potential adverse impacts to other organizations and injury to the national interest or outside of the national interest.

Related controls and activities: CM-08, MP-04, PL-02, PL-10, PL-11, PM-07, RA-03, RA-05, RA-07, RA-08, SA-08, SA-400, SC-07, SC-38, SI-12.

Enhancements:

(01) Security categorization: Impact-level prioritization

Conduct an impact-level prioritization of organizational systems to obtain additional granularity on system impact levels.

Discussion: Organizations should apply the highest determined values to each system categorized in accordance with Organizational cyber security and privacy risk management activities (ITSP.10.036), resulting in systems designated as very low, low, medium, high, or very high impact. Impact-level prioritization of the system allows organizations to focus their investments related to security control selection and the tailoring of control baselines when responding to identified risks.

GC discussion: Impact-level prioritization can also be used to determine those systems that may be of heightened interest or value to adversaries or may represent a critical loss to the GC, sometimes described as high-value assets. For such high-value assets, organizations may be more focused on complexity, aggregation, and information exchanges.

Related controls and activities: None.

References:

- Organizational cyber security and privacy risk management activities (ITSP.10.036)
- [TBS Directive on Security Management, Appendix J: Standard on Security Categorization](#)
- [TBS Directive on Privacy Practices, Appendix C: Standard on Privacy Impact Assessment](#)

RA-03 Risk assessment

Activity:

- A. Conduct a risk assessment, including
 1. identifying threats to and vulnerabilities in the system
 2. determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it handles, stores, or transmits, and any related information
 3. determining the likelihood and impact of adverse effects on individuals arising from the handling of personal information
- B. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments
- C. Document risk assessment results in [Selection (1): security and privacy plans; risk assessment report; [Assignment: organization-defined document]]
- D. Review risk assessment results [Assignment: organization-defined frequency]
- E. Disseminate risk assessment results to [Assignment: organization-defined personnel or roles]
- F. Update the risk assessment [Assignment: organization-defined frequency] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system

Discussion: Risk assessments should consider threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and Canada. Risk assessments should also consider risk from external parties, including contractors who operate systems on behalf of the organization, individuals who access organizational systems, service providers, and outsourcing entities.

Organizations can conduct risk assessments at all 3 levels in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any stage in the system development lifecycle. Risk assessments can also be conducted at various steps in the risk management process, such as Organizational cyber security and privacy risk management activities (ITSP.10.036), including preparation, categorization, control selection and allocation, control implementation, control assessment, authorization, and control monitoring. Risk assessment is an ongoing activity carried out throughout the system development lifecycle.

Risk assessments can also address information related to the system, including system design, the intended use of the system, testing results, and supply chain-related information or artifacts. Risk assessments can play an important role in control selection processes, particularly during the application of tailoring guidance and in the earliest phases of capability determination.

Related controls and activities: CA-03, CA-06, CM-04, CM-13, CP-06, CP-07, IA-08, MA-05, PE-03, PE-08, PE-18, PL-02, PL-10, PL-11, PM-08, PM-09, PM-28, PT-02, PT-07, RA-02, RA-05, RA-07, SA-08, SA-09, SA-400, SC-38, SI-12.

Enhancements:

(01) Risk assessment: Supply chain risk assessment

- a. Assess supply chain risks associated with [Assignment: organization-defined systems, system components, and system services]
- b. Update the supply chain risk assessment [Assignment: organization-defined frequency], when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain

Discussion: Supply chain-related events include disruption, use of defective components, insertion of counterfeits, theft, malicious development practices, improper delivery practices, and insertion of malicious code. These events can have a significant impact on the confidentiality, integrity, or availability of a system and its information and, therefore, can also adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and Canada. The supply chain-related events may be unintentional or malicious and can occur at any point during the system lifecycle. An analysis of supply chain risk can help an organization identify systems or components for which additional supply chain risk mitigations are required.

Related controls and activities: RA-02, RA-09, PM-17, PM-30, SR-02.

(02) Risk assessment: Use of all-source intelligence

Use all-source intelligence to assist in the analysis of risk.

Discussion: Organizations should employ all-source intelligence to inform engineering, acquisition, and risk management decisions.

All-source intelligence consists of information derived from all available sources, including publicly available or open-source information, or any available corporate intelligence sources. All-source intelligence is used to analyze the risk of vulnerabilities (both intentional and unintentional) from development, manufacturing, and delivery processes, people, and the environment. The risk analysis may be performed on suppliers at multiple tiers in the supply chain sufficient to manage risks. Organizations may develop agreements to share all-source intelligence information or resulting decisions with other organizations, as appropriate.

GC discussion: In the GC, all-source intelligence sources include the ones above, with the addition of human intelligence, signals intelligence, and imagery intelligence.

Related controls and activities: None.

(03) Risk assessment: Dynamic threat awareness

Determine the current cyber threat environment on an ongoing basis using [Assignment: organization-defined means].

Discussion: The threat awareness information that is gathered feeds into the organization's information security operations to ensure that procedures are updated in response to the changing threat environment. For example, at higher threat levels, organizations may change the privilege or authentication thresholds required to perform certain operations.

Related controls and activities: AT-02.

(04) Risk assessment: Predictive cyber analytics

Employ the following advanced automation and analytics capabilities to predict and identify risks to [Assignment: organization-defined systems or system components]: [Assignment: organization-defined advanced automation and analytics capabilities].

Discussion: A properly resourced SOC or computer incident response team (CIRT) may be overwhelmed by the volume of information generated by the proliferation of security tools and appliances unless it employs advanced automation and analytics to analyze the data. Advanced automation and analytics capabilities are typically supported by artificial intelligence (AI) concepts, including machine learning (ML). Examples include automated threat discovery and response (which includes broad-based collection, context-based analysis, and adaptive response capabilities), automated workflow operations, and machine-assisted decision tools.

Note, however, that sophisticated adversaries may be able to extract information related to analytic parameters and retrain the ML to classify malicious activity as benign. Accordingly, ML should be augmented by human monitoring to ensure that sophisticated adversaries are not able to conceal their activities.

Related controls and activities: None.

References:

- [CSE-RCMP Harmonized Threat and Risk Assessment Methodology \(TRA-1\)](#)
- [TBS Guide to Integrated Risk Management](#)
- Organizational cyber security and privacy risk management activities (ITSP.10.036)
- [Cyber supply chain: An approach to assessing risk \(ITSAP.10.070\)](#)
- [Supply chain security for small and medium-sized organizations \(ITSAP.00.070\)](#)
- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [TBS Directive on Security Management, Appendix J: Standard on Security Categorization](#)

RA-04 Risk assessment update

Withdrawn: Incorporated into RA-03.

RA-05 Vulnerability monitoring and scanning**Activity:**

- A. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported
- B. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for
 1. enumerating platforms, software flaws, and improper configurations
 2. formatting checklists and test procedures
 3. measuring vulnerability impact
- C. Analyze vulnerability scan reports and results from vulnerability monitoring
- D. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk
- E. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems

F. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned

Discussion: Security categorization of information and systems guides the frequency and comprehensiveness of vulnerability monitoring (including scans). Organizations should determine the required vulnerability monitoring for system components, ensuring that the potential sources of vulnerabilities—such as infrastructure components (e.g., switches, routers, guards, sensors), and networked printers, scanners, and copiers—are not overlooked.

The capability to readily update vulnerability monitoring tools as new vulnerabilities are discovered and announced and as new scanning methods are developed helps to ensure that new vulnerabilities are not missed by employed vulnerability monitoring tools. The vulnerability monitoring tool update process helps to ensure that potential vulnerabilities in the system are identified and addressed as quickly as possible. Vulnerability monitoring and analyses for custom software may require additional approaches, such as static analysis, dynamic analysis, binary analysis, or a hybrid of the 3 approaches. Organizations can use these analysis approaches in source code reviews and in a variety of tools, including web-based application scanners, static analysis tools, and binary analyzers.

Vulnerability monitoring includes scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for flow control mechanisms that are improperly configured or operating incorrectly.

Vulnerability monitoring may also include continuous vulnerability monitoring tools that use instrumentation to continuously analyze components. Instrumentation-based tools may improve accuracy and may be run throughout an organization without scanning. Vulnerability monitoring tools that facilitate interoperability include tools that are Security Content Automated Protocol (SCAP)-validated. Thus, organizations should consider using scanning tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that employ the Open Vulnerability Assessment Language (OVAL) to determine the presence of vulnerabilities.

Sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). Control assessments, such as red team exercises, provide additional sources of potential vulnerabilities for which to scan. Organizations should also consider using scanning tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS).

Vulnerability monitoring includes a channel and process for receiving reports from the public about security vulnerabilities. Vulnerability disclosure programs can be as simple as publishing a monitored email address or web form that can receive reports, including notifications that authorize good-faith research and disclosure of security vulnerabilities. Organizations generally expect that such research is happening with or without their authorization and can use public vulnerability disclosure channels to increase the likelihood that discovered vulnerabilities are reported directly to the organization for remediation.

Organizations may also use financial incentives (also known as bug bounties) to further encourage external security researchers to report discovered vulnerabilities. Bug bounty programs can be tailored to the organization's needs. Bounties can be operated indefinitely or over a defined period and can be offered to the general public or to a curated group. Organizations may run public and private bounties simultaneously and could choose to offer partially credentialed access to certain participants in order to evaluate security vulnerabilities from privileged vantage points.

Related controls and activities: CA-02, CA-07, CA-08, CM-02, CM-04, CM-06, CM-08, RA-02, RA-03, SA-11, SA-15, SC-38, SI-02, SI-03, SI-04, SI-07, SR-11.

Enhancements:

(01) Vulnerability monitoring and scanning: Update tool capability

Withdrawn: Incorporated into RA-05.

(02) Vulnerability monitoring and scanning: Update vulnerabilities to be scanned

Update the system vulnerabilities to be scanned [Selection (1 or more): [Assignment: organization-defined frequency]; prior to a new scan; when new vulnerabilities are identified and reported].

Discussion: Due to the complexity of modern software, systems, and other factors, new vulnerabilities are regularly discovered. It is important that newly discovered vulnerabilities are added to the list of vulnerabilities to be scanned to ensure that the organization can take steps to mitigate those vulnerabilities in a timely manner.

Related controls and activities: SI-05.

(03) **Vulnerability monitoring and scanning: Breadth and depth of coverage**

Define the breadth and depth of vulnerability scanning coverage.

Discussion: The breadth of vulnerability scanning coverage can be expressed as a percentage of components within the system, by the particular types of systems, by the criticality of systems, or by the number of vulnerabilities to be checked. Conversely, the depth of vulnerability scanning coverage can be expressed as the level of the system design that the organization intends to monitor (e.g., component, module, subsystem, element).

Organizations can determine the sufficiency of vulnerability scanning coverage with regard to its risk tolerance and other factors. Scanning tools and how the tools are configured may affect the depth and coverage. Multiple scanning tools may be needed to achieve the desired depth and coverage.

Related controls and activities: None.

(04) **Vulnerability monitoring and scanning: Discoverable information**

Determine information about the system that is discoverable and take [Assignment: organization-defined corrective actions].

Discussion: Discoverable information includes information that adversaries could obtain without compromising or breaching the system, for example, by collecting information that the system is exposing or by conducting extensive web searches. Corrective actions include notifying appropriate organizational personnel, removing designated information, or changing the system to make the designated information less relevant or attractive to adversaries. This enhancement excludes intentionally discoverable information that may be part of a decoy capability (e.g., honeypots, honeynets, or deception nets) deployed by the organization.

Related controls and activities: AU-13, SC-26.

(05) **Vulnerability monitoring and scanning: Privileged access**

Implement privileged access authorization to [Assignment: organization-defined system components] for [Assignment: organization-defined vulnerability scanning activities].

Discussion: In certain situations, vulnerability scanning may be more intrusive, or the system component that is the subject of the scanning may contain classified or protected information, such as personal information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and protects the sensitive nature of such scanning.

Related controls and activities: None.

(06) **Vulnerability monitoring and scanning: Automated trend analyses**

Compare the results of multiple vulnerability scans using [Assignment: organization-defined automated mechanisms].

Discussion: Using automated mechanisms to analyze multiple vulnerability scans over time can help determine trends in system vulnerabilities and identify patterns of attack.

Related controls and activities: None.

(07) **Vulnerability monitoring and scanning: Automated detection and notification of unauthorized components**

Withdrawn: Incorporated into CM-08.

(08) **Vulnerability monitoring and scanning: Review historic audit logs**

Review historic audit logs to determine if a vulnerability identified in a [Assignment: organization-defined system] has been previously exploited within an [Assignment: organization-defined time period].

Discussion: Reviewing historic audit logs to determine if a recently detected vulnerability in a system has been previously exploited by an adversary can provide important information for forensic analyses. Such analyses can help identify, for example, the extent of a previous intrusion, the tradecraft employed during the attack, organizational information exfiltrated or modified, mission or business capabilities affected, and the duration of the attack.

Related controls and activities: AU-06, AU-11.

(09) **Vulnerability monitoring and scanning: Penetration testing and analyses**

Withdrawn: Incorporated into CA-08.

(10) **Vulnerability monitoring and scanning: Correlate scanning information**

Correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability and multi-hop attack vectors.

Discussion: An attack vector is a path or means by which an adversary can gain access to a system to deliver malicious code or exfiltrate information. Organizations can use attack trees to show how hostile activities by adversaries interact and combine to produce adverse impacts or negative consequences to systems and organizations. Such information, together with correlated data from vulnerability scanning tools, can provide greater clarity regarding multi-vulnerability and multi-hop attack vectors.

The correlation of vulnerability scanning information is especially important when organizations are transitioning from older technologies to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols). During such transitions, some system components may inadvertently be unmanaged and could create opportunities for adversary exploitation.

Related controls and activities: None.

(11) **Vulnerability monitoring and scanning: Public disclosure program**

Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.

Discussion: The reporting channel should be publicly discoverable and contain clear language authorizing good-faith research and the disclosure of vulnerabilities to the organization. The organization should not condition its authorization on an expectation of indefinite non-disclosure to the public by the reporting entity but may request a specific timeframe to properly remediate the vulnerability.

Related controls and activities: None.

References:

- [TBS Policy on Government Security](#)
- [TBS Directive on Security Management](#)
- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [TBS Directive on Security Management, Appendix J: Standard on Security Categorization](#)
- [TBS Patch Management Guidance](#)
- [TBS Guideline on Service and Digital](#)
- [TBS Directive on Service and Digital, Appendix H: Standard on At-Risk Information Technology](#)
- [Top 10 IT security actions: No.2 patch operating systems and applications \(ITSM.10.096\)](#)

RA-06 Technical surveillance countermeasures survey

Control: Employ a technical surveillance countermeasures survey at [Assignment: organization-defined locations] [Selection (1 or more): [Assignment: organization-defined frequency]]; when the following events or indicators occur: [Assignment: organization-defined events or indicators]].

Discussion: A technical surveillance countermeasures survey is a service provided by qualified personnel to detect any presence of technical surveillance devices and hazards and to identify technical security weaknesses that could be used in the conduct of a technical penetration of the surveyed facility. Technical surveillance countermeasures surveys also provide evaluations of the technical security posture of organizations and facilities and include internal and external visual, electronic, and physical examinations of surveyed facilities. The surveys also provide useful input for risk assessments and information regarding organizational exposure to potential adversaries.

Related controls and activities: None.

Enhancements: None.

References: None.

RA-07 Risk response

Activity: Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.

Discussion: Organizations have many options for responding to risk, including mitigating risk by implementing new controls or strengthening existing controls, accepting risk with appropriate justification or rationale, sharing or transferring risk, or avoiding risk. The risk tolerance of the organization influences risk response decisions and actions. Risk response addresses the need to determine an appropriate response to risk before generating a plan of action and defining milestones. For example, the response may be to accept risk or reject risk, or it may be possible to mitigate the risk immediately so that a plan of action and milestones are not needed. However, if the risk response is to mitigate the risk, and the mitigation cannot be completed immediately, a plan of action and milestones are generated.

Related controls and activities: CA-05, IR-09, PM-04, PM-28, RA-02, RA-03, SR-02.

Enhancements: None.

References:

- [CSE-RCMP Harmonized Threat and Risk Assessment Methodology \(TRA-1\)](#)
- [TBS Guide to Integrated Risk Management](#)
- [TBS Framework for the Management of Risk](#)

RA-08 Privacy impact assessments

Activity: Conduct PIAs for systems, programs or other activities when:

- A. designing, developing or procuring means of handling personal information
- B. initiating a new collection of personal information
- AA. making substantial modifications to existing systems, programs or activities where personal information is handled

Discussion: To manage security risk, an injury assessment is required. Many systems will handle personal information from which injury can arise from privacy violations (as opposed to, for example, financial information, or intellectual property). In addition to the potential harm to the subject individuals, there may also be legal and regulatory repercussions to consider, or business and reputational harm that could occur. Therefore, a privacy-specific assessment of potential injuries is required to determine the security categorization of the intended system.

A PIA is an analysis of how personal information is handled to ensure that handling conforms to applicable privacy requirements and to determine the potential privacy injuries associated with an information system or activity. A PIA is both an analysis and a formal document that details the process and the outcome of the analysis.

Organizations should conduct and develop a PIA with sufficient clarity and specificity to demonstrate that the organization fully considered privacy and has incorporated privacy threats from the earliest stages of the organization's activity and throughout the information lifecycle.

To conduct a meaningful PIA, the organization's appropriate privacy senior official or executive may work closely with program managers, information custodians, information management practitioners, IT experts, security architects, counsel, and other relevant organization personnel. A PIA is not a time-restricted activity that is limited to a particular milestone or stage of the information system or personal information lifecycles. Rather, the privacy analysis continues throughout the system and personal information lifecycles. Accordingly, a PIA should be continuously revised and updated whenever there are changes to the IT or to the organization's practices, or when other factors alter the potential privacy injuries associated with the use of such IT.

After conducting the PIA, organizations may use this information to inform both security and privacy risk assessments. Organizations may also use other related processes that may have different names, including algorithmic impact assessments. A PIA can also inform the public about the organization's posture with respect to privacy.

GC discussion: For federal departments and agencies, PIAs are triggered under the TBS Directive on Privacy Practices. Federal departments are required to follow the steps detailed within this directive. Departments and agencies should consult their appropriate privacy senior official or executive and legal counsel about this requirement and should be aware of any statutory exceptions and TBS guidance relating to the provision. Prior to conducting privacy analysis, organizations need to complete a privacy checklist, following any existing TBS template, to determine whether a privacy protocol or a PIA is required.

GC organizations are required to conduct PIAs for programs or other activities when personal information is used for or is intended to be used as part of a decision-making process that directly affects the individual and when substantial modifications are made to existing programs or activities where personal information is used or intended to be used for an administrative purpose. However, GC organizations should remain cognizant of potential harm to individuals and consider completing a PIA even if the personal information held by the organization is not being used for decision-making or administrative purposes.

Approval of the PIA must be obtained from the executive or senior official who manages the program or activity and the official responsible for section 10 of the *Privacy Act*. Upon approval, the PIA needs to be transmitted to TBS and to the OPC. Organizations are required to create a mitigation plan for compliance gaps or privacy risks identified during the PIA process.

For multi-institutional PIAs, participating organizations should refer to the directive for specific requirements. GC organizations must share copies of the approved PIA and other relevant documentation with partners or other government institutions in a manner that respects security requirements as well as any other confidentiality or legal consideration.

Related controls and activities: CM-04, CM-09, CM-13, PT-02, PT-03, PT-05, RA-01, RA-02, RA-03, RA-07.

Enhancements: None.

References:

- [TBS Directive on Privacy Practices, Appendix C: Standard on Privacy Impact Assessment](#)
- [TBS Guideline on Service and Digital](#)

RA-09 Criticality analysis

Activity: Identify critical system components and functions by performing a criticality analysis for [Assignment: organization-defined systems, system components, or system services] at [Assignment: organization-defined decision points in the system development lifecycle].

Discussion: Not all system components, functions, or services necessarily require significant protections. For example, criticality analysis is a key tenet of supply chain risk management and informs the prioritization of protection activities. The identification of critical system components and functions considers applicable laws, Orders in Council, regulations, directives, policies, standards, system functionality requirements, system and component interfaces, and system and component dependencies.

Systems engineers conduct a functional decomposition of a system to identify mission-critical functions and components. The functional decomposition includes the identification of organizational missions supported by the system, decomposition into the specific functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions, including when the functions are shared by many components within and external to the system.

The operational environment of a system or a system component may impact the criticality, including the connections to and dependencies on cyber physical systems, devices, system-of-systems, and outsourced IT services. System components that allow unmediated access to critical system components or functions are considered critical due to the inherent vulnerabilities that such components create. Component and function criticality are assessed in terms of the impact of a component or function failure on the organizational missions that are supported by the system that contains the components and functions.

Criticality analysis is performed when an architecture or design is being developed, modified, or upgraded. If such analysis is performed early in the system development lifecycle, organizations may be able to modify the system design to reduce the critical nature of these components and functions, such as by adding redundancy or alternate paths into the system design.

Criticality analysis can also influence the protection measures required by development contractors. In addition to criticality analysis for systems, system components, and system services, criticality analysis of information is an important consideration. Such analysis is conducted as part of security categorization in RA-02.

Related controls and activities: CP-02, PL-02, PL-08, PL-11, PM-01, PM-11, RA-02, SA-08, SA-15, SA-20, SR-05.

Enhancements: None.

References:

- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [TBS Directive on Security Management, Appendix J: Standard on Security Categorization](#)
- System lifecycle cyber security and privacy risk management activities (ITSP.10.037)

RA-10 Threat hunting

Control:

- A. Establish and maintain a cyber threat hunting capability to
 1. search for indicators of compromise in organizational systems
 2. detect, track, and disrupt threats that evade existing controls
- B. Employ the threat hunting capability [Assignment: organization-defined frequency]

Discussion: Threat hunting is an active means of cyber defence, in contrast to traditional passive protection measures, such as firewalls, intrusion detection and prevention systems, quarantining malicious code in sandboxes, and SIEM technologies and systems.

Cyber threat hunting involves proactively searching organizational systems, networks, and infrastructure for advanced threats. The objective is to track and disrupt cyber adversaries as early as possible in the attack sequence and to measurably improve the speed and accuracy of organizational responses. Indications of compromise include unusual network traffic, unusual file changes, and the presence of malicious code.

Threat hunting teams leverage existing threat intelligence and may create new threat intelligence, which is shared with peer organizations, information sharing and analysis organizations (ISAOs), information sharing and analysis centres (ISACs), and relevant government departments and agencies.

Related controls and activities: CA-02, CA-07, CA-08, RA-03, RA-05, RA-06, SI-04.

Enhancements: None.

References:

- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
-

Family: System and services acquisition

The controls and activities in the System and services acquisition (SA) family deal with the contracting of products and services required to support the implementation and operation of organizational systems. They ensure that sufficient resources are allocated for the adequate protection of organizational systems, and they support system development lifecycle processes that incorporate security considerations.

SA-01 System and services acquisition policy and procedures

Activity:

- A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]
 - 1. [Selection (1 or more): Organization-level; Mission/business process-level; System-level] system and services acquisition policy that
 - a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
 - b. is consistent with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines
 - 2. procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls
- B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures
- C. Review and update the current system and services acquisition
 - 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]
 - 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]

Discussion: System and services acquisition policy and procedures address the controls in the SA family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of system and services acquisition policy and procedures.

In general, security and privacy program policies and procedures at the organization level are preferable and may remove the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations.

Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.

Events that may precipitate an update to system and services acquisition policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, Orders in Council, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related controls and activities: PM-09, PS-08, SA-08, SI-02, SI-12.

Enhancements: None.

References:

- [TBS Directive on Security Management](#)

- [TBS Directive on Security Management: Appendix F: Mandatory Procedures for Security in Contracts and Other Arrangements Control](#)
- [TBS Framework for the Management of Risk](#)
- [TBS Guide to Integrated Risk Management](#)
- [TBS Directive on Privacy Practices](#)
- [PSPC Contract Security Manual](#)
- [CSE-RCMP Harmonized Threat and Risk Assessment Methodology \(TRA-1\)](#)

SA-02 Allocation of resources

Control:

- Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning
- Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process
- Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation

Discussion: Resource allocation for information security and privacy includes funding for system and services acquisition, sustainment, and supply-chain-related risks throughout the system development lifecycle.

Related controls and activities: PL-07, PM-03, PM-11, SA-09, SR-03, SR-05.

Enhancements: None.

References:

- [TBS Policy on Government Security](#)
- [TBS Directive on Security Management](#)
- [TBS Directive on Privacy Practices](#)
- [TBS Guideline on Service and Digital](#)

SA-03 System development lifecycle

Activity:

- Acquire, develop, and manage the system using [Assignment: organization-defined system development lifecycle] that incorporates information security and privacy considerations
- Define and document information security and privacy roles and responsibilities throughout the system development lifecycle
- Identify individuals having information security and privacy roles and responsibilities
- Integrate the organizational information security and privacy risk management process into system development lifecycle activities

Discussion: A system development lifecycle process provides the foundation for the successful development, implementation, and operation of organizational systems. The integration of security and privacy considerations early in the system development lifecycle is a foundational principle of systems security engineering and privacy engineering. Applying the required controls within the system development lifecycle requires a basic understanding of information security and privacy, threats, vulnerabilities, adverse impacts, and risk to critical mission and business functions.

The security engineering principles in SA-08 help individuals properly design, code, and test systems and system components. Organizations include qualified personnel (e.g., senior officials in the department's security governance, appropriate privacy senior officials or executives, security and privacy architects, and security and privacy engineers) in system development lifecycle processes to ensure that established security and privacy requirements are incorporated into organizational systems. Role-based security and privacy training programs can ensure that individuals with key security and privacy roles and responsibilities have the experience, skills, and expertise to conduct assigned system development lifecycle activities.

The effective integration of security and privacy requirements into enterprise architecture also helps ensure that important security and privacy considerations are addressed throughout the system lifecycle and that those considerations are directly related to organizational mission and business processes. This process also facilitates the integration of the information security and privacy architectures into the enterprise architecture, consistent with the risk management strategy of the organization. Because the system development lifecycle involves multiple organizations (e.g., external suppliers, developers, integrators, service providers), acquisition and supply chain risk management functions and controls play significant roles in the effective management of the system during the lifecycle.

Related controls and activities: AT-03, PL-08, PM-07, SA-04, SA-05, SA-08, SA-11, SA-15, SA-17, SA-22, SA-400, SR-03, SR-04, SR-05, SR-09.

Enhancements:

(01) **System development lifecycle: Manage pre-production environment**

Protect system pre-production environments commensurate with risk throughout the system development lifecycle for the system, system component, or system service.

Discussion: The pre-production environment includes development, test, and integration environments. Criticality analysis and the application of controls on developers also contribute to a more secure system development environment.

Related controls and activities: CM-02, CM-04, RA-03, RA-09, SA-04.

(02) **System development lifecycle: Use of live or operational data**

- a. Approve, document, and control the use of live data in pre-production environments for the system, system component, or system service
- b. Protect pre-production environments for the system, system component, or system service at the same impact or classification level as any live data in use within the pre-production environments

Discussion: Live data is also referred to as operational data. The use of live or operational data in pre-production (i.e., development, test, and integration) environments can result in significant risks to organizations. In addition, the use of live data that is personal information in testing, research, and training increases the risk of unauthorized disclosure or misuse of such information. Therefore, it is important for the organization to manage any additional risks that may result from the use of live or operational data.

Organizations can minimize such risks by using test or dummy data during the design, development, and testing of systems, system components, and system services. Risk assessment techniques may be used to determine if the risk of using live or operational data is acceptable. The use of personal information for testing requires that individuals are informed about the use in advance.

GC discussion: When using personal information in testing activities, organizations may rely on testing as a consistent use of the information, in accordance with 8(2)(a) of the *Privacy Act*. For this to be acceptable, individuals must have been given notice about the use of their information for testing, at the point that the personal information was collected and, where appropriate, the associated PIBs need to reflect the use of the information for testing purposes. If individuals were not provided with notice at the point of collection, or if the use of the information for testing purposes is not listed as a consistent use in the associated PIB, program officials should

contact their privacy officials for advice about whether this would be considered a consistent use or a secondary use.

Related controls and activities: PM-25, RA-03.

(03) **System development lifecycle: Technology refresh**

Plan for and implement a technology refresh schedule for the system throughout the system development lifecycle.

Discussion: Technology refresh planning may encompass hardware, software, firmware, processes, personnel skill sets, suppliers, service providers, and facilities. The use of obsolete or nearing obsolete technology may increase the security and privacy risks associated with unsupported components, counterfeit or repurposed components, components unable to implement security or privacy requirements, slow or inoperable components, components from untrusted sources, inadvertent personnel error, or increased complexity. Technology refreshes typically occur during the operations and maintenance stage of the system development lifecycle.

Related controls and activities: MA-06.

References:

- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [TBS Directive on Service and Digital, Appendix H: Standard on At-Risk Information Technology](#)
- [TBS Guideline on Service and Digital](#)
- [TBS Government of Canada Enterprise Architecture Framework](#)

SA-04 Acquisition process

Control: Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (1 or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service:

- A. security and privacy functional requirements
- B. strength of mechanism requirements
- C. security and privacy assurance requirements
- D. controls needed to satisfy the security and privacy requirements
- E. security and privacy documentation requirements
- F. requirements for protecting security and privacy documentation
- G. a description of the system development environment and the environment in which the system is intended to operate
- H. the allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management
- I. acceptance criteria

Discussion: Security and privacy functional requirements are typically derived from the high-level security and privacy requirements described in SA-02. The derived requirements include security and privacy capabilities, functions, and mechanisms. Strength requirements associated with such capabilities, functions, and mechanisms include degree of correctness, completeness, resistance to tampering or bypass, and resistance to direct attack.

Assurance requirements can be specified in a statement of work as part of a contract and can include development processes, procedures, and methodologies, as well as the evidence from development and assessment activities that provide grounds for confidence that the required functionality is implemented and possesses the required strength of

mechanism. The Cyber Centre publication System lifecycle cyber security and privacy risk management activities (ITSP.10.037) describes the process of requirements engineering as part of the system development lifecycle.

Controls can be viewed as descriptions of the safeguards and protection capabilities appropriate for achieving the particular security and privacy objectives of the organization and for reflecting the security and privacy requirements of stakeholders. Controls are selected and implemented to satisfy system requirements and include developer and organizational responsibilities. Controls can include technical, administrative, privacy, and physical aspects. In some cases, the selection and implementation of a control may necessitate additional specification by the organization in the form of derived requirements or instantiated control parameter values. The derived requirements and control parameter values may be necessary to provide the appropriate level of implementation detail for controls within the system development lifecycle.

Security and privacy documentation requirements address all stages of the system development lifecycle. Documentation provides user and administrator guidance for the implementation and operation of controls. The level of detail required in such documentation is based on the security categorization or classification level of the system and the degree to which organizations depend on the capabilities, functions, or mechanisms to meet risk response expectations. Requirements can include mandated configuration settings that specify allowed functions, ports, protocols, and services. Acceptance criteria for systems, system components, and system services are defined in the same manner as the criteria for any organizational acquisition or procurement.

Organizations can determine other requirements that support security and operations, to include responsibilities for the organization and developer, and notification and timing requirements for support, maintenance and updates.

GC discussion: Functional requirements for the protection of personal information can be found in the PSPC Supply Manual, Chapter 1, Section 1.70 – Privacy in contracting. The TBS guidance document: Taking Privacy Into Account Before Making Contracting Decisions, presents additional information on the handling of personal information. Functional requirements include the contractual obligations for ownership of personal information, the maintenance of accuracy, privacy and integrity of personal information, limitations to the secondary use or disclosure without consent, disposition of records containing personal information, including returning the records back to the GC if required, acceptance of privacy audit possibilities, privacy breach and privacy complaint mechanisms, and legal requirements to disclose personal information.

Related controls and activities: CM-06, CM-08, PS-07, SA-03, SA-05, SA-08, SA-11, SA-15, SA-16, SA-17, SA-21, SA-400, SR-03, SR-05.

Enhancements:

(01) **Acquisition process: Functional properties of controls**

Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.

Discussion: Functional properties of security and privacy controls describe the functionality (i.e., security or privacy capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls.

Related controls and activities: None.

(02) **Acquisition process: Design and implementation information for controls**

Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: [Selection (1 or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design and implementation information]] at [Assignment: organization-defined level of detail].

Discussion: Organizations may require different levels of detail in the documentation for the design and implementation of controls in organizational systems, system components, or system services based on mission and business requirements, requirements for resiliency and robustness, and requirements for analysis and testing. Systems can be partitioned into multiple subsystems. Each subsystem within the system can contain one or more modules. The high-level design for the system is expressed in terms of subsystems and the interfaces between

subsystems providing security-relevant functionality. The low-level design for the system is expressed in terms of modules and the interfaces between modules providing security-relevant functionality. Design and implementation documentation can include manufacturer, version, serial number, verification hash signature, software libraries used, date of purchase or download, and the vendor or download source. Source code and hardware schematics are referred to as the implementation representation of the system.

Related controls and activities: None.

(03) Acquisition process: Development methods, techniques, and practices

Require the developer of the system, system component, or system service to demonstrate the use of a system development lifecycle process that includes:

- a. [Assignment: organization-defined systems engineering methods]
- b. [Selection (1 or more): [Assignment: organization-defined systems security engineering methods]; [Assignment: organization-defined privacy engineering methods]]
- c. [Assignment: organization-defined software development methods; testing, evaluation, assessment, verification, and validation methods; and quality control processes]

Discussion: Following a system development lifecycle that includes state-of-the-practice software development methods, systems engineering methods, systems security and privacy engineering methods, and quality control processes helps to reduce the number and severity of latent errors within systems, system components, and system services. Reducing the number and severity of such errors reduces the number of vulnerabilities in those systems, components, and services.

Transparency in the methods and techniques that developers select and implement for systems engineering, systems security and privacy engineering, software development, component and system assessments, and quality control processes provides an increased level of assurance in the security functionality of the system, system component, or system service being acquired.

Related controls and activities: None.

(04) Acquisition process: Assignment of components to systems

Withdrawn: Incorporated into CM-08(09).

(05) Acquisition process: System, component, and service configurations

Require the developer of the system, system component, or system service to:

- a. deliver the system, component, or service with [Assignment: organization-defined security configurations] implemented
- b. use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade

Discussion: Examples of security configurations include the Cyber Centre's Baseline security requirements for network security zones (ITSP.80.022), STIGs, and any limitations on functions, ports, protocols, and services. Security characteristics can include requiring that default passwords have been changed.

GC discussion: GC departments and agencies can also refer to the [GC System Management Configuration Requirements](#), as well as to the TBS Standard on Enterprise IT Service Common Configurations.

Related controls and activities: None.

(06) Acquisition process: Use of cyber security products

- a. Employ only government off-the-shelf or COTS cyber security and cyber security-enabled IT products that compose a Cyber Centre-approved solution to protect classified information when the networks used to transmit the information are at a lower classification level than the information being transmitted
- b. Ensure that these products have been evaluated or validated by the Cyber Centre or in accordance with Cyber Centre-approved procedures

Discussion: None.

GC discussion: COTS cyber security or cyber security-enabled IT products used to protect classified information by cryptographic means may be required to use Cyber Centre-approved key management. See Government of Canada Key Management Infrastructure (GC KMI) for more information (restricted to GC).

Related controls and activities: SC-08, SC-12, SC-13.

(07) **Acquisition process: Canadian Common Criteria Program - recognized protection profiles**

- a. Limit the use of commercially provided cyber security and cyber security-enabled IT products to those products that have been successfully evaluated against a Canadian Common Criteria Program (CCCP) recognized protection profile for a specific technology type, if such a profile exists
- b. If no CCCP-recognized protection profile exists for a specific technology type but a commercially provided IT product relies on cryptographic functionality to enforce its security policy, require that the cryptographic module is FIPS-validated or CCCP-recognized

Discussion: The Cyber Centre operates the CCCP to certify products. See the [Common Criteria Portal](#) for additional information on protection profiles. See the Cyber Centre's CMVP for additional information on FIPS-validated cryptographic modules.

Related controls and activities: IA-07, SC-12, SC-13.

(08) **Acquisition process: Continuous monitoring plan for controls**

Require the developer of the system, system component, or system service to produce a plan for continuous monitoring of control effectiveness that is consistent with the continuous monitoring program of the organization.

Discussion: The objective of continuous monitoring plans is to determine if the planned, required, and deployed controls within the system, system component, or system service continue to be effective over time based on the inevitable changes that occur.

Developer continuous monitoring plans include a sufficient level of detail such that the information can be incorporated into continuous monitoring programs implemented by organizations. Continuous monitoring plans can include the types of control assessment and monitoring activities planned, frequency of control monitoring, and actions to be taken when controls fail or become ineffective.

Related controls and activities: CA-07.

(09) **Acquisition process: Functions, ports, protocols, and services in use**

Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.

Discussion: The identification of functions, ports, protocols, and services early in the system development lifecycle (e.g., during the initial requirements definition and design stages) allows organizations to influence the design of the system, system component, or system service.

This early involvement in the system development lifecycle helps organizations avoid or minimize the use of functions, ports, protocols, or services that pose unnecessarily high risks and understand the trade-offs involved in blocking specific ports, protocols, or services or requiring system service providers to do so.

Early identification of functions, ports, protocols, and services avoids costly retrofitting of controls after the system, component, or system service has been implemented. SA-09 describes the requirements for external system services. Organizations identify which functions, ports, protocols, and services are provided from external sources.

Related controls and activities: CM-07, SA-09.

(10) **Acquisition process: Use of approved digital credentials products**

Employ only IT products that are recommended by the Cyber Centre for digital credentials capability implemented within organizational systems.

Discussion: Products should meet the Cyber Centre requirements outlined in the publication User authentication guidance for information technology systems (ITSP.30.031) for authentication level of assurance (LoA) and robustness level (RL) for digital credentials of GC employees and contractors. Authentication tokens such as smart cards are used for MFA in systems and organizations.

Related controls and activities: IA-02, IA-08, PM-09.

(11) **Acquisition process: System of record**

Include [Assignment: organization-defined *Privacy Act* requirements] in the acquisition contract for the operation of a system of record on behalf of an organization to accomplish an organizational mission or function.

Discussion: When, by contract, an organization provides for the operation of a system of record to accomplish an organizational mission or function, the organization, consistent with its authority, causes the requirements of the *Privacy Act* to be applied to the system of records.

At times, contractors will represent the GC and collect personal information associated with operating programs or services. Contractors must be transparent that they are representing the GC and inform individuals about how their personal information may be shared with the government. When contractors are representing the GC, privacy and security obligations apply. Clarify in the acquisition contract custodial rights to personal information, in the event that the contractor will be representing the GC and collecting personal information from individuals.

Related controls and activities: PT-06.

(12) **Acquisition process: Data ownership**

- a. Include organizational data ownership requirements in the acquisition contract
- b. Require all data to be removed from the contractor's system and returned to the organization within [Assignment: organization-defined time frame]

Discussion: Contractors who operate a system that contains data owned by an organization initiating the contract have policies and procedures in place to remove the data from their systems and/or return the data in a timeframe defined by the contract.

Related controls and activities: None.

References:

- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [TBS Directive on Security Management: Appendix F: Mandatory Procedures for Security in Contracts and Other Arrangements Control](#)
- [TBS Directive on Service and Digital, Appendix G: Standard on Enterprise Information Technology Service Common Configurations](#)
- [TBS Directive on Identity Management, Appendix A: Standard on Identity and Credential Assurance](#)
- [Baseline security requirements for network security zones \(ITSP.80.022\)](#)
- [Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B information \(ITSP.40.111\)](#)
- [Cryptographic Module Validation Program \(CMVP\)](#)

- [User authentication guidance for information technology systems \(ITSP.30.031\)](#)
- [PSPC Supply Manual, Chapter 1 – Public procurement, Section 1.70 Privacy in contracting](#)
- [TBS Guidance Document: Taking Privacy into Account Before Making Contracting Decisions](#)

SA-05 System documentation

Activity:

- A. Obtain or develop administrator documentation for the system, system component, or system service that describes
 1. secure configuration, installation, and operation of the system, component, or service
 2. effective use and maintenance of security and privacy functions and mechanisms
 3. known vulnerabilities regarding configuration and use of administrative or privileged functions
- B. Obtain or develop user documentation for the system, system component, or system service that describes
 1. user-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms
 2. methods for user interaction, which enable individuals to use the system, component, or service in a more secure manner and protect individual privacy
 3. user responsibilities in maintaining the security of the system, component, or service and privacy of individuals
- C. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or non-existent and take [Assignment: organization-defined actions] in response
- D. Distribute documentation to [Assignment: organization-defined personnel or roles]

Discussion: System artifacts and documentation created by the developer helps organizational personnel understand the implementation and operation of controls. Organizations consider establishing specific measures to determine the quality and completeness of the content provided. System documentation may be used to delineate roles, responsibilities, and expectations of the developer and organization, support the management of supply chain risk, incident response, and other functions. Personnel or roles that require documentation include system owners, system security officers, and system administrators. Attempts to obtain documentation include contacting manufacturers or suppliers and conducting web-based searches.

The inability to obtain documentation may occur due to the age of the system or component or the lack of support from developers and contractors. When documentation cannot be obtained, organizations may need to recreate the documentation if it is essential to the implementation or operation of the controls.

The protection provided for the documentation is commensurate with the security category or classification of the system. Documentation that addresses system vulnerabilities may require an increased level of protection. Secure operation of the system includes initially starting the system and resuming secure system operation after a lapse in system operation.

Related controls and activities: CM-04, CM-06, CM-07, CM-08, PL-02, PL-04, PL-08, PS-02, SA-03, SA-04, SA-08, SA-09, SA-10, SA-11, SA-15, SA-16, SA-17, SI-12, SR-03.

Enhancements:

- (01) **System documentation: Functional properties of security controls**
Withdrawn: Incorporated into SA-04(01).
- (02) **System documentation: Security-relevant external system interfaces**
Withdrawn: Incorporated into SA-04(02).
- (03) **System documentation: High-level design**
Withdrawn: Incorporated into SA-04(02).
- (04) **System documentation: Low-level design**

Withdrawn: Incorporated into SA-04(02).

(05) **System documentation: Source code**

Withdrawn: Incorporated into SA-04(02).

References: None.

SA-06 Software usage restrictions

Withdrawn: Incorporated into CM-10 and SI-07.

SA-07 User-installed software

Withdrawn: Incorporated into CM-11 and SI-07.

SA-08 Security and privacy engineering principles

Control: Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [Assignment: organization-defined systems security and privacy engineering principles].

Discussion: Systems security and privacy engineering principles are closely related to and implemented throughout the system development lifecycle (see SA-03). Organizations can apply systems security and privacy engineering principles to new systems under development or to systems undergoing upgrades. For existing systems, organizations apply systems security and privacy engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware components within those systems.

The application of systems security and privacy engineering principles helps organizations develop trustworthy, secure, and resilient systems and reduces the susceptibility to disruptions, hazards, threats, and the creation of privacy problems for individuals. Examples of system security engineering principles include developing layered protections; establishing security and privacy policies, architecture, and controls as the foundation for design and development; incorporating security and privacy requirements into the system development lifecycle; delineating physical and logical security boundaries; ensuring that developers are trained on how to build secure software; tailoring controls to meet organizational needs; and performing threat modelling to identify use cases, threat agents, attack vectors and patterns, design patterns, and compensating controls needed to mitigate risk.

Organizations that apply systems security and privacy engineering concepts and principles can facilitate the development of trustworthy, secure systems, system components, and system services; reduce risk to acceptable levels; and make informed risk management decisions. System security engineering principles can also be used to protect against certain supply chain risks, including incorporating tamper-resistant hardware into a design.

GC discussion: There are 10 Fair Information Principles that guide privacy protections for federal programs. In general, organizations need policies that dictate privacy policies; limit the collection, use, disclosure, and retention of personal information; and ensure individuals are informed about the handling of their personal information and have the right to access their personal information.

Related controls and activities: PL-08, PM-07, RA-02, RA-03, RA-09, SA-03, SA-04, SA-15, SA-17, SA-20, SC-02, SC-03, SC-32, SC-39, SI-400, SR-02, SR-03, SR-04, SR-05.

Enhancements:

(01) **Security and privacy engineering principles: Clear abstractions**

Implement the security design principle of clear abstractions.

Discussion: The principle of clear abstractions states that a system has simple, well-defined interfaces and functions that provide a consistent and intuitive view of the data and how the data is managed. The clarity, simplicity, necessity, and sufficiency of the system interfaces—combined with a precise definition of their functional behaviour—promotes ease of analysis, inspection, and testing, as well as the correct and secure use of the system. The clarity of an abstraction is subjective.

Examples that reflect the application of this principle include avoiding redundant, unused interfaces; information hiding; and avoiding semantic overloading of interfaces or their parameters. Information hiding (i.e., representation-independent programming) is a design discipline used to ensure that the internal representation of information in one system component is not visible to another system component invoking or calling the first component, such that the published abstraction is not influenced by how the data may be managed internally.

Related controls and activities: None.

(02) **Security and privacy engineering principles: Least common mechanism**

Implement the security design principle of least common mechanism in [Assignment: organization-defined systems or system components].

Discussion: The principle of least common mechanism states that the amount of mechanism common to more than one user and depended on by all users is minimized (Popek, 1974). Mechanism minimization implies that different components of a system refrain from using the same mechanism to access a system resource.

Every shared mechanism (especially a mechanism involving shared variables) represents a potential information path between users and is designed with care to ensure that it does not unintentionally compromise security (Saltzer & Schroeder, 1975). Implementing the principle of least common mechanism helps to reduce the adverse consequences of sharing the system state among different programs.

A single program that corrupts a shared state (including shared variables) has the potential to corrupt other programs that are dependent on the state. The principle of least common mechanism also supports the principle of simplicity of design and addresses the issue of covert storage channels (Lampson, 1973).

Related controls and activities: None.

(03) **Security and privacy engineering principles: Modularity and layering**

Implement the security design principles of modularity and layering in [Assignment: organization-defined systems or system components].

Discussion: The principles of modularity and layering are fundamental across system engineering disciplines. Modularity and layering derived from functional decomposition are effective in managing system complexity by making it possible to comprehend the structure of the system. Modular decomposition, or refinement in system design, is challenging and resists general statements of principle.

Modularity serves to isolate functions and related data structures into well-defined logical units. Layering allows the relationships of these units to be better understood so that dependencies are clear and undesired complexity can be avoided. The security design principle of modularity extends functional modularity to include considerations based on trust relationships, privilege, and security policy.

Security-informed modular decomposition includes the allocation of policies to systems in a network, separation of system applications into processes with distinct address spaces, allocation of system policies to layers, and separation of processes into subjects with distinct privileges based on hardware-supported privilege domains.

Related controls and activities: SC-02, SC-03.

(04) **Security and privacy engineering principles: Partially ordered dependencies**

Implement the security design principle of partially ordered dependencies in [Assignment: organization-defined systems or system components].

Discussion: The principle of partially ordered dependencies states that the synchronization, calling, and other dependencies in the system are partially ordered. A fundamental concept in system design is layering, whereby the system is organized into well-defined, functionally related modules or components. The layers are linearly ordered with respect to inter-layer dependencies, such that higher layers are dependent on lower layers.

While providing functionality to higher layers, some layers can be self-contained and are not dependent on lower layers. Although a partial ordering of all functions in a given system may not be possible, if circular dependencies are constrained to occur within layers, the inherent problems of circularity can be more easily managed.

Partially ordered dependencies and system layering contribute significantly to the simplicity and coherency of the system design. Partially ordered dependencies also facilitate system testing and analysis.

Related controls and activities: None.

(05) **Security and privacy engineering principles: Efficiently mediated access**

Implement the security design principle of efficiently mediated access in [Assignment: organization-defined systems or system components].

Discussion: The principle of efficiently mediated access states that policy enforcement mechanisms utilize the least common mechanism available while satisfying stakeholder requirements within expressed constraints. The mediation of access to system resources (i.e., CPU, memory, devices, communication ports, services, infrastructure, data, and information) is often the predominant security function of secure systems. It also enables the realization of protections for the capability provided to stakeholders by the system.

Mediation of resource access can result in performance bottlenecks if the system is not designed correctly. For example, efficiently mediated access can be achieved by using hardware mechanisms. Once access to a low-level resource such as memory has been obtained, hardware protection mechanisms can ensure that out-of-bounds access does not occur.

Related controls and activities: AC-25.

(06) **Security and privacy engineering principles: Minimized sharing**

Implement the security design principle of minimized sharing in [Assignment: organization-defined systems or system components].

Discussion: The principle of minimized sharing states that no computer resource is shared between system components (e.g., subjects, processes, functions) unless it is absolutely necessary to do so. Minimized sharing helps to simplify system design and implementation.

To protect user-domain resources from arbitrary active entities, no resource is shared unless that sharing has been explicitly requested and granted. The need for resource sharing can be motivated by the design principle of least common mechanism in the case of internal entities or driven by stakeholder requirements. However, internal sharing is carefully designed to avoid problem related to performance, covert storage, and timing channel problems.

Sharing via common mechanism can increase the susceptibility of data and information to unauthorized access, disclosure, use, or modification and can adversely affect the inherent capability provided by the system. To minimize sharing induced by common mechanisms, such mechanisms can be designed to be re-entrant or virtualized to preserve separation. Moreover, the use of global data to share information is carefully scrutinized. The lack of encapsulation may obfuscate relationships among the sharing entities.

Related controls and activities: SC-31.

(07) **Security and privacy engineering principles: Reduced complexity**

Implement the security design principle of reduced complexity in [Assignment: organization-defined systems or system components].

Discussion: The principle of reduced complexity states that the system design is as simple and small as possible. A small and simple design is more understandable, more analyzable, and less prone to error. The reduced complexity principle applies to any aspect of a system, but it has particular importance for security due to the various analyses performed to obtain evidence about the emergent security property of the system. For such analyses to be successful, a small and simple design is essential.

Application of the principle of reduced complexity contributes to the ability of system developers to understand the correctness and completeness of system security functions. It also facilitates the identification of potential vulnerabilities. The corollary of reduced complexity states that the simplicity of the system is directly related to the number of vulnerabilities it will contain; that is, simpler systems contain fewer vulnerabilities.

Benefits of reduced complexity are that it is easier to understand whether the intended security policy has been captured in the system design and that fewer vulnerabilities are likely to be introduced during engineering development. An additional benefit is that any such conclusion about correctness, completeness, and the existence of vulnerabilities can be reached with a higher degree of assurance in contrast to conclusions reached in situations where the system design is inherently more complex.

Transitioning from older technologies to newer technologies (e.g., transitioning from Ipv4 to Ipv6) may require implementing the older and newer technologies simultaneously during the transition period. This may result in a temporary increase in system complexity during the transition.

Related controls and activities: None.

(08) **Security and privacy engineering principles: Secure evolvability**

Implement the security design principle of secure evolvability in [Assignment: organization-defined systems or system components].

Discussion: The principle of secure evolvability states that a system is developed to facilitate the maintenance of its security properties when there are changes to the system's structure, interfaces, interconnections (i.e., system architecture), functionality, or configuration (i.e., security policy enforcement). Changes include a new, enhanced, or upgraded system capability; maintenance and sustainment activities; and reconfiguration.

Although it is not possible to plan for every aspect of system evolution, system upgrades and changes can be anticipated by analyses of mission or business strategic direction, anticipated changes in the threat environment, and anticipated maintenance and sustainment needs. It is unrealistic to expect that complex systems remain secure in contexts not envisioned during development, whether such contexts are related to the operational environment or to usage.

A system may be secure in some new contexts, but there is no guarantee that its emergent behaviour will always be secure. It is easier to build robustness into a system from the outset, and it follows that the sustainment of system robustness requires planning for change as opposed to adapting in an ad hoc or non-methodical manner.

The benefits of this principle include reduced vendor lifecycle costs, reduced cost of ownership, improved system security, more effective management of security risk, and less risk uncertainty.

Related controls and activities: CM-03.

(09) **Security and privacy engineering principles: Trusted components**

Implement the security design principle of trusted components in [Assignment: organization-defined systems or system components].

Discussion: The principle of trusted components states that a component is both trustworthy and robust to at least a level commensurate with the security dependencies it supports (i.e., how much it is trusted to perform its security functions by other components). This principle enables the composition of components such that trustworthiness and robustness are not inadvertently diminished, and the trust is not consequently misplaced. Ultimately, this

principle demands some metric by which the trust in a component and the trustworthiness and robustness of a component can be measured on the same abstract scale.

The principle of trusted components is particularly relevant when considering systems and components in which there are complex chains of trust dependencies. A trust dependency is also referred to as a trust relationship and there may be chains of trust relationships.

The principle of trusted components also applies to a compound component that consists of subcomponents (e.g., a subsystem), which may have varying levels of trustworthiness. The conservative assumption is that the trustworthiness of a compound component is that of its least trustworthy subcomponent. It may be possible to provide a security engineering rationale that the trustworthiness of a particular compound component is greater than the conservative assumption. However, any such rationale reflects logical reasoning based on a clear statement of the trustworthiness objectives as well as relevant and credible evidence. The trustworthiness of a compound component is not the same as increased application of defence-in-depth layering within the component or a replication of components. Defence-in-depth techniques do not increase the trustworthiness of the whole above that of the least trustworthy component.

Related controls and activities: None.

(10) **Security and privacy engineering principles: Hierarchical trust**

Implement the security design principle of hierarchical trust in [Assignment: organization-defined systems or system components].

Discussion: The principle of hierarchical trust for components builds on the principle of trusted components and states that the security dependencies in a system will form a partial ordering if they preserve the principle of trusted components. The partial ordering provides the basis for both trustworthiness and robustness reasoning when composing a secure system from independently developed or sourced components.

To analyze a system composed of independently developed or sourced components for both trustworthiness and robustness, it is essential to eliminate circular dependencies. If a more trustworthy or robust component located in a lower layer of the system were to depend on a less trustworthy or less robust component in a higher layer, this would reduce the overall trust or the robustness of the system to that of the weaker element that is being depended upon.

Trust relationships, or chains of trust, can have various manifestations. For example, the root certificate of a certificate hierarchy is the most trusted node in the hierarchy, whereas the leaves in the hierarchy may be less trustworthy nodes. Another example occurs in a layered high-assurance system where the security kernel (including the hardware base), which is located at the lowest layer of the system, is the most trustworthy component.

The principle of hierarchical trust, however, does not prohibit the use of overly trustworthy components. There may be cases in a system of low trustworthiness where it is reasonable to employ a highly trustworthy component rather than one that is less trustworthy (e.g., due to availability or another cost-benefit driver). For such a case, any dependency of the highly trustworthy component upon a less trustworthy component does not degrade the trustworthiness of the resulting low-trust system, nor does it raise its trustworthiness or robustness.

Related controls and activities: None.

(11) **Security and privacy engineering principles: Inverse modification threshold**

Implement the security design principle of inverse modification threshold in [Assignment: organization-defined systems or system components].

Discussion: The principle of inverse modification threshold builds on the principles of trusted components and of hierarchical trust and states that the degree of protection provided to a component is commensurate with its trustworthiness. As the trust placed in a component increases, the protection against unauthorized modification of the component increases to the same degree.

Protection from unauthorized modification can come in the form of the component's own self-protection and innate robustness, or it can come from the protections afforded to the component from other elements or attributes of the security architecture (to include protections in the environment of operation).

Related controls and activities: None.

(12) **Security and privacy engineering principles: Hierarchical protection**

Implement the security design principle of hierarchical protection in [Assignment: organization-defined systems or system components].

Discussion: The principle of hierarchical protection states that a component need not be protected from more trustworthy components. In the degenerate case of the most trusted component, it protects itself from all other components. For example, if an operating system kernel is deemed the most trustworthy component in a system, then it protects itself from all untrusted applications it supports, but the applications, conversely, do not need to protect themselves from the kernel.

The trustworthiness of users is a consideration for applying the principle of hierarchical protection. A trusted system need not protect itself from an equally trustworthy user, reflecting use of untrusted systems in system high environments where users are highly trustworthy and where other protections are put in place to bound and protect the system high execution environment.

Related controls and activities: None.

(13) **Security and privacy engineering principles: Minimized security elements**

Implement the security design principle of minimized security elements in [Assignment: organization-defined systems or system components].

Discussion: The principle of minimized security elements states that the system does not have extraneous trusted components. The principle of minimized security elements has 2 aspects: the overall cost of security analysis and the complexity of security analysis.

Trusted components are generally costlier to construct and implement, owing to the increased rigour of development processes and supply chain integrity requirements. Trusted components require greater security analysis to qualify their robustness and enhance supply chain controls to qualify their trustworthiness. Thus, to reduce the cost and decrease the complexity of the security analysis, a system contains as few trusted components as possible.

The analysis of the interaction of trusted components with other components of the system is one of the most important aspects of system security verification. If the interactions between components are unnecessarily complex, the security of the system will also be more difficult to ascertain than one whose internal trust relationships are simple and elegantly constructed. In general, fewer trusted components result in fewer internal trust relationships and a simpler system.

Related controls and activities: None.

(14) **Security and privacy engineering principles: Least privilege**

Implement the security design principle of least privilege in [Assignment: organization-defined systems or system components].

Discussion: The principle of least privilege states that each system component is allocated sufficient privileges to accomplish its specified functions but no more. Applying the principle of least privilege limits the scope of the component's actions, which has 2 desirable effects: the security impact of a failure, corruption, or misuse of the component will have a smaller security impact, and the security analysis of the component will be simplified. Least privilege is a pervasive principle that is reflected in all aspects of the secure system design. Interfaces used to invoke component capability are available to only certain subsets of the user population, and component design supports a sufficiently fine granularity of privilege decomposition.

For example, in the case of an audit mechanism, there may be an interface for the audit manager, who configures the audit settings; an interface for the audit operator, who ensures that audit data is safely collected and stored; and, finally, yet another interface for the audit reviewer, who only needs to view the audit data that has been collected but does not need to perform operations on that data.

In addition to its manifestations at the system interface, least privilege can be used as a guiding principle for the internal structure of the system itself. One aspect of internal least privilege is to construct modules so that only the elements encapsulated by the module are directly operated on by the functions within the module. Elements external to a module that may be affected by the module's operation are indirectly accessed through interaction (e.g., via a function call) with the module that contains those elements. Another aspect of internal least privilege is that the scope of a given module or component includes only those system elements that are necessary for its functionality and that the access modes for the elements (e.g., read, write) are minimal. An example of least privilege in software development is minimizing the functions that operate with elevated privileges (for example, limiting the tools and functions that operate in kernel mode).

Related controls and activities: AC-06, CM-07.

(15) **Security and privacy engineering principles: Predicate permission**

Implement the security design principle of predicate permission in [Assignment: organization-defined systems or system components].

Discussion: The principle of predicate permission states that system designers consider requiring multiple authorized entities to provide consent before a highly critical operation or access to highly sensitive data, information, or resources is allowed to proceed.

Saltzer (Saltzer & Schroeder, 1975) originally named predicate permission the separation of privilege. It is also equivalent to separation of duty. The division of privilege among multiple parties decreases the likelihood of abuse and provides the safeguard that no single accident, deception, or breach of trust is sufficient to enable an unrecoverable action that can lead to significantly damaging effects.

The design options for such a mechanism may require simultaneous action (e.g., the firing of a nuclear weapon requires 2 different authorized individuals to give the correct command within a small time window) or a sequence of operations where each successive action is enabled by some prior action, but no single individual is able to enable more than one action.

Related controls and activities: AC-05.

(16) **Security and privacy engineering principles: Self-reliant trustworthiness**

Implement the security design principle of self-reliant trustworthiness in [Assignment: organization-defined systems or system components].

Discussion: The principle of self-reliant trustworthiness states that systems minimize their reliance on other systems for their own trustworthiness. A system is trustworthy by default, and any connection to an external entity is used to supplement its function. If a system were required to maintain a connection with another external entity in order to maintain its trustworthiness, then that system would be vulnerable to malicious and non-malicious threats that could result in the loss or degradation of that connection.

The benefit of the principle of self-reliant trustworthiness is that the isolation of a system will make it less vulnerable to attack. A corollary to this principle relates to the ability of the system (or system component) to operate in isolation and then resynchronize with other components when it is rejoined with them.

Related controls and activities: None.

(17) **Security and privacy engineering principles: Secure distributed composition**

Implement the security design principle of secure distributed composition in [Assignment: organization-defined systems or system components].

Discussion: The principle of secure distributed composition states that the composition of distributed components that enforce the same system security policy result in a system that enforces that policy at least as well as the individual components do.

Many of the design principles for secure systems deal with how components can or should interact. The need to create or enable a capability from the composition of distributed components can magnify the relevancy of these principles. In particular, the translation of security policy from a standalone to a distributed system or a system-of-systems can have unexpected or emergent results.

Communication protocols and distributed data consistency mechanisms help to ensure consistent policy enforcement across a distributed system. To ensure a system-wide level of assurance of correct policy enforcement, the security architecture of a distributed composite system is thoroughly analyzed.

Related controls and activities: None.

(18) **Security and privacy engineering principles: Trusted communications channels**

Implement the security design principle of trusted communications channels in [Assignment: organization-defined systems or system components].

Discussion: The principle of trusted communication channels states that when composing a system where there is a potential threat to communications between components (i.e., the interconnections between components), each communication channel is trustworthy to a level commensurate with the security dependencies it supports (i.e., how much it is trusted by other components to perform its security functions). Trusted communication channels are achieved by a combination of restricting access to the communication channel (to ensure an acceptable match in the trustworthiness and the robustness of the endpoints involved in the communication) and employing end-to-end protections for the data transmitted over the communication channel (to protect against interception and modification and to further increase the assurance of proper end-to-end communication).

Related controls and activities: SC-08, SC-12, SC-13.

(19) **Security and privacy engineering principles: Continuous protection**

Implement the security design principle of continuous protection in [Assignment: organization-defined systems or system components].

Discussion: The principle of continuous protection states that components and data used to enforce the security policy have uninterrupted protection that is consistent with the security policy and the security architecture assumptions. No assurances that the system can provide the confidentiality, integrity, availability, and privacy protections for its design capability can be made if there are gaps in the protection. Any assurances about the ability to secure a delivered capability require that data and information are continuously protected. That is, there are no periods during which data and information are left unprotected while under control of the system (i.e., during the creation, storage, processing, or communication of the data and information, as well as during system initialization, execution, failure, interruption, and shutdown).

Continuous protection requires adherence to the precepts of the reference monitor concept (i.e., every request is validated by the reference monitor; the reference monitor is able to protect itself from tampering; and sufficient assurance of the correctness and completeness of the mechanism can be ascertained from analysis and testing) and the principle of secure failure and recovery (i.e., preservation of a secure state during error, fault, failure, and successful attack; preservation of a secure state during recovery to normal, degraded, or alternative operational modes).

Continuous protection also applies to systems designed to operate in varying configurations, including those that deliver full operational capability and degraded-mode configurations that deliver partial operational capability. The continuous protection principle requires that changes to the system security policies be traceable to the operational need that drives the configuration and be verifiable (i.e., it is possible to verify that the proposed changes will not put the system into an insecure state).

Insufficient traceability and verification may lead to inconsistent states or protection discontinuities due to the complex or undecidable nature of the problem. The use of pre-verified configuration definitions that reflect the new security policy enables analysis to determine that a transition from old to new policies is essentially atomic and that any residual effects from the old policy are guaranteed to not conflict with the new policy. The ability to demonstrate continuous protection is rooted in the clear articulation of lifecycle protection needs as stakeholder security requirements.

Related controls and activities: AC-25.

(20) **Security and privacy engineering principles: Secure metadata management**

Implement the security design principle of secure metadata management in [Assignment: organization-defined systems or system components].

Discussion: The principle of secure metadata management states that metadata is a first-class object with respect to security policy when the policy requires either complete protection of information or that the security subsystem be self-protecting. The principle of secure metadata management is driven by the recognition that a system, subsystem, or component cannot achieve self-protection unless it protects the data it relies on for correct execution.

Data is generally not interpreted by the system that stores it. It may have semantic value (i.e., it comprises information) to users and programs that process the data. In contrast, metadata is information about data, such as a file name or the date when the file was created. Metadata is bound to the target data that it describes in a way that the system can interpret, but it need not be stored inside of or proximate to its target data. There may be metadata whose target is itself metadata (e.g., the classification level or impact level of a file name), including self-referential metadata.

The apparent secondary nature of metadata can lead to neglect of its legitimate need for protection, resulting in a violation of the security policy that includes the exfiltration of information. A particular concern associated with insufficient protections for metadata is associated with multilevel secure (MLS) systems. MLS systems mediate access by a subject to an object based on relative sensitivity levels. It follows that all subjects and objects in the scope of control of the MLS system are either directly labelled or indirectly attributed with sensitivity levels.

The corollary of labelled metadata for MLS systems states that objects containing metadata are labelled. As with protection needs assessments for data, attention is given to ensure that the confidentiality and integrity protections are individually assessed, specified, and allocated to metadata, as would be done for mission, business, and system data.

Related controls and activities: None.

(21) **Security and privacy engineering principles: Self-analysis**

Implement the security design principle of self-analysis in [Assignment: organization-defined systems or system components].

Discussion: The principle of self-analysis states that a system component is able to assess its internal state and functionality to a limited extent at various stages of execution, and that this self-analysis capability is commensurate with the level of robustness invested in the system. At the system level, self-analysis can be achieved through hierarchical assessments of robustness established in a bottom-up fashion. In this approach, the lower-level components check for data integrity and correct functionality (to a limited extent) of higher-level components. For example, trusted boot sequences involve a trusted lower-level component that attests to the integrity of the next higher-level components so that a transitive chain of trust can be established.

At the root, a component attests to itself, which usually involves an axiomatic or environmentally enforced assumption about its integrity. Results of the self-analyses can be used to guard against externally induced errors, internal malfunction, or transient errors. By following this principle, some simple malfunctions or errors can be detected without allowing the effects of the error or malfunction to propagate outside of the component. Further, the

self-test can be used to attest to the configuration of the component, detecting any potential conflicts in configuration with respect to the expected configuration.

Related controls and activities: CA-07.

(22) **Security and privacy engineering principles: Accountability and traceability**

Implement the security design principle of accountability and traceability in [Assignment: organization-defined systems or system components].

Discussion: The principle of accountability and traceability states that it is possible to trace security-relevant actions (i.e., subject-object interactions) to the entity on whose behalf the action is being taken. The principle of accountability and traceability requires a trustworthy infrastructure that can record details about actions that affect system security (e.g., an audit subsystem).

To record the details about actions, the system is able to uniquely identify the entity on whose behalf the action is being carried out and also record the relevant sequence of actions that is carried out. The accountability policy also requires that the audit trail itself be protected from unauthorized access and modification.

The principle of least privilege assists in tracing the actions to particular entities, as it increases the granularity of accountability. Associating specific actions with system entities, and ultimately with users, and making the audit trail secure against unauthorized access and modifications provide non-repudiation because once an action is recorded, it is not possible to change the audit trail.

Another important function that accountability and traceability serves is in the routine and forensic analysis of events associated with the violation of security policy. Analysis of audit logs may provide additional information that may be helpful in determining the path or component that allowed the violation of the security policy and the actions of individuals associated with the violation of the security policy.

Related controls and activities: AC-06, AU-02, AU-03, AU-06, AU-09, AU-10, AU-12, IA-02, IR-04.

(23) **Security and privacy engineering principles: Secure defaults**

Implement the security design principle of secure defaults in [Assignment: organization-defined systems or system components].

Discussion: The principle of secure defaults states that the default configuration of a system (including its constituent subsystems, components, and mechanisms) reflects a restrictive and conservative enforcement of security policy. The principle of secure defaults applies to the initial (i.e., default) configuration of a system as well as to the security engineering and design of access control and other security functions that follow a deny-unless-explicitly-authorized strategy.

The initial configuration aspect of this principle requires that any as-shipped configuration of a system, subsystem, or system component does not aid in the violation of the security policy and can prevent the system from operating in the default configuration for those cases where the security policy itself requires configuration by the operational user.

Restrictive defaults mean that the system will operate as shipped with adequate self-protection and will be able to prevent security breaches before the intended security policy and system configuration is established. In cases where the protection provided by the as-shipped product is inadequate, stakeholders assess the risk of using it prior to establishing a secure initial state.

Adherence to the principle of secure defaults guarantees that a system is established in a secure state upon successfully completing initialization. In situations where the system fails to complete initialization, it will perform a requested operation using secure defaults or it will not perform the operation. Refer to the principles of continuous protection and secure failure and recovery that parallel this principle to provide the ability to detect and recover from failure.

The security engineering approach to this principle states that security mechanisms deny requests unless the request is found to be well-formed and consistent with the security policy. The insecure alternative is to allow a request unless it is shown to be inconsistent with the policy. In a large system, the conditions that are satisfied to grant a request that is denied by default are often far more compact and complete than those that would need to be checked in order to deny a request that is granted by default.

Related controls and activities: CM-02, CM-06, SA-04.

(24) **Security and privacy engineering principles: Secure failure and recovery**

Implement the security design principle of secure failure and recovery in [Assignment: organization-defined systems or system components].

Discussion: The principle of secure failure and recovery states that neither a failure in a system function or mechanism nor any recovery action in response to failure leads to a violation of security policy. The principle of secure failure and recovery parallels the principle of continuous protection to ensure that a system is capable of detecting (within limits) actual and impending failure at any stage of its operation (i.e., initialization, normal operation, shutdown, and maintenance) and to take appropriate steps to ensure that security policies are not violated. In addition, when specified, the system is capable of recovering from impending or actual failure to resume normal, degraded, or alternative secure operations while ensuring that a secure state is maintained such that security policies are not violated.

Failure is a condition in which the behaviour of a component deviates from its specified or expected behaviour for an explicitly documented input. Once a failed security function is detected, the system may reconfigure itself to circumvent the failed component while maintaining security and provide all or part of the functionality of the original system, or it may completely shut itself down to prevent any further violation of security policies. For this to occur, the reconfiguration functions of the system are designed to ensure continuous enforcement of security policy during the various phases of reconfiguration.

Another technique that can be used to recover from failures is to perform a rollback to a secure state (which may be the initial state) and then either shut down or replace the service or component that failed such that secure operations may resume. Failure of a component may or may not be detectable to the components using it. The principle of secure failure indicates that components fail in a state that denies rather than grants access.

For example, a nominally atomic operation interrupted before completion does not violate security policy and is designed to handle interruption events by employing higher-level atomicity and rollback mechanisms (e.g., transactions). If a service is being used, its atomicity properties are well-documented and characterized so that the component availing itself of that service can detect and handle interruption events appropriately. For example, a system is designed to gracefully respond to disconnection and support resynchronization and data consistency after disconnection.

Failure protection strategies that employ replication of policy enforcement mechanisms, sometimes called defence in depth, can allow the system to continue in a secure state even when one mechanism has failed to protect the system. If the mechanisms are similar, however, the additional protection may be illusory, as the adversary can simply attack in series. Similarly, in a networked system, breaking the security on one system or service may enable an attacker to do the same on other similar replicated systems and services.

By employing multiple protection mechanisms whose features are significantly different, the possibility of attack replication or repetition can be reduced. Analyses are conducted to weigh the costs and benefits of such redundancy techniques against increased resource usage and adverse effects on the overall system performance.

Additional analyses are conducted as the complexity of these mechanisms increases, as could be the case for dynamic behaviours. Increased complexity generally reduces robustness. When a resource cannot be continuously protected, it is critical to detect and repair any security breaches before the resource is once again used in a secure context.

Related controls and activities: CP-10, CP-12, SC-07, SC-08, SC-24, SI-13.

(25) **Security and privacy engineering principles: Economic security**

Implement the security design principle of economic security in [Assignment: organization-defined systems or system components].

Discussion: The principle of economic security states that security mechanisms are not costlier than the potential damage that could occur from a security breach. This is the security-relevant form of the cost-benefit analyses used in risk management. The cost assumptions of cost-benefit analysis prevent the system designer from incorporating security mechanisms of greater strength than necessary, where strength of mechanism is proportional to cost. The principle of economic security also requires analysis of the benefits of assurance relative to the cost of that assurance in terms of the effort expended to obtain relevant and credible evidence.

Related controls and activities: RA-03.

(26) **Security and privacy engineering principles: Performance security**

Implement the security design principle of performance security in [Assignment: organization-defined systems or system components].

Discussion: The principle of performance security states that security mechanisms are constructed so that they do not degrade system performance unnecessarily. Stakeholder and system design requirements for performance and security are precisely articulated and prioritized. For the system implementation to meet its design requirements and be found acceptable to stakeholders (i.e., validation against stakeholder requirements), the designers adhere to the specified constraints that capability performance needs place on protection needs.

The overall impact of computationally intensive security services (e.g., cryptography) are assessed and demonstrated to pose no significant impact to higher-priority performance considerations or are deemed to provide an acceptable trade-off of performance for trustworthy protection. The trade-off considerations include less computationally intensive security services unless they are unavailable or insufficient. The insufficiency of a security service is determined by functional capability and strength of mechanism. The strength of mechanism is selected with respect to security requirements, performance-critical overhead issues (e.g., cryptographic key management), and an assessment of the capability of the threat.

The principle of performance security leads to the incorporation of features that help in the enforcement of security policy but incur minimum overhead, such as low-level hardware mechanisms upon which higher-level services can be built. Such low-level mechanisms are usually very specific, have very limited functionality, and are optimized for performance. For example, once access rights to a portion of memory are granted, many systems use hardware mechanisms to ensure that all further accesses involve the correct memory address and access mode.

Application of this principle reinforces the need to design security into the system from the ground up and to incorporate simple mechanisms at the lower layers that can be used as building blocks for higher-level mechanisms.

Related controls and activities: SC-12, SC-13, SI-02, SI-07.

(27) **Security and privacy engineering principles: Human-factored security**

Implement the security design principle of human factored security in [Assignment: organization-defined systems or system components].

Discussion: The principle of human-factored security states that the user interface for security functions and supporting services is intuitive, user-friendly, and provides feedback for user actions that affect such policy and its enforcement. The mechanisms that enforce security policy are not intrusive to the user and are designed not to degrade user efficiency.

Security policy enforcement mechanisms also provide the user with meaningful, clear, and relevant feedback and warnings when insecure choices are being made. Particular attention is given to interfaces through which personnel

responsible for system administration and operation configure and set up the security policies. Ideally, these personnel are able to understand the impact of their choices.

Personnel with system administrative and operational responsibilities are able to configure systems before start-up and administer them during runtime with confidence that their intent is correctly mapped to the system's mechanisms. Security services, functions, and mechanisms do not impede or unnecessarily complicate the intended use of the system. There is a trade-off between system usability and the strictness necessary for security policy enforcement. If security mechanisms are frustrating or difficult to use, then users may disable them, avoid them, or use them in ways inconsistent with the security requirements and protection needs that the mechanisms were designed to satisfy.

Related controls and activities: None.

(28) **Security and privacy engineering principles: Acceptable security**

Implement the security design principle of acceptable security in [Assignment: organization-defined systems or system components].

Discussion: The principle of acceptable security requires that the level of privacy and performance that the system provides is consistent with the users' expectations. The perception of personal privacy may affect user behaviour, morale, and effectiveness. Based on the organizational privacy policy and the system design, users should be able to restrict their actions to protect their privacy. When systems fail to provide intuitive interfaces or to meet privacy and performance expectations, users may either choose to completely avoid the system or use it in ways that may be inefficient or even insecure.

Related controls and activities: None.

(29) **Security and privacy engineering principles: Repeatable and documented procedures**

Implement the security design principle of repeatable and documented procedures in [Assignment: organization-defined systems or system components].

Discussion: The principle of repeatable and documented procedures states that the techniques and methods employed to construct a system component permit the same component to be completely and correctly reconstructed at a later time. Repeatable and documented procedures support the development of a component that is identical to the component created earlier, which may be in widespread use.

In the case of other system artifacts (e.g., documentation and testing results), repeatability supports consistency and the ability to inspect the artifacts. Repeatable and documented procedures can be introduced at various stages within the system development lifecycle and can contribute to the ability to evaluate assurance claims for the system. Examples include systematic procedures for code development and review, procedures for the configuration management of development tools and system artifacts, and procedures for system delivery.

Related controls and activities: CM-01, SA-01, SA-10, SA-11, SA-15, SA-17, SC-01, SI-01.

(30) **Security and privacy engineering principles: Procedural rigour**

Implement the security design principle of procedural rigour in [Assignment: organization-defined systems or system components].

Discussion: The principle of procedural rigour states that the rigour of a system lifecycle process is commensurate with its intended trustworthiness and robustness. Procedural rigour defines the scope, depth, and detail of the system lifecycle procedures. Rigorous system lifecycle procedures contribute to the assurance that the system is correct and free of unintended functionality in several ways. First, the procedures impose checks and balances on the lifecycle process such that the introduction of unspecified functionality is prevented.

Second, rigorous procedures applied to systems security engineering activities that produce specifications and other system design documents contribute to the ability to understand the system as it has been built rather than trusting that the component, as implemented, is the authoritative (and potentially misleading) specification.

Finally, it is easier to make modifications to an existing system component when there are detailed specifications that describe its current design than it is to study source code or schematics to try to understand how the component works.

Procedural rigour helps ensure that security functional and assurance requirements have been satisfied, and it contributes to a better-informed basis for determining trustworthiness and robustness. Procedural rigour is commensurate with the degree of assurance desired for the system. If the required assurance of the system is low, a high level of procedural rigour may add unnecessary cost, whereas when high assurance is critical, the cost of high procedural rigour is merited.

Related controls and activities: None.

(31) **Security and privacy engineering principles: Secure system modification**

Implement the security design principle of secure system modification in [Assignment: organization-defined systems or system components].

Discussion: The principle of secure system modification states that system modification maintains system security with respect to the security requirements and risk tolerance of stakeholders. Upgrades or modifications to systems can transform secure systems into systems that are not secure. The procedures for system modification ensure that if the system is to maintain its trustworthiness and robustness, the same rigour that was applied to its initial development is applied to any system changes. Because modifications can affect the ability of the system to maintain its secure state, a careful security analysis of the modification is needed prior to its implementation and deployment. This principle parallels the principle of secure evolvability.

Related controls and activities: CM-03, CM-04.

(32) **Security and privacy engineering principles: Sufficient documentation**

Implement the security design principle of sufficient documentation in [Assignment: organization-defined systems or system components].

Discussion: The principle of sufficient documentation states that organizational personnel with responsibilities to interact with the system are provided with adequate documentation and other information such that the personnel contribute to, rather than detract from, system security. Despite attempts to comply with principles such as human-factored security and acceptable security, systems are inherently complex, and the design intent for the use of security mechanisms and the ramifications of the misuse or misconfiguration of security mechanisms are not always obvious.

Uninformed and insufficiently trained users can introduce vulnerabilities due to errors of omission and commission. The availability of documentation and training can help to ensure a knowledgeable cadre of personnel, all of whom have a critical role in the achievement of principles such as continuous protection. Documentation is written clearly and supported by training that provides security awareness and understanding of security-relevant responsibilities.

Related controls and activities: AT-02, AT-03, SA-05.

(33) **Security and privacy engineering principles: Minimization**

Implement the privacy principle of minimization using [Assignment: organization-defined processes].

Discussion: The principle of minimization states that organizations must collect only personal or sensitive information if it relates directly to an operating program or activity of the institution. Along the same lines, organizations must only retain personal or sensitive information for as long as is necessary to accomplish the purpose. In the event that personal or sensitive information is required to be shared with other programs or organizations, the personal or sensitive information shared must be limited to that which is expressly required by the recipient program or organization. Organizations should have processes in place, consistent with applicable laws and policies, to implement the principle of minimization.

GC discussion: This enhancement is mandatory for GC departments and agencies.

Related controls and activities: PE-08, PM-25, SC-42, SI-12.

(400) **Security and privacy engineering principles: Licensed and certified engineers**

Employ licensed and certified security engineers that assume responsibility for the specification, design, development, and implementation of information system security and privacy solutions.

Discussion: None.

Related controls and activities: None.

References:

- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [TBS Directive on Service and Digital](#)
- [TBS Guideline on Service and Digital](#)
- [TBS Policy on Privacy Protection](#)
- [TBS Directive on Privacy Practices](#)
- [Baseline security requirements for network security zones \(ITSP.80.022\)](#)
- Overview, Cyber security and privacy risk management: A lifecycle approach (ITSP.10.035)
- System lifecycle cyber security and privacy risk management activities (ITSP.10.037)

SA-09 External system services

Control:

- A. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: [Assignment: organization-defined controls]
- B. Define and document organizational oversight and user roles and responsibilities with regard to external system services
- C. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: [Assignment: organization-defined processes, methods, and techniques]

Discussion: External system services are provided by an external provider, and the organization has no direct control over the implementation of the required controls or the assessment of control effectiveness. Organizations establish relationships with external service providers in a variety of ways, including through business partnerships, contracts, inter-agency agreements, lines of business arrangements, licensing agreements, joint ventures, and supply chain exchanges.

The responsibility for managing risks from using external system services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a certain level of confidence that each provider in the consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust vary based on relationships between organizations and the external providers. Organizations document the basis for the trust relationships so that the relationships can be monitored.

External system services documentation includes government, service providers, and end-user security roles and responsibilities, and service-level agreements. Service-level agreements define the performance expectations for implemented controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of non-compliance.

Related controls and activities: AC-20, CA-03, CP-02, IR-04, IR-07, PL-10, PL-11, PS-07, SA-02, SA-04, SR-03, SR-05, SA-400.

Enhancements:

(01) External system services: Risk assessments and organizational approvals

- a. Conduct an organizational risk assessment prior to acquiring or outsourcing information security services
- b. Verify that the acquisition or outsourcing of dedicated information security services is approved by [Assignment: organization-defined personnel or roles]

Discussion: Information security services include the operation of security devices, such as firewalls or key management services, as well as incident monitoring, analysis, and response. Risks assessed can include system, mission or business, security, privacy, or supply chain risks.

Related controls and activities: CA-06, RA-03, RA-08.

(02) External system services: Identification of functions, ports, protocols, and services

Require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: [Assignment: organization-defined external system services].

Discussion: Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be useful when the need arises to understand the trade-offs involved in restricting certain functions and services or blocking certain ports and protocols.

Related controls and activities: CM-06, CM-07.

(03) External system services: Establish and maintain trust relationship with providers

Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization-defined security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships].

Discussion: Trust relationships between organizations and external service providers reflect the degree of confidence that the risk from using external services is at an acceptable level. Trust relationships can help organizations gain increased levels of confidence that service providers are providing adequate protection for the services rendered. They can also be useful when conducting incident response or when planning for upgrades or obsolescence.

Trust relationships can be complicated due to the potentially large number of entities participating in the consumer-provider interactions, subordinate relationships and levels of trust, and types of interactions between the parties. In some cases, the degree of trust is based on the level of control that organizations can exert on external service providers regarding the controls necessary for the protection of the service, information, or individual privacy and on the evidence brought forth as to the effectiveness of the implemented controls. The level of control is established by the terms and conditions of the contracts or service-level agreements.

Related controls and activities: SR-02.

(04) External system services: Consistent interests of consumers and providers

Take the following actions to verify that the interests of [Assignment: organization-defined external service providers] are consistent with and reflect organizational interests: [Assignment: organization-defined actions].

Discussion: As organizations increasingly use external service providers, it is possible that the interests of the service providers may diverge from organizational interests. In such situations, simply having the required technical, management, or operational controls in place may not be sufficient if the providers that implement and manage those controls are not operating in a manner consistent with the interests of the consuming organizations. Actions that organizations can take to address such concerns include requiring background checks for selected service provider personnel; examining ownership records; employing only trustworthy service providers, such as providers with which organizations have had successful trust relationships; and conducting routine, periodic, and unscheduled visits to service provider facilities.

Related controls and activities: None.

(05) **External system services: Processing, storage, and service location**

Restrict the location of [Selection (1 or more): information processing; information or data; system services] to [Assignment: organization-defined locations] based on [Assignment: organization-defined requirements or conditions].

Discussion: The location of information processing, information and data storage, or system services can have a direct impact on the ability of organizations to successfully execute their mission and business functions. The impact occurs when external providers control the location of processing, storage, or services. The criteria that external providers use to select processing, storage, or service locations may be different from the criteria that organizations use.

For example, organizations may want data or information storage locations to be restricted to certain locations to facilitate incident response activities in case of information security incidents or breaches. Incident response activities, including forensic analyses and after-the-fact investigations, may be adversely affected by the governing laws, policies, or protocols in the locations where processing and storage occur and/or the locations from which system services emanate.

Related controls and activities: SA-05, SA-400, SR-04.

(06) **External system services: Organization-controlled cryptographic keys**

Maintain exclusive control of cryptographic keys for encrypted material stored or transmitted through an external system.

Discussion: Maintaining exclusive control of cryptographic keys in an external system prevents decryption of organizational data by external system staff. Organizational control of cryptographic keys can be implemented by encrypting and decrypting data inside the organization as data is sent to and received from the external system or by employing a component that permits encryption and decryption functions to be local to the external system but allows exclusive organizational access to the encryption keys.

Related controls and activities: SC-12, SC-13, SI-04.

(07) **External system services: Organization-controlled integrity checking**

Provide the capability to check the integrity of information while it resides in the external system.

Discussion: Storage of organizational information in an external system could limit visibility into the security status of its data. The ability of the organization to verify and validate the integrity of its stored data without transferring it out of the external system provides such visibility.

Related controls and activities: SI-07.

(08) **External system services: Processing and storage location—within Canada**

Restrict the geographic location of information processing and data storage to facilities located within the legal jurisdictional boundary of Canada.

Discussion: The geographic location of information processing and data storage can have a direct impact on the ability of organizations to successfully execute their mission and business functions. A compromise or breach of high-impact information and systems can have severe adverse or catastrophic impacts on organizational assets and operations, individuals, other organizations, and Canada. Restricting the processing and storage of high-impact information to facilities within the legal jurisdictional boundary of Canada provides greater control over such processing and storage.

Related controls and activities: SA-05, SA-400, SR-04.

References:

- [TBS Directive on Security Management: Appendix F: Mandatory Procedures for Security in Contracts and Other Arrangements Control](#)
- [PSPC Contract Security Manual](#)
- [TBS Guideline on Service and Digital](#)
- [TBS Guidance Document: Taking Privacy into Account Before Making Contracting Decisions](#)
- [TBS Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice \(SPIN\)](#)
- [TBS Directive on Privacy Practices](#)
- [TBS Directive on Privacy Practices, Appendix C: Standard on Privacy Impact Assessment](#)
- [CSE-RCMP Harmonized Threat and Risk Assessment Methodology \(TRA-1\)](#)

SA-10 Developer configuration management

Activity: Require the developer of the system, system component, or system service to:

- perform configuration management during system, component, or service [Selection (1 or more): design; development; implementation; operation; disposal]
- document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management]
- implement only organization-approved changes to the system, component, or service
- document approved changes to the system, component, or service and the potential security and privacy impacts of such changes
- track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel]

Discussion: Organizations consider the quality and completeness of configuration management activities conducted by developers as direct evidence that effective security controls have been applied. Controls include protecting the master copies of material used to generate security-relevant portions of the system hardware, software, and firmware from unauthorized modification or destruction. Maintaining the integrity of changes to the system, system component, or system service requires strict configuration control throughout the system development lifecycle to track authorized changes and prevent unauthorized changes.

The configuration items that are placed under configuration management include the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the current running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and source code with previous versions; and test fixtures and documentation.

Depending on the mission and business needs of organizations and the nature of the contractual relationships in place, developers may provide configuration management support during the operations and maintenance stage of the system development lifecycle.

Related controls and activities: CM-02, CM-03, CM-04, CM-07, CM-09, SA-04, SA-05, SA-08, SA-15, SI-02, SR-03, SR-04, SR-05, SR-06.

Enhancements:

(01) Developer configuration management: Software and firmware integrity verification

Require the developer of the system, system component, or system service to enable integrity verification of software and firmware components.

Discussion: Software and firmware integrity verification allows organizations to detect unauthorized changes to software and firmware components using developer-provided tools, techniques, and mechanisms. The integrity

checking mechanisms can also address counterfeiting of software and firmware components. Organizations verify the integrity of software and firmware components, for example, through secure one-way hashes provided by developers. Delivered software and firmware components also include any updates to such components.

Related controls and activities: SI-07, SR-11.

(02) **Developer configuration management: Alternative configuration management processes**

Provide an alternate configuration management process using organizational personnel in the absence of a dedicated developer configuration management team.

Discussion: Alternate configuration management processes may be required when organizations use COTS IT products. Alternate configuration management processes include organizational personnel who review and approve proposed changes to systems, system components, and system services and who conduct security and privacy impact analyses prior to the implementation of changes to systems, components, or services.

Related controls and activities: None.

(03) **Developer configuration management: Hardware integrity verification**

Require the developer of the system, system component, or system service to enable integrity verification of hardware components.

Discussion: Hardware integrity verification allows organizations to detect unauthorized changes to hardware components using developer-provided tools, techniques, methods, and mechanisms. Organizations may verify the integrity of hardware components with hard-to-copy labels or verifiable serial numbers provided by developers, and by requiring the use of anti-tamper technologies. Delivered hardware components also include hardware and firmware updates to such components.

Related controls and activities: SI-07.

(04) **Developer configuration management: Trusted generation**

Require the developer of the system, system component, or system service to employ tools for comparing newly generated versions of security-relevant hardware descriptions, source code, and object code with previous versions.

Discussion: The trusted generation of descriptions, source code, and object code addresses authorized changes to hardware, software, and firmware components between versions during development. The focus is on the efficacy of the developer's configuration management process to ensure that newly generated versions of security-relevant hardware descriptions, source code, and object code continue to enforce the security policy for the system, system component, or system service. In contrast, SA-10(01) and SA-10(03) allow organizations to detect unauthorized changes to hardware, software, and firmware components using tools, techniques, or mechanisms provided by developers.

Related controls and activities: None.

(05) **Developer configuration management: Mapping integrity for version control**

Require the developer of the system, system component, or system service to maintain the integrity of the mapping between the master build data describing the current version of security-relevant hardware, software, and firmware and the onsite master copy of the data for the current version.

Discussion: Mapping integrity for version control addresses changes to hardware, software, and firmware components during initial development and system development lifecycle updates. Maintaining the integrity between the master copies of security-relevant hardware, software, and firmware (including designs, hardware drawings, and source code) and the equivalent data in master copies in operational environments is essential to ensuring the availability of organizational systems that support critical mission and business functions.

Related controls and activities: None.

(06) Developer configuration management: Trusted distribution

Require the developer of the system, system component, or system service to execute procedures for ensuring that security-relevant hardware, software, and firmware updates distributed to the organization are exactly as specified by the master copies.

Discussion: The trusted distribution of security-relevant hardware, software, and firmware updates helps ensure that the updates are correct representations of the master copies maintained by the developer and have not been tampered with during distribution.

Related controls and activities: None.

(07) Developer configuration management: Security and privacy representatives

Require [Assignment: organization-defined security and privacy representatives] to be included in the [Assignment: organization-defined configuration change management and control process].

Discussion: Information security and privacy representatives can include system security officers, senior officials in the department's security governance, appropriate privacy senior officials or executives, and system privacy officers. Representation by personnel with information security and privacy expertise is important because changes to system configurations can have unintended side effects, some of which may be security- or privacy-relevant. Detecting such changes early in the process can help avoid unintended, negative consequences that could ultimately affect the security and privacy posture of systems. The configuration change management and control process in this control enhancement refers to the change management and control process defined by organizations in SA-10B.

Related controls and activities: None.

References:

- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)

SA-11 Developer testing and evaluation

Activity: At all post-design stages of the system development lifecycle, require the developer of the system, system component, or system service to:

- develop and implement a plan for ongoing security and privacy control assessments
- perform [Selection (1 or more): unit; integration; system; regression] testing/evaluation [Assignment: organization-defined frequency] at [Assignment: organization-defined depth and coverage]
- produce evidence of the execution of the assessment plan and the results of the testing and evaluation
- implement a verifiable flaw remediation process
- correct flaws identified during testing and evaluation

Discussion: Developmental testing and evaluation confirm that the required controls are implemented correctly, operating as intended, enforcing the desired security and privacy policies, and meeting established security and privacy requirements. Security properties of systems and the privacy of individuals may be affected by the interconnection of system components or changes to those components. The interconnections or changes—including upgrading or replacing applications, operating systems, and firmware—may adversely affect previously implemented controls.

Ongoing assessment during development allows for additional types of testing and evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications may require approaches such as manual code review, security architecture review, and penetration testing, as well as static analysis, dynamic analysis, binary analysis, or a hybrid of the 3 analysis approaches.

Developers can use the analysis approaches, along with security instrumentation and fuzzing, in a variety of tools and in source code reviews. The security and privacy assessment plans include the specific activities that developers plan to carry out, including the types of analyses, testing, evaluation, and reviews of software and firmware components; the degree of rigour to be applied; the frequency of the ongoing testing and evaluation; and the types of artifacts produced during those processes.

The depth of testing and evaluation refers to the rigour and level of detail associated with the assessment process. The coverage of testing and evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security and privacy assessment plans, flaw remediation processes, and the evidence that the plans and processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or classification level of the system. Contracts may specify protection requirements for documentation.

Related controls and activities: CA-02, CA-07, CM-04, SA-03, SA-04, SA-05, SA-08, SA-15, SA-17, SI-02, SR-05, SR-06, SR-07.

Enhancements:

(01) Developer testing and evaluation: Static code analysis

Require the developer of the system, system component, or system service to employ static code analysis tools to identify common flaws and to document the results of the analysis.

Discussion: Static code analysis provides a technology and methodology for security reviews and includes checking for weaknesses in the code as well as for the incorporation of libraries or other included code that contain known vulnerabilities or that are out of date and not supported. Static code analysis can be used to identify vulnerabilities and enforce secure coding practices. It is most effective when used early in the development process, when each code change can automatically be scanned for potential weaknesses. Static code analysis can provide clear remediation guidance and identify defects for developers to fix. Evidence of the correct implementation of static analysis can include aggregate defect density for critical defect types; evidence that defects were inspected by developers or security professionals; and evidence that defects were remediated. A high density of ignored findings, commonly referred to as false positives, indicates a potential problem with the analysis process or the analysis tool. In such cases, organizations weigh the validity of the evidence against evidence from other sources.

Related controls and activities: None.

(02) Developer testing and evaluation: Threat modelling and vulnerability analyses

Require the developer of the system, system component, or system service to perform threat modelling and vulnerability analyses during the development and the subsequent testing and evaluation of the system, component, or service that:

- a. uses the following contextual information: [Assignment: organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels]
- b. employs the following tools and methods: [Assignment: organization-defined tools and methods]
- c. conducts the modelling and analyses at the following level of rigour: [Assignment: organization-defined breadth and depth of modelling and analyses]
- d. produces evidence that meets the following acceptance criteria: [Assignment: organization-defined acceptance criteria]

Discussion: Systems, system components, and system services may deviate significantly from the functional and design specifications created during the requirements and design stages of the system development lifecycle. Therefore, updates to threat modelling and vulnerability analyses of those systems, system components, and system services during development and prior to delivery are critical to the effective operation of those systems, components, and services. Threat modelling and vulnerability analyses at this stage of the system development

lifecycle ensure that design and implementation changes have been accounted for and that vulnerabilities created because of those changes have been reviewed and mitigated.

Related controls and activities: PM-15, RA-03, RA-05.

(03) **Developer testing and evaluation: Independent verification of assessment plans and evidence**

- a. Require an independent agent satisfying [Assignment: organization-defined independence criteria] to verify the correct implementation of the developer security and privacy assessment plans and the evidence produced during testing and evaluation
- b. Verify that the independent agent is provided with sufficient information to complete the verification process or granted the authority to obtain such information

Discussion: Independent agents have the qualifications—including the expertise, skills, training, certifications, and experience—to verify the correct implementation of developer security and privacy assessment plans.

Related controls and activities: AT-03, RA-05.

(04) **Developer testing and evaluation: Manual code reviews**

Require the developer of the system, system component, or system service to perform a manual code review of [Assignment: organization-defined specific code] using the following processes, procedures, and/or techniques: [Assignment: organization-defined processes, procedures, and/or techniques].

Discussion: Manual code reviews are usually reserved for the critical software and firmware components of systems. Manual code reviews are effective at identifying weaknesses that require knowledge of the application's requirements or context that, in most cases, is unavailable to automated analytic tools and techniques, such as static and dynamic analysis. The benefits of manual code review include the ability to verify access control matrices against application controls and review detailed aspects of cryptographic implementations and controls.

Related controls and activities: None.

(05) **Developer testing and evaluation: Penetration testing**

Require the developer of the system, system component, or system service to perform penetration testing:

- a. at the following level of rigour: [Assignment: organization-defined breadth and depth of testing]
- b. under the following constraints: [Assignment: organization-defined constraints]

Discussion: Penetration testing is an assessment methodology in which assessors, using all available IT product or system documentation and working under specific constraints, attempt to circumvent the implemented security and privacy features of IT products and systems.

Useful information for assessors who conduct penetration testing includes product and system design specifications, source code, and administrator and operator manuals. Penetration testing can include open-box, grey-box, or closed-box testing with analyses performed by skilled professionals who simulate adversary actions.

The objective of penetration testing is to discover vulnerabilities in systems, system components, and services that result from implementation errors, configuration faults, or other operational weaknesses or deficiencies. Penetration tests can be performed in conjunction with automated and manual code reviews to provide a greater level of analysis than would ordinarily be possible.

When user session information and other personal information is captured or recorded during penetration testing, such information is handled appropriately to protect privacy.

Related controls and activities: CA-08, PM-14, PM-25, PT-02, SA-03, SI-02, SI-06.

(06) **Developer testing and evaluation: Attack surface reviews**

Require the developer of the system, system component, or system service to perform attack surface reviews.

Discussion: Attack surfaces of systems and system components are exposed areas that make those systems more vulnerable to attacks. Attack surfaces include any accessible areas where weaknesses or deficiencies in the hardware, software, and firmware components provide opportunities for adversaries to exploit vulnerabilities. Attack surface reviews ensure that developers analyze the design and implementation changes to systems and mitigate attack vectors generated as a result of the changes. The correction of identified flaws includes deprecation of unsafe functions.

Related controls and activities: SA-15.

(07) **Developer testing and evaluation: Verify scope of testing and evaluation**

Require the developer of the system, system component, or system service to verify that the scope of testing and evaluation provides complete coverage of the required controls at the following level of rigour: [Assignment: organization-defined breadth and depth of testing and evaluation].

Discussion: Verifying that testing and evaluation provides complete coverage of required controls can be accomplished by a variety of informal and formal analytic techniques. Each of these techniques provides an increasing level of assurance that corresponds to the degree of formality of the analysis. Rigorously demonstrating control coverage at the highest levels of assurance can be achieved using formal modelling and analysis techniques, including correlation between control implementation and corresponding test cases.

Related controls and activities: SA-15.

(08) **Developer testing and evaluation: Dynamic code analysis**

Require the developer of the system, system component, or system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.

Discussion: Dynamic code analysis provides runtime verification of software programs using tools capable of monitoring programs for memory corruption, user privilege issues, and other potential security problems. Dynamic code analysis employs runtime tools to ensure that security functionality performs in the way it was designed.

A type of dynamic analysis, known as fuzz testing, induces program failures by deliberately introducing malformed or random data into software programs. Fuzz testing strategies are derived from the intended use of applications and the functional and design specifications for the applications.

To understand the scope of dynamic code analysis and the assurance provided, organizations may also consider conducting code coverage analysis (i.e., checking the degree to which the code has been tested using metrics such as percentage of subroutines tested or percentage of program statements called during execution of the test suite) and/or concordance analysis (i.e., checking for words that are out of place in software code, such as non-English or non-French language words or derogatory terms).

Related controls and activities: None.

(09) **Developer testing and evaluation: Interactive application security testing**

Require the developer of the system, system component, or system service to employ interactive application security testing tools to identify flaws and document the results.

Discussion: Interactive (also known as instrumentation-based) application security testing is a method of detecting vulnerabilities by observing applications as they run during testing. The use of instrumentation relies on direct measurements of the actual running applications and uses access to the code, user interaction, libraries, frameworks, backend connections, and configurations to directly measure control effectiveness.

When combined with analysis techniques, interactive application security testing can identify potential vulnerabilities and confirm control effectiveness. Instrumentation-based testing works in real time and can be used continuously throughout the system development lifecycle.

Related controls and activities: None.

References:

- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [TBS Security Playbook for Information System Solutions](#)
- [ISO/IEC 15408-3 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security, Part 3: Security assurance components](#)
- [CSE-RCMP Harmonized Threat and Risk Assessment Methodology \(TRA-1\)](#)

SA-12 Supply chain protection

Withdrawn: Moved to SR Family.

Enhancements:**(01) Supply chain protection: Acquisition strategies / tools / methods**

Withdrawn: Moved to SR-05.

(02) Supply chain protection: Supplier reviews

Withdrawn: Moved to SR-06.

(03) Supply chain protection: Trusted shipping and warehousing

Withdrawn: Incorporated into SR-03.

(04) Supply chain protection: Diversity of suppliers

Withdrawn: Moved to SR-03(01).

(05) Supply chain protection: Limitation of harm

Withdrawn: Moved to SR-03(02).

(06) Supply chain protection: Minimizing procurement time

Withdrawn: Incorporated into SR-05(01).

(07) Supply chain protection: Assessments prior to selection / acceptance / update

Withdrawn: Moved to SR-05(02).

(08) Supply chain protection: Use of all-source intelligence

Withdrawn: Incorporated into RA-03(02).

(09) Supply chain protection: Operations security

Withdrawn: Moved to SR-07.

(10) Supply chain protection: Validate as genuine and not altered

Withdrawn: Moved to SR-04(03).

(11) Supply chain protection: Penetration testing / analysis of elements, processes, and actors

Withdrawn: Moved to SR-06(01).

(12) Supply chain protection: Inter-organizational agreements

Withdrawn: Moved to SR-08.

(13) Supply chain protection: Critical information system components

Withdrawn: Incorporated into MA-06 and RA-09.

(14) Supply chain protection: Identity and traceability

Withdrawn: Moved to SR-04(01) and SR-04(02).

(15) Supply chain protection: Processes to address weaknesses or deficiencies

Withdrawn: Incorporated into SR-03.

SA-13 Trustworthiness

Withdrawn: Incorporated into SA-08.

SA-14 Criticality analysis

Withdrawn: Incorporated into RA-09.

Enhancements:**(01) Criticality analysis: Critical components with no viable alternative sourcing**

Withdrawn: Incorporated into SA-20.

SA-15 Development process, standards, and tools

Activity:

- A.** Require the developer of the system, system component, or system service to follow a documented development process that
 - 1. explicitly addresses security and privacy requirements
 - 2. identifies the standards and tools used in the development process
 - 3. documents the specific tool options and tool configurations used in the development process
 - 4. documents, manages, and ensures the integrity of changes to the process and/or tools used in development
- B.** Review the development process, standards, tools, tool options, and tool configurations [Assignment: organization-defined frequency] to determine if the process, standards, tools, tool options, and tool configurations selected and employed can satisfy the following security and privacy requirements: [Assignment: organization-defined security and privacy requirements]

Discussion: Development tools include programming languages and computer-aided design systems. Reviews of development processes include the use of maturity models to determine the potential effectiveness of such processes. Maintaining the integrity of changes to tools and processes facilitates effective supply chain risk assessment and mitigation. Such integrity requires configuration control throughout the system development lifecycle to track authorized changes and prevent unauthorized changes.

Related controls and activities: MA-06, SA-03, SA-04, SA-08, SA-10, SA-11, SI-02, SR-03, SR-04, SR-05, SR-06, SR-09.

Enhancements:**(01) Development process, standards, and tools: Quality metrics**

Require the developer of the system, system component, or system service to:

- a. define quality metrics at the beginning of the development process
- b. provide evidence of meeting the quality metrics [Selection (1 or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined program review milestones]; upon delivery]

Discussion: Organizations use quality metrics to establish acceptable levels of system quality. Metrics can include quality gates, which are collections of completion criteria or sufficiency standards that represent the satisfactory execution of specific phases of the system development project. For example, a quality gate may require the elimination of all compiler warnings or a determination that such warnings have no impact on the effectiveness of required security or privacy capabilities. During the execution phases of development projects, quality gates provide clear, unambiguous indications of progress. Other metrics apply to the entire development project. Metrics can include defining the severity thresholds of vulnerabilities in accordance with organizational risk tolerance, such as requiring no known vulnerabilities in the delivered system with a CVSS severity of medium or high.

Related controls and activities: None.

(02) **Development process, standards, and tools: Security and privacy control traceability tools**

Require the developer of the system, system component, or system service to select and employ security and privacy controls traceability tools for use during the development process.

Discussion: The objective is to create a security and privacy requirements traceability matrix. System development teams select and deploy security and privacy tracking tools, including vulnerability or work item tracking systems that facilitate assignment, sorting, filtering, and tracking of completed work items or tasks associated with development processes.

Related controls and activities: SA-11.

(03) **Development process, standards, and tools: Criticality analysis**

Require the developer of the system, system component, or system service to perform a criticality analysis:

- a. at the following decision points in the system development lifecycle: [Assignment: organization-defined decision points in the system development lifecycle]
- b. at the following level of rigour: [Assignment: organization-defined breadth and depth of criticality analysis]

Discussion: Criticality analysis performed by the developer provides input to the criticality analysis performed by organizations. Developer input is essential to organizational criticality analysis because organizations may not have access to detailed design documentation for system components that are developed as COTS products. Such design documentation includes functional specifications, high-level designs, low-level designs, source code, and hardware schematics.

Criticality analysis is important for organizational systems that are designated as high-value assets. High-value assets can be moderate- or high-impact systems due to heightened adversarial interest or potential adverse effects on the federal enterprise. Developer input is especially important when organizations conduct supply chain criticality analyses.

Related controls and activities: RA-09.

(04) **Development process, standards, and tools: Threat modelling and vulnerability analysis**

Withdrawn: Incorporated into SA-11(02).

(05) **Development process, standards, and tools: Attack surface reduction**

Require the developer of the system, system component, or system service to reduce attack surfaces to [Assignment: organization-defined thresholds].

Discussion: Attack surface reduction is closely aligned with threat and vulnerability analyses and system architecture and design. Attack surface reduction is a means of reducing risk to organizations by giving attackers less opportunity to exploit weaknesses or deficiencies (i.e., potential vulnerabilities) within systems, system components, and system services. Attack surface reduction includes implementing the concept of layered defences, applying the principles of least privilege and least functionality, applying secure software development practices,

deprecating unsafe functions, reducing entry points available to unauthorized users, reducing the amount of code that executes, and eliminating APIs that are vulnerable to attacks.

Related controls and activities: AC-06, CM-07, RA-03, SA-11.

(06) **Development process, standards, and tools: Continuous improvement**

Require the developer of the system, system component, or system service to implement an explicit process to continuously improve the development process.

Discussion: Developers of systems, system components, and system services consider the effectiveness and efficiency of their development processes in meeting quality objectives and addressing the security and privacy capabilities in current threat environments.

Related controls and activities: None.

(07) **Development process, standards, and tools: Automated vulnerability analysis**

Require the developer of the system, system component, or system service [Assignment: organization-defined frequency] to:

- a. perform an automated vulnerability analysis using [Assignment: organization-defined tools]
- b. determine the exploitation potential for discovered vulnerabilities
- c. determine potential risk mitigations for delivered vulnerabilities
- d. deliver the outputs of the tools and results of the analysis to [Assignment: organization-defined personnel or roles]

Discussion: Automated tools can be more effective at analyzing exploitable weaknesses or deficiencies in large and complex systems, prioritizing vulnerabilities by severity, and providing recommendations for risk mitigations.

Related controls and activities: RA-05, SA-11.

(08) **Development process, standards, and tools: Reuse of threat and vulnerability information**

Require the developer of the system, system component, or system service to use threat modelling and vulnerability analyses from similar systems, components, or services to inform the current development process.

Discussion: Analysis of vulnerabilities found in similar software applications can inform potential design and implementation issues for systems under development. Similar systems or system components may exist within developer organizations. Vulnerability information is available from a variety of public and private sector sources, including the [NIST National Vulnerability Database](#).

Related controls and activities: None.

(09) **Development process, standards, and tools: Use of live data**

Withdrawn: Incorporated into SA-03(02).

(10) **Development process, standards, and tools: Incident response plan**

Require the developer of the system, system component, or system service to provide, implement, and test an incident response plan.

Discussion: The incident response plan provided by developers may provide information not readily available to organizations and may be incorporated into organizational incident response plans. Developer information may also be extremely helpful, such as when organizations respond to vulnerabilities in COTS products.

Related controls and activities: IR-08.

(11) **Development process, standards, and tools: Archive system or component**

Require the developer of the system or system component to archive the system or component to be released or delivered together with the corresponding evidence supporting the final security and privacy review.

Discussion: Archiving system or system components requires the developer to retain key development artifacts, including hardware specifications, source code, object code, and relevant documentation from the development process that can provide a readily available configuration baseline for system and component upgrades or modifications.

Related controls and activities: CM-02.

(12) **Development process, standards, and tools: Minimize personal information**

Require the developer of the system or system component to minimize the use of personal information in development and test environments.

Discussion: Organizations can minimize the risk to an individual's privacy by using techniques such as de-identification or synthetic data. Limiting the use of personal information in development and test environments helps reduce the level of privacy risk created by a system.

GC discussion: Development and test environments should not be conducted using identifiable personal information, except in exceptional circumstances. It is recommended that system testing be completed using dummy data, scrambled data, or personal information that is otherwise obfuscated. At times, system testing may be outsourced. Even with obfuscated personal information, it is recommended that contracting documents require the deletion of testing data by the third-party vendor when development or testing is complete, to protect against the possibility of re-identification and breach.

Related controls and activities: PM-25, SA-03, SA-08.

(13) **Development process, standards, and tools: Logging syntax**

Require the developer of the system, system component, or system service to use [Assignment: organization-defined secure logging format] to log [assignment: organization-defined event types] at [assignment: organization-defined level of detail].

Discussion: In support of better incident response and the ability to more quickly reconstruct security-related actions, identifying specific requirements for secure logging facilitates the ability to connect application-produced audit event logs with operational data. Event types are consistent with the event types defined in AU-02.

Related controls and activities: AU-02, AU-03, IR-04, IR-08, SA-05. **References:**

- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [TBS Security Playbook for Information System Solutions](#)
- [CSE-RCMP Harmonized Threat and Risk Assessment Methodology \(TRA-1\)](#)

SA-16 Developer-provided training

Control: Require the developer of the system, system component, or system service to provide the following training on the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms: [Assignment: organization-defined training].

Discussion: Developer-provided training applies to external and internal (in-house) developers. Personnel training is essential to ensuring the effectiveness of the controls implemented within organizational systems. Training may be web-based, computer-based, classroom style, or hands-on (including micro-training). Organizations can also request training materials from developers to conduct in-house training or offer self-training to organizational personnel. Organizations determine the type of training necessary and may require different types of training for different security and privacy functions, controls, and mechanisms.

Related controls and activities: AT-02, AT-03, PE-03, SA-04, SA-05.

Enhancements: None.

References: [TBS Directive on Security Management, Appendix H: Mandatory Procedures for Security Awareness and Training Control](#)

SA-17 Developer security and privacy architecture and design

Activity: Require the developer of the system, system component, or system service to produce a design specification and security and privacy architecture that:

- A. is consistent with the organization's security and privacy architecture that is an integral part the organization's enterprise architecture
- B. accurately and completely describes the required security and privacy functionality and the allocation of controls among physical and logical components
- C. expresses how individual security and privacy functions, mechanisms, and services work together to provide required security and privacy capabilities and a unified approach to protection

Discussion: Developer security and privacy architecture and design are directed at external developers, although they could also be applied to internal (in-house) development. In contrast, PL-08 is directed at internal developers to ensure that organizations develop a security and privacy architecture that is integrated with the enterprise architecture. The distinction between SA-17 and PL-08 is especially important when organizations outsource the development of systems, system components, or system services and when there is a requirement to demonstrate consistency with the enterprise architecture and security and privacy architecture of the organization.

ISO/IEC 15408-2, ISO/IEC 15408-3, and the Cyber Centre's System lifecycle cyber security and privacy risk management activities (ITSP.10.037) provide information on security architecture and design, including formal policy models, security-relevant components, formal and informal correspondence, conceptually simple design, and structuring for least privilege and testing.

Related controls and activities: PL-02, PL-08, PM-07, SA-03, SA-04, SA-08, SC-07.

Enhancements:

(01) Developer security and privacy architecture and design: Formal policy model

Require the developer of the system, system component, or system service to:

- a. produce, as an integral part of the development process, a formal policy model describing the [Assignment: organization-defined elements of organizational security and privacy policy] to be enforced
- b. prove that the formal policy model is internally consistent and sufficient to enforce the defined elements of the organizational security and privacy policy when implemented

Discussion: Formal models describe specific behaviours or security and privacy policies using formal languages, thus enabling the correctness of those behaviours and policies to be formally proven. Not all components of systems can be modelled. Generally, formal specifications are scoped to the behaviours or policies of interest, such as non-discretionary access control policies. Organizations choose the formal modelling language and approach based on the nature of the behaviours and policies to be described and the available tools.

Related controls and activities: AC-03, AC-04, AC-25.

(02) Developer security and privacy architecture and design: Security-relevant components

Require the developer of the system, system component, or system service to:

- a. define security-relevant hardware, software, and firmware

- b. provide a rationale that the definition for security-relevant hardware, software, and firmware is complete

Discussion: The security-relevant hardware, software, and firmware represent the portion of the system, component, or service that is trusted to perform correctly to maintain required security properties.

Related controls and activities: AC-25, SA-05.

(03) **Developer security and privacy architecture and design: Formal correspondence**

Require the developer of the system, system component, or system service to:

- a. produce, as an integral part of the development process, a formal top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects
- b. show, via proof to the extent feasible with additional informal demonstration as necessary, that the formal top-level specification is consistent with the formal policy model
- c. show, via informal demonstration, that the formal top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware
- d. show that the formal top-level specification is an accurate description of the implemented security-relevant hardware, software, and firmware
- e. describe the security-relevant hardware, software, and firmware mechanisms not addressed in the formal top-level specification but strictly internal to the security-relevant hardware, software, and firmware

Discussion: Correspondence is an important part of the assurance gained through modelling. It demonstrates that the implementation is an accurate transformation of the model, and that any additional code or implementation details that are present have no impact on the behaviours or policies being modelled.

Formal methods can be used to show that the high-level security properties are satisfied by the formal system description, and that the formal system description is correctly implemented by a description of some lower level, including a hardware description.

Consistency between the formal top-level specification and the formal policy models is generally not amenable to being fully proven. Therefore, a combination of formal and informal methods may be needed to demonstrate such consistency. Consistency between the formal top-level specification and the actual implementation may require the use of an informal demonstration due to limitations on the applicability of formal methods to prove that the specification accurately reflects the implementation. Hardware, software, and firmware mechanisms internal to security-relevant components include mapping registers and direct memory input and output.

Related controls and activities: AC-03, AC-04, AC-25, SA-04, SA-05.

(04) **Developer security and privacy architecture and design: Informal correspondence**

Require the developer of the system, system component, or system service to:

- a. produce, as an integral part of the development process, an informal descriptive top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects
- b. show, via [Selection (1): informal demonstration; convincing argument with formal methods as feasible], that the descriptive top-level specification is consistent with the formal policy model
- c. show, via informal demonstration, that the descriptive top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware
- d. show that the descriptive top-level specification is an accurate description of the interfaces to security-relevant hardware, software, and firmware

- e. describe the security-relevant hardware, software, and firmware mechanisms not addressed in the descriptive top-level specification but strictly internal to the security-relevant hardware, software, and firmware

Discussion: Correspondence is an important part of the assurance gained through modelling. It demonstrates that the implementation is an accurate transformation of the model, and that additional code or implementation detail has no impact on the behaviours or policies being modelled. Consistency between the descriptive top-level specification (i.e., high-level/low-level design) and the formal policy model is generally not amenable to being fully proven. Therefore, a combination of formal and informal methods may be needed to show such consistency. Hardware, software, and firmware mechanisms strictly internal to security-relevant hardware, software, and firmware include mapping registers and direct memory input and output.

Related controls and activities: AC-03, AC-04, AC-25, SA-04, SA-05.

(05) **Developer security and privacy architecture and design: Conceptually simple design**

Require the developer of the system, system component, or system service to:

- a. design and structure the security-relevant hardware, software, and firmware to use a complete, conceptually simple protection mechanism with precisely defined semantics
- b. internally structure the security-relevant hardware, software, and firmware with specific regard for this mechanism

Discussion: The principle of reduced complexity states that the system design is as simple and small as possible (see SA-08(07)). A small and simple design is easier to understand and analyze and is also less prone to error (see AC-25, SA-08(13)). The principle of reduced complexity applies to any aspect of a system, but it has particular importance for security due to the various analyses performed to obtain evidence about the emergent security property of the system. For such analyses to be successful, a small and simple design is essential.

Application of the principle of reduced complexity helps system developers to understand the correctness and completeness of system security functions and facilitates the identification of potential vulnerabilities. The corollary of reduced complexity states that the simplicity of the system is directly related to the number of vulnerabilities it will contain. That is, simpler systems contain fewer vulnerabilities.

Two important benefits of reduced complexity are that it is easier to understand whether the security policy has been captured in the system design and that fewer vulnerabilities are likely to be introduced during engineering development. An additional benefit is that any such conclusion about correctness, completeness, and existence of vulnerabilities can be reached with a higher degree of assurance in contrast to conclusions reached in situations where the system design is inherently more complex.

Related controls and activities: AC-25, SA-08, SC-03.

(06) **Developer security and privacy architecture and design: Structure for testing**

Require the developer of the system, system component, or system service to structure security-relevant hardware, software, and firmware to facilitate testing.

Discussion: Applying the security design principles in NIST SP 800-160 Volume 1 Revision 1 and the development framework in System lifecycle cyber security and privacy risk management activities (ITSP.10.037) promote complete, consistent, and comprehensive testing and evaluation of systems, system components, and services. The thoroughness of such testing contributes to the evidence produced to generate an effective assurance case or argument as to the robustness of the system, system component, or service.

Related controls and activities: SA-05, SA-11.

(07) **Developer security and privacy architecture and design: Structure for least privilege**

Require the developer of the system, system component, or system service to structure security-relevant hardware, software, and firmware to facilitate controlling access with least privilege.

Discussion: The principle of least privilege states that each component is allocated sufficient privileges to accomplish its specified functions but no more (see SA-08(14)). Applying the principle of least privilege limits the scope of the component's actions, which has 2 desirable effects. First, the security impact of a failure, corruption, or misuse of the system component results in a minimized security impact. Second, the security analysis of the component is simplified.

Least privilege is a pervasive principle that is reflected in all aspects of the secure system design. Interfaces used to invoke component capability are available to only certain subsets of the user population, and component design supports a sufficiently fine granularity of privilege decomposition.

For example, in the case of an audit mechanism, there may be an interface for the audit manager, who configures the audit settings; an interface for the audit operator, who ensures that audit data is safely collected and stored; and, finally, yet another interface for the audit reviewer, who only has a need to view the audit data that has been collected but no need to perform operations on that data.

In addition to its manifestations at the system interface, least privilege can be used as a guiding principle for the internal structure of the system itself. One aspect of internal least privilege is to construct modules so that only the elements encapsulated by the module are directly operated upon by the functions within the module. Elements external to a module that may be affected by the module's operation are indirectly accessed through interaction (e.g., via a function call) with the module that contains those elements.

Another aspect of internal least privilege is that the scope of a given module or component includes only those system elements that are necessary for its functionality, and the access modes to the elements (e.g., read, write) are minimal.

Related controls and activities: AC-05, AC-06, SA-08.

(08) **Developer security and privacy architecture and design: Orchestration**

Design [Assignment: organization-defined critical systems or system components] with coordinated behaviour to implement the following capabilities: [Assignment: organization-defined capabilities, by system or component].

Discussion: Security resources that are distributed, located at different layers or in different system elements can interact in unforeseen or incorrect ways. Adverse consequences can include cascading failures, interference, or coverage gaps. Coordination of the behaviour of security resources (e.g., by ensuring that one patch is installed across all resources before making a configuration change that assumes that the patch is propagated) can avert such negative interactions.

Related controls and activities: None.

(09) **Developer security and privacy architecture and design: Design diversity**

Use different designs for [Assignment: organization-defined critical systems or system components] to satisfy a common set of requirements or to provide equivalent functionality.

Discussion: Design diversity is achieved by supplying the same requirements specification to multiple developers, each of whom is responsible for developing a variant of the system or system component that meets the requirements. Variants can be in software design, in hardware design, or in both hardware and a software design. Differences in the designs of the variants can result from developer experience (e.g., prior use of a design pattern), design style (e.g., when decomposing a required function into smaller tasks, determining what constitutes a separate task and how far to decompose tasks into sub-tasks), selection of libraries to incorporate into the variant, and the development environment (e.g., different design tools make some design patterns easier to visualize).

Hardware design diversity includes making different decisions about what information to keep in analog form and what information to convert to digital form, transmitting the same information at different times, and introducing delays in sampling (temporal diversity). Design diversity is commonly used to support fault tolerance.

Related controls and activities: None.

References:

- [ISO/IEC 15408-2 Information security, cybersecurity, and privacy protection – Evaluation criteria for IT security, Part 2: Security functional components](#)
- [ISO/IEC 15408-3 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security, Part 3: Security assurance components](#)
- System lifecycle cyber security and privacy risk management activities (ITSP.10.037)
- [NIST SP 800-160 Volume 1 Revision 1, Engineering Trustworthy Secure Systems](#)

SA-18 Tamper resistance and detection

Withdrawn: Moved to SR-09.

Enhancements:

(01) **Tamper resistance and detection: Multiple phases of system development lifecycle**

Withdrawn: Moved to SR-09(01).

(02) **Tamper resistance and detection: Inspection of systems or components**

Withdrawn: Moved to SR-10.

SA-19 Component authenticity

Withdrawn: Moved to SR-11.

Enhancements:

(01) **Component authenticity: Anti-counterfeit training**

Withdrawn: Moved to SR-11(01).

(02) **Component authenticity: Configuration control for component service and repair**

Withdrawn: Moved to SR-11(02).

(03) **Component authenticity: Component disposal**

Withdrawn: Moved to SR-12.

(04) **Component authenticity: Anti-counterfeit scanning**

Withdrawn: Moved to SR-11(03).

SA-20 Customized development of critical components

Control: Reimplement or custom develop the following critical system components: [Assignment: organization-defined critical system components].

Discussion: Organizations determine that certain system components likely cannot be trusted due to specific threats to and vulnerabilities in those components for which there are no viable security controls to adequately mitigate risk. Reimplementation or custom development of such components may satisfy requirements for higher assurance and is

carried out by initiating changes to system components (including hardware, software, and firmware) such that the standard attacks by adversaries are less likely to succeed.

In situations where no alternative sourcing is available and organizations choose not to reimplement or custom develop critical system components, additional controls can be employed. Controls include enhanced auditing, restrictions on source code and system utility access, and protection from deletion of system and application files.

Related controls and activities: CP-02, RA-09, SA-08.

Enhancements: None.

References: System lifecycle cyber security and privacy risk management activities (ITSP.10.037)

SA-21 Developer screening

Control: Require that the developer of [Assignment: organization-defined system, system component, or system service]:

- A. has appropriate access authorizations as determined by assigned [Assignment: organization-defined official government duties]
- B. satisfies the following additional personnel screening criteria: [Assignment: organization-defined additional personnel screening criteria]

Discussion: Developer screening is directed at external developers. Internal developer screening is addressed by PS-03. Because the system, system component, or system service may be used in critical activities essential to the national or economic security interests of Canada, organizations have a strong interest in ensuring that developers are trustworthy. The degree of trust required of developers may need to be consistent with that of the individuals who access the systems, system components, or system services once deployed.

Authorization and personnel screening criteria include clearances, background checks, citizenship, and nationality. Developer trustworthiness may also include a review and analysis of company ownership and relationships that the company has with entities that may potentially affect the quality and reliability of the systems, components, or services being developed.

Satisfying the required access authorizations and personnel screening criteria includes providing a list of all individuals who are authorized to perform development activities on the selected system, system component, or system service so that organizations can validate that the developer has satisfied the authorization and screening requirements.

Related controls and activities: PS-02, PS-03, PS-06, PS-07, SA-04, SR-06.

Enhancements:

(01) **Developer screening: Validation of screening**

Withdrawn: Incorporated into SA-21.

References:

- [PSPC Contract Security Manual](#)
- [TBS Directive on Security Management, Appendix A: Mandatory Procedures for Security Screening Control](#)

SA-22 Unsupported system components

Control:

- A. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer

- B.** Provide the following options for alternative sources for continued support for unsupported components [Selection (1 or more): in-house support; [Assignment: organization-defined support from external providers]]

Discussion: Support for system components includes software patches, firmware updates, replacement parts, and maintenance contracts. An example of unsupported components is when vendors no longer provide critical software patches or product updates, which can result in an opportunity for adversaries to exploit weaknesses in the installed components. Exceptions to replacing unsupported system components include systems that provide critical mission or business capabilities where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option.

Alternative sources for support address the need to provide continued support for system components that are no longer supported by the original manufacturers, developers, or vendors when such components remain essential to organizational mission and business functions. If necessary, organizations can establish in-house support by developing customized patches for critical software components or, alternatively, obtain the services of external providers who provide ongoing support for the designated unsupported components through contractual relationships. Such contractual relationships can include open-source software value-added vendors. The increased risk of using unsupported system components can be mitigated, for example, by prohibiting the connection of such components to public or uncontrolled networks or implementing other forms of isolation.

Related controls and activities: PL-02, SA-03, SA-400.

Enhancements:

(01) **Unsupported system components: Alternative sources for continued support**

Withdrawn: Incorporated into SA-22.

References: [TBS Directive on Service and Digital, Appendix H: Standard on At-Risk Information Technology](#)

SA-23 Specialization

Activity: Employ [Selection (1 or more): design; modification; augmentation; reconfiguration] on [Assignment: organization-defined systems or system components] supporting mission-essential services or functions to increase the robustness in those systems or components.

Discussion: It is often necessary to enhance a system or system component that supports mission-essential services or functions to maximize the robustness of the resource. Sometimes this enhancement is done at the design level. In other instances, it is done post-design, either by modifying the system in question or by augmenting the system with additional components. For example, supplemental authentication or non-repudiation functions may be added to the system to enhance the identity of critical resources to other resources that depend on the organization-defined resources.

Related controls and activities: RA-09, SA-08.

Enhancements: None.

References: System lifecycle cyber security and privacy risk management activities (ITSP.10.037)

SA-24 Design for cyber resiliency

Control:

- A.** Design organizational systems, system components, or system services to achieve cyber resiliency by:
1. defining the following cyber resiliency goals: [Assignment: organization-defined cyber resiliency goals]
 2. defining the following cyber resiliency objectives: [Assignment: organization-defined cyber resiliency objectives]

3. defining the following cyber resiliency techniques: [Assignment: organization-defined cyber resiliency techniques]
 4. defining the following cyber resiliency implementation approaches: [Assignment: organization-defined cyber resiliency implementation approaches]
 5. defining the following cyber resiliency design principles: [Assignment: organization-defined cyber resiliency design principles]
- B. Implement and review the selected cyber resiliency goals, objectives, techniques, implementation approaches, and design principles as part of an organizational risk management process or systems security engineering process

Discussion: Cyber resiliency is critical to ensuring the survivability of mission-critical systems and high value assets. Cyber resiliency focuses on limiting the damage from adversity or the conditions that can cause a loss of assets. Damage can affect (1) organizations (for example, loss of reputation, increased existential risk), (2) mission or business functions (for example, decreased capability to complete current missions and to accomplish future missions), (3) security (for example, decreased capability to achieve security objectives or to prevent, detect, and respond to cyber incidents), (4) systems (for example, unauthorized use of system resources or decreased capability to meet system requirements), or (5) specific system elements (for example, physical destruction; corruption, modification, or fabrication of information).

Cyber resiliency goals are intended to help organizations maintain a state of informed preparedness for adversity, continue essential mission or business functions despite adversity, restore mission or business functions during and after adversity, and modify mission or business functions and their supporting capabilities in response to predicted changes in technical, operational, or threat environments.

NIST SP 800-160 Volume 2 Revision 1 provides additional information on the Cyber Resiliency Engineering Framework, including detailed descriptions of cyber resiliency goals, objectives, techniques, implementation approaches, and design principles. NIST SP 800-160 Volume 1 Revision 1 provides additional information on achieving cyber resiliency as an emergent property of an engineered system.

Related controls and activities: CA-07, CP-02, CP-04, CP-09, CP-10, CP-11, CP-12, CP-13, IR-04, IR-05, PE-11, PE-12, PE-17, PL-08, PM-07, PM-16, PM-30, PM-31, RA-03, RA-05, RA-09, SA-03, SA-08, SA-09, SA-17, SC-03, SC-05, SC-07, SC-10, SC-11, SC-29, SC-30, SC-34, SC-35, SC-36, SC-37, SC-39, SC-44, SC-47, SC-48, SC-49, SC-50, SC-51, SI-03, SI-04, SI-14, SI-17, SI-20, SI-21, SI-22, SI-23, SR-03, SR-04, SR-05, SR-07.

Enhancements: None.

References:

- [NIST SP 800-160 Volume 1 Revision 1, Engineering Trustworthy Secure Systems](#)
- [NIST SP 800-160 Volume 2 Revision 1, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach](#)

SA-400 Sovereignty and jurisdiction

Control: Require the organizational business function to conduct a sovereignty and jurisdiction threat and risk assessment process at the [Selection (1 or more): organization-level, mission/business-level, system-level] that:

- A. conducts an injury assessment to determine the maximum potential injuries that may be suffered due to external legal compulsion of the business functions or information assets by
 1. considering the business needs for security including any laws or regulations which require that data not be disclosed or compromised
 2. updating the security categorization of the business functions or information assets
 3. documenting the negative consequences of legal compulsion
- B. performs jurisdiction-specific threat assessment that establishes a likelihood of being targeted

- C. undertakes a vulnerability assessment to evaluate the potential means by which the external jurisdiction could exploit the business functions or information assets
- D. completes a jurisdiction-specific risk assessment

Discussion: Data sovereignty refers to Canada's right to control access to and disclosure of digital information that is subject to its legislation. Data residency refers to the physical or geographical location of an organization's data while at rest. Jurisdiction refers to a realm of authority, which in this context, references the ability to compel compliance from entities within that realm as the key threat.

A concern with having data hosted in a foreign jurisdiction is that data could be observed, modified, or denied through legal compulsion, which should not happen if an organization had sovereignty over its data. Exposure of a business function to a different legal jurisdiction can effectively remove sovereign legal barriers to compromise within the original jurisdiction. For example, the protection of citizen privacy often is not afforded to non-citizens, and service providers may be legally compelled to provide access to data or services that would have been legally protected in the original jurisdiction. In the case of business functions, consider as an example OT that controls critical infrastructures hosted in the cloud being modified or rendered unavailable by a hostile foreign jurisdiction.

The techniques employed may be very sophisticated and will generally be executed with full insider administrative privilege. Legal compulsion by sophisticated jurisdictions is exceedingly effective at bypassing other controls. Multiple jurisdictions may apply e.g., municipality, city, county, reservation, district, region, province, state, canton, territory, or nation. All levels must be identified to assess capabilities for compulsion.

Other jurisdictions may compel the compromise of business functions in confidentiality, integrity or availability. An injury assessment must document the negative consequences of legal compulsion, including any specific business needs for security (e.g., laws or regulations which require that data not be compromised).

An organization simply may not be at liberty to take a risk management approach (e.g., due to legislative mandate or indigenous data sovereignty) and must avoid risk scenarios outright.

GC discussion: The TBS Directive on Service and Digital, section 4.4.3.14 requires that sensitive information or data that is classified or categorized as Protected B or Protected C be located within Canadian jurisdiction as the principal delivery option. Canadian jurisdiction refers to the geographic boundaries of Canada or within the boundary of a diplomatic or consular mission of the GC abroad. The Cyber Centre recommends that all data and business functions of significant sensitivity be retained within Canadian jurisdictions.

Related controls and activities: AT-02, CA-02, RA-01, RA-02.

Enhancements:

(01) **Sovereignty and jurisdiction: Threat and risk assessment**

Require the organization to perform threat and risk assessments in relation to data sovereignty, considering its jurisdiction and by which surfaces legal compulsion may be effective.

Discussion: The organization establishes the injury value of business functions proposed to occupy other jurisdictions. Each of the 4 surfaces (logical, physical, personnel, and lifecycle) discussed in System lifecycle cyber security and privacy risk management activities (ITSP.10.037) may be vulnerable.

Related controls and activities: CA-02, RA-03.

(02) **Sovereignty and jurisdiction: Legal and contractual assessment**

Evaluate security assurance for business processes via legal or contractual mechanisms.

Discussion: Many jurisdictions will have different opportunities for protecting business functions from legal compulsion, at different assurance levels. International/multilateral agreements may help improve protection. Contract terms may be available from suppliers that can assist with reducing exposure or reporting on compulsion (note that some forms of compulsion may additionally compel non-disclosure in any form).

Where service delivery involves third-party vendors, ensure contractual documents reflect data sovereignty and jurisdiction obligations. If organizations choose to address sovereignty and jurisdiction obligations at the organization or project level, this obligation should be included in associated contractual obligations.

Organizations should seek specialist advice from the target jurisdiction if legal or contractual mechanisms are relied upon to prevent foreign legal compulsion, since any compulsive legislation is likely to take precedence over protective contracts or legislation. What constitutes due process in other jurisdictions may not be satisfactory from a Canadian perspective.

Related controls and activities: CA-02, SA-09.

(03) **Sovereignty and jurisdiction: Business process attribute marking**

Ensure business processes receive the intended handling with respect to legal jurisdiction.

Discussion: Metadata attributes can be defined and attached to business processes or data to assist management processes in correctly handling the intended legal jurisdiction. For example, documents may be marked with “Canadian Jurisdiction Only” or “Sovereign Indigenous” as an attribute. The automated handling of metadata attributes can be of great assistance for shared-infrastructure providers who may have multiple differing jurisdictional requirements.

Related controls and activities: AC-16, MP-03.

(04) **Sovereignty and jurisdiction: Protection of data at rest**

Prevent data from residing in any other legal jurisdiction.

Discussion: Permitting data at rest to remain in other jurisdictions provides the greatest opportunity for compulsion of the data at any time. Hosting data at rest within Canadian jurisdictions will increase the work factor and may eliminate some capabilities. Encryption of data at rest is of limited value but may be somewhat effective in preventing physical retrieval of the data.

There is no minimum time with respect to the data being “at rest”. If the data could, even momentarily, be written to non-volatile media, it must be considered at rest. This can particularly affect emergency/unexpected situations such as core dumps, memory caching/swapping and disaster recovery operations.

Consideration of data at rest must also include how the stored data will eventually be decommissioned and disposed of, to ensure that the data will remain outside foreign compulsion at the end of the system lifespan.

Related controls and activities: CP-06, CP-09, MP-06, MP-08, SA-03, SA-04, SA-22, SC-28.

(05) **Sovereignty and jurisdiction: Protection of data in transit**

Prevent data from transiting through any other legal jurisdiction.

Discussion: Permitting data in transit to pass through other jurisdictions provides numerous opportunities for compulsion of the data. Routing data strictly within Canadian jurisdictions eliminates many capabilities for compulsion. Encrypting data in transit may also have value.

Related controls and activities: CP-08, SC-08.

(06) **Sovereignty and jurisdiction: Protection of data in use**

Prevent data from being used in any other legal jurisdiction.

Discussion: Permitting data in use to exist in other jurisdictions provides opportunity for compulsion of the data. Processing data strictly within trusted jurisdictions eliminates many capabilities for compulsion.

There is currently no approved method of encryption to protect data in use. In principle, a form of encryption referred to as homomorphic encryption could permit certain kinds of processing while the data remains encrypted, but the Cyber Centre does not currently assess homomorphic encryption to be sufficient for cryptographic use as per the

Cyber Centre's Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B information (ITSP.40.111). Therefore, if homomorphic encryption is employed to protect data in use, it must currently be assessed as cleartext (i.e., not providing cryptographic protection as per SC-13).

There is no minimum time with respect to data being in use. Presence in a system for a single CPU cycle would be sufficient for compulsion.

Related controls and activities: CP-07, SC-13.

(07) **Sovereignty and jurisdiction: Protection against extraterritorial compulsion**

Prevent business functions from being compromised by individuals or corporations that are being compelled by a different legal jurisdiction.

Discussion: Adversaries may have means to compel individuals and/or corporations to compromise business functions even while those functions are kept entirely outside the adversary's jurisdiction. Consider the loyalty of individuals or corporations, direct ties between entities (e.g., affiliated corporations, family members, foreign assets) and indirect ties (e.g., partnerships and relationships).

Individuals residing in Canada who hold both Canadian and foreign citizenships may find themselves compelled by their other nationalities, despite also being bound to Canadian law, and could then be forced to choose between legal consequences in either jurisdiction.

Related controls and activities: MA-05.

(08) **Sovereignty and jurisdiction: Protection of business lifecycle**

Prevent business functions from being compromised by lifecycle attacks embedded via legal compulsion in or from a different legal jurisdiction.

Discussion: Employing products or services (e.g., software, firmware, hardware, design services, consultancy, etc.) that have previously been within the scope of compulsion may expose business functions to embedded compromises in those products or services. Most current systems contain elements from multiple legal jurisdictions, and a risk-based approach will be required to select solutions that address identified threats, according to the business needs for security.

Strong network isolation is recommended as a compensating control for any embedded compromises.

Related controls and activities: SA-03, SA-04, SC-07.

(09) **Sovereignty and jurisdiction: Public ownership**

Prevent business functions from being compromised by ownership transfer of lifecycle functions to a different legal jurisdiction.

Discussion: While system dependencies might be secured against foreign compulsion at the outset of implementation, if a transfer of ownership occurs during the system lifespan, the system could become subject to lifecycle attacks from foreign compulsion. To prevent this possibility, organizations select lifecycle support and supply arrangements that will be under Canadian public ownership for the entire lifespan of the system.

Related controls and activities: SA-03, SA-04, SA-22.

References:

- [TBS Directive on Service and Digital](#)
- [TBS Directive on Security Management, Appendix J: Standard on Security Categorization](#)
- System lifecycle cyber security and privacy risk management activities (ITSP.10.037)
- [Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B information \(ITSP.40.111\)](#)

Family: System and communications protection

The controls and activities in the System and communications protection (SC) family support the monitoring, control and protection of the systems themselves and of the communications between and within the systems.

SC-01 System and communications protection policy and procedures

Activity:

- A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]
 - 1. [Selection (1 or more): Organization-level; Mission/business process-level; System-level] system and communications protection policy that
 - a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
 - b. is consistent with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines
 - 2. procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls
- B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and communications protection policy and procedures
- C. Review and update the current system and communications protection
 - 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]
 - 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]

Discussion: System and communications protection policy and procedures address the controls in the SC family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of system and communications protection policy and procedures.

Security and privacy program policies and procedures at the organization level are preferable, in general, and may remove the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations.

Procedures can be established for security and privacy programs, for mission or business processes, and for systems, as needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.

Events that may precipitate an update to system and communications protection policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related controls and activities: PM-09, PS-08, SA-08, SI-02, SI-12.

Enhancements: None.

References: [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)

SC-02 Separation of system and user functionality

Control: Separate user functionality, including user interface services, from system management functionality.

Discussion: System management functionality includes functions that are necessary to administer databases, network components, workstations, or servers. These functions typically require privileged user access. User functions are separated from system management functions physically or logically.

Organizations may separate system management functions from user functions by using different computers, instances of operating systems, central processing units, or network addresses; by employing virtualization techniques; or through some combination of these or other methods.

The separation of system management functions from user functions includes web administrative interfaces that employ separate authentication methods for users of any other system resources. The separation of system and user functions may include isolating administrative interfaces on different domains and with additional access controls. The separation of system and user functionality can be achieved by applying the systems security engineering design principles in SA-08, including SA-08(01), SA-08(03), SA-08(04), SA-08(10), SA-08(12), SA-08(13), SA-08(14), and SA-08(18).

Related controls and activities: AC-06, SA-04, SA-08, SC-03, SC-07, SC-22, SC-32, SC-39, SI-400.

Enhancements:

(01) Separation of system and user functionality: Interfaces for non-privileged users

Prevent the presentation of system management functionality at interfaces to non-privileged users.

Discussion: Preventing the presentation of system management functionality at interfaces to non-privileged users ensures that system administration options, including administrator privileges, are not available to the general user population. Restricting user access also prohibits the use of the grey-out option commonly used to eliminate accessibility to such information. One potential solution is to withhold system administration options until users establish sessions with administrator privileges.

Related controls and activities: AC-03.

(02) Separation of system and user functionality: Disassociability

Store state information separately from applications and software.

Discussion: If a system is compromised, storing applications and software separately from state information about users' interactions with an application may better protect individuals' privacy.

Related controls and activities: None.

References: None.

SC-03 Security function isolation

Control: Isolate security functions from non-security functions.

Discussion: Security functions are isolated from non-security functions by means of an isolation boundary implemented within a system via partitions and domains. The isolation boundary controls access to, and protects the integrity of, the hardware, software, and firmware that perform system security functions.

Systems implement code separation in many ways, such as through the provision of security kernels via processor rings or processor modes. For non-kernel code, security function isolation is often achieved through file system protections that protect the code on disk and address space protections that protect executing code.

Systems can restrict access to security functions using access control mechanisms and by implementing least-privilege capabilities. Ideally, all code within the defined security function isolation boundary should only contain security-relevant code; however, it is sometimes necessary to include non-security functions as an exception.

The isolation of security functions from non-security functions can be achieved by applying the systems security engineering design principles in SA-08, including SA-08(01), SA-08(03), SA-08(04), SA-08(10), SA-08(12), SA-08(13), SA-08(14), and SA-08(18).

Related controls and activities: AC-03, AC-06, AC-25, CM-02, CM-04, SA-04, SA-05, SA-08, SA-15, SA-17, SC-02, SC-07, SC-32, SC-39, SI-16.

Enhancements:

(01) **Security function isolation: Hardware separation**

Employ hardware separation mechanisms to implement security function isolation.

Discussion: Hardware separation mechanisms include hardware ring architectures that are implemented within microprocessors and hardware-enforced address segmentation used to support logically distinct storage objects with separate attributes (i.e., readable, writeable).

Related controls and activities: None.

(02) **Security function isolation: Access and flow control functions**

Isolate security functions enforcing access and information flow control from non-security functions and from other security functions.

Discussion: Security function isolation occurs because of implementation. The functions can still be scanned and monitored. Security functions that are potentially isolated from access and flow-control enforcement functions include auditing, intrusion detection, and malicious code protection functions.

Related controls and activities: None.

(03) **Security function isolation: Minimize non-security functionality**

Minimize the number of non-security functions included within the isolation boundary containing security functions.

Discussion: Where it is not feasible to achieve strict isolation of non-security functions from security functions, it is necessary to take actions to minimize non-security-relevant functions within the security function boundary. Non-security functions contained within the isolation boundary are considered security-relevant because errors or malicious code in the software can directly impact the security functions of systems. The fundamental design objective is that the specific portions of systems that provide information security are of minimal size and complexity. Minimizing the number of non-security functions in the security-relevant system components allows designers and implementers to focus only on those functions which are necessary to provide the desired security capability (typically access enforcement). By minimizing the non-security functions within the isolation boundaries, the amount of code that is trusted to enforce security policies is significantly reduced, thus contributing to understandability.

Related controls and activities: None.

(04) **Security function isolation: Module coupling and cohesiveness**

Implement security functions as largely independent modules that maximize internal cohesiveness within modules and minimize coupling between modules.

Discussion: Reducing inter-module interactions helps constrain security functions and manage complexity. The concepts of coupling and cohesiveness are important with respect to modularity in software design. Coupling refers to the dependencies that one module has on other modules. Cohesiveness refers to the relationship between functions within a module. Best practices in software engineering and systems security engineering rely on layering, minimization, and modular decomposition to reduce and manage complexity. This produces software modules that are highly cohesive and loosely coupled.

Related controls and activities: None.

(05) Security function isolation: Layered structures

Implement security functions as a layered structure, minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.

Discussion: The implementation of layered structures with minimized interactions among security functions and non-looping layers (i.e., lower-layer functions do not depend on higher-layer functions) enables the isolation of security functions and the management of complexity.

Related controls and activities: None.

References:

- [Baseline security requirements for network security zones \(ITSP.80.022\)](#)
- [Network security zoning – Design considerations for placement of services within zones \(ITSG-38\)](#)

SC-04 Information in shared system resources

Control: Prevent unauthorized and unintended information transfer via shared system resources.

Discussion: Preventing unauthorized and unintended information transfer via shared system resources stops information produced by the actions of prior users or roles (or the actions of processes acting on behalf of prior users or roles) from being available to current users or roles (or current processes acting on behalf of current users or roles) that obtain access to shared system resources after those resources have been released back to the system.

Information in shared system resources also applies to encrypted representations of information. In other contexts, control of information in shared system resources is referred to as object reuse and residual information protection. Information in shared system resources does not address information remanence, which refers to the residual representation of data that has been nominally deleted; covert channels (including storage and timing channels), where shared system resources are manipulated to violate information flow restrictions; or components within systems for which there are only single users or roles.

Related controls and activities: AC-03, AC-04, SA-08.

Enhancements:**(01) Information in shared system resources: Security levels**

Withdrawn: Incorporated into SC-04.

(02) Information in shared system resources: Multilevel or periods processing

Prevent unauthorized information transfer via shared resources in accordance with [Assignment: organization-defined procedures] when system processing explicitly switches between different information classification levels or security categories.

Discussion: Changes in processing levels can occur during multilevel or periods processing with information at different classification levels or security categories. It can also occur during serial reuse of hardware components at different classification levels. Organization-defined procedures can include approved sanitization processes for electronically stored information.

Related controls and activities: None.

References: None.

SC-05 Denial-of-service protection**Control:**

- A. [Selection (1): Protect against; Limit] the effects of the following types of denial-of-service events: [Assignment: organization-defined types of denial-of-service events]
- B. Employ the following controls to achieve the denial-of-service objective: [Assignment: organization-defined controls by type of denial-of-service event]

Discussion: Denial-of-service events may occur due to various internal and external causes, such as an attack by an adversary or a lack of planning to support organizational needs with respect to capacity and bandwidth. Attacks can occur across a wide range of network protocols (e.g., IPv4, IPv6). Various technologies are available to limit or eliminate the origination and effects of denial-of-service events. For example, boundary protection devices can filter certain types of packets to protect system components on internal networks from being directly affected by or being the source of denial-of-service attacks. Employing increased network capacity and bandwidth combined with service redundancy also reduces the susceptibility to denial-of-service events.

Related controls and activities: CP-02, IR-04, SC-06, SC-07, SC-40.

Enhancements:

(01) Denial-of-service protection: Restrict ability to attack other systems

Restrict the ability of individuals to launch the following denial-of-service attacks against other systems: [Assignment: organization-defined denial-of-service attacks].

Discussion: Restricting the ability of individuals to launch denial-of-service attacks requires the mechanisms commonly used for such attacks to be unavailable. Individuals of concern include hostile insiders or external adversaries who have breached or compromised the system and are using it to launch a denial-of-service attack.

Organizations can restrict the ability of individuals to connect and transmit arbitrary information on the transport medium (i.e., wired networks, wireless networks, spoofed Internet protocol packets). Organizations can also limit the ability of individuals to use excessive system resources. Protection against individuals having the ability to launch denial-of-service attacks may be implemented on specific systems or boundary devices that prohibit egress to potential target systems.

Related controls and activities: None.

(02) Denial-of-service protection: Capacity, bandwidth, and redundancy

Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding denial-of-service attacks.

Discussion: Managing capacity ensures that sufficient capacity is available to counter flooding attacks. Managing capacity includes establishing selected usage priorities, quotas, partitioning, or load balancing.

Related controls and activities: None.

(03) Denial-of-service protection: Detection and monitoring

- a. Employ the following monitoring tools to detect indicators of denial-of-service attacks against, or launched from, the system: [Assignment: organization-defined monitoring tools]
- b. Monitor the following system resources to determine if sufficient resources exist to prevent effective denial-of-service attacks: [Assignment: organization-defined system resources]

Discussion: Organizations consider the utilization and capacity of system resources when managing risk associated with a denial of service due to malicious attacks. Denial-of-service attacks can originate from external or internal sources. System resources that are sensitive to denial of service include physical disk storage, memory, and CPU cycles.

Techniques used to prevent denial-of-service attacks related to storage utilization and capacity include instituting disk quotas, configuring systems to automatically alert administrators when specific storage capacity thresholds

are reached, using file compression technologies to maximize available storage space, and imposing separate partitions for system and user data.

Related controls and activities: CA-07, SI-04.

References:

- [Baseline security requirements for network security zones \(ITSP.80.022\)](#)
- [Protecting your organization against denial of service attacks \(ITSAP.80.100\)](#)

SC-06 Resource availability

Control: Protect the availability of resources by allocating [Assignment: organization-defined resources] by [Selection (1 or more): priority; quota; [Assignment: organization-defined controls]].

Discussion: Priority protection prevents lower-priority processes from delaying or interfering with the system that services higher-priority processes. Quotas prevent users or processes from obtaining more than predetermined amounts of resources.

Related controls and activities: SC-05.

Enhancements: None.

References:

- [Baseline security requirements for network security zones \(ITSP.80.022\)](#)
- [Protecting your organization against denial of service attacks \(ITSAP.80.100\)](#)

SC-07 Boundary protection

Control:

- A. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system
- B. Implement subnetworks for publicly accessible system components that are [Selection (1): physically; logically] separated from internal organizational networks
- C. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture

Discussion: Managed interfaces include gateways, routers, firewalls, guards, network-based malicious code analysis, virtualization systems, or encrypted tunnels implemented within a security architecture. Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones (DMZs).

Restricting or prohibiting interfaces within organizational systems includes restricting external web traffic to designated web servers within managed interfaces, prohibiting external traffic that appears to be spoofing internal addresses, and prohibiting internal traffic that appears to be spoofing external addresses. NIST SP 800-189 provides additional information on source address validation techniques to prevent ingress and egress of traffic with spoofed addresses.

Commercial telecommunications services are provided by network components and consolidated management systems shared by customers. These services may also include third-party-provided access lines and other service elements. Such services may represent sources of increased risk despite contract security provisions. Boundary protection may be implemented as a common control for all or part of an organizational network such that the boundary to be protected is greater than a system-specific boundary (i.e., an authorization boundary).

Related controls and activities: AC-04, AC-17, AC-18, AC-19, AC-20, AU-13, CA-03, CM-02, CM-04, CM-07, CM-10, CP-08, CP-10, IR-04, MA-04, PE-03, PL-08, PM-12, SA-08, SA-17, SA-400, SC-05, SC-26, SC-32, SC-35, SC-43, SI-400.

Enhancements:

(01) **Boundary protection: Physically separated subnetworks**

Withdrawn: Incorporated into SC-07.

(02) **Boundary protection: Public access**

Withdrawn: Incorporated into SC-07.

(03) **Boundary protection: Access points**

Limit the number of external network connections to the system.

Discussion: Limiting the number of external network connections facilitates monitoring of inbound and outbound communications traffic. Limiting the number of external network connections to the system is important during transition periods from older to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols). Such transitions may require implementing the older and newer technologies simultaneously during the transition period and thus increase the number of access points to the system.

GC discussion: The TBS Directive on Service and Digital, Appendix F: Standard on Enterprise Information Technology Usage Restrictions is an example of a federal guideline that requires limits on the number of external network connections. It requires that local Internet access services be obtained through SSC.

Related controls and activities: None.

(04) **Boundary protection: External telecommunications services**

- a. Implement a managed interface for each external telecommunication service
- b. Establish a traffic flow policy for each managed interface
- c. Protect the confidentiality and integrity of the information being transmitted across each interface
- d. Document each exception to the traffic flow policy with a supporting mission or business need and the duration of that need
- e. Review exceptions to the traffic flow policy [Assignment: organization-defined frequency] and remove exceptions that are no longer supported by an explicit mission or business need
- f. Prevent unauthorized exchange of control plane traffic with external networks
- g. Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks
- h. Filter unauthorized control plane traffic from external networks

Discussion: External telecommunications services can provide data and/or voice communications services. Examples of control plane traffic include Border Gateway Protocol (BGP) routing, DNS, and management protocols. See NIST SP 800-189 for additional information on the use of the resource public key infrastructure (RPKI) to protect BGP routes and detect unauthorized BGP announcements.

Related controls and activities: AC-03, SC-08, SC-20, SC-21, SC-22.

(05) **Boundary protection: Deny by default – allow by exception**

Deny network communications traffic by default and allow network communications traffic by exception [Selection (1 or more): at managed interfaces; for [Assignment: organization-defined systems]].

Discussion: Denying by default and allowing by exception applies to inbound and outbound network communications traffic. A deny-all, allow by exception network communications traffic policy ensures that only

those system connections that are essential and approved are allowed. Deny by default, allow by exception also applies to a system that is connected to an external system.

Related controls and activities: None.

(06) **Boundary protection: Response to recognized failures**

Withdrawn: Incorporated into SC-07(18).

(07) **Boundary protection: Split tunneling for remote devices**

Prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using [Assignment: organization-defined safeguards].

Discussion: Split tunneling is the process of allowing a remote user or device to establish a non-remote connection with a system and simultaneously communicate via some other connection to a resource in an external network. This method of network access enables a user to access remote devices and, simultaneously, access uncontrolled networks.

Split tunneling might be desirable to remote users for communicating with local system resources, such as printers or file servers. However, split tunneling can facilitate unauthorized external connections, making the system vulnerable to attack and to exfiltration of organizational information. Split tunneling can be prevented by disabling configuration settings that allow such capability in remote devices and by preventing those configuration settings from being configurable by users. Prevention can also be achieved by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling.

A VPN can be used to securely provision a split tunnel. A securely provisioned VPN includes locking connectivity to exclusive, managed, and named environments, or to a specific set of pre-approved addresses, without user control.

GC discussion: As per the TBS Directive on Service and Digital, Appendix G: Standard on Enterprise Information Technology Service Common Configurations – Endpoint Management Configuration Requirements, split tunneling is disabled except for domains that are included in the list approved by the GC Enterprise Architecture Review Board. All other network traffic to or from the Internet must flow through the GC-approved pathways to the Internet rather than via a direct connection to the Internet.

Related controls and activities: None.

(08) **Boundary protection: Route traffic to authenticated proxy servers**

Route [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers at managed interfaces.

Discussion: External networks are networks outside of organizational control. A proxy server is a server (i.e., system or application) that acts as an intermediary for clients requesting system resources from non-organizational or other organizational servers. System resources that may be requested include files, connections, web pages, or services.

Client requests established through a connection to a proxy server are assessed to manage complexity and provide additional protection by limiting direct connectivity. Web content filtering devices are one of the most common proxy servers that provide access to the Internet.

Proxy servers can support the logging of Transmission Control Protocol (TCP) sessions and the blocking of specific URLs, IP addresses, and domain names. Web proxies can be configured with organization-defined lists of authorized and unauthorized websites. Note that proxy servers may inhibit the use of VPNs and create the potential for adversary-in-the-middle attacks (depending on the implementation).

Related controls and activities: AC-03.

(09) **Boundary protection: Restrict threatening outgoing communications traffic**

- a. Detect and deny outgoing communications traffic posing a threat to external systems
- b. Audit the identity of internal users associated with denied communications

Discussion: Detecting outgoing communications traffic from internal actions that may pose threats to external systems is known as extrusion detection. Extrusion detection is carried out within the system at managed interfaces. Extrusion detection includes the analysis of incoming and outgoing communications traffic while searching for indications of internal threats to the security of external systems.

Internal threats to external systems include traffic indicative of denial-of-service attacks, traffic with spoofed source addresses, and traffic that contains malicious code. Organizations should have criteria to determine, update, and manage identified threats related to extrusion detection.

Related controls and activities: AU-02, AU-06, SC-05, SC-38, SC-44, SI-03, SI-04.

(10) **Boundary protection: Prevent exfiltration**

- a. Prevent the exfiltration of information
- b. Conduct exfiltration tests [Assignment: organization-defined frequency]

Discussion: Prevention of exfiltration applies to both the intentional and unintentional exfiltration of information. Techniques used to prevent the exfiltration of information from systems may be implemented at internal endpoints, external boundaries, and across managed interfaces and include adherence to protocol formats, monitoring for beaconing activity from systems, disconnecting external network interfaces except when explicitly needed, employing traffic profile analysis to detect deviations from the volume and types of traffic expected, call-backs to command and control centres, conducting penetration testing, monitoring for steganography, disassembling and reassembling packet headers, and using data loss and data leakage prevention tools.

Devices that enforce strict adherence to protocol formats include deep packet inspection firewalls and Extensible Markup Language (XML) gateways. The devices verify adherence to protocol formats and specifications at the application layer and identify vulnerabilities that cannot be detected by devices that operate at the network or transport layers.

The prevention of exfiltration is similar to data loss prevention or data leakage prevention and is closely associated with cross-domain solutions and system guards that enforce information flow requirements.

Related controls and activities: AC-02, CA-08, SI-03.

(11) **Boundary protection: Restrict incoming communications traffic**

Only allow incoming communications from [Assignment: organization-defined authorized sources] to be routed to [Assignment: organization-defined authorized destinations].

Discussion: General source-address validation techniques are applied to restrict the use of illegal and unallocated source addresses as well as source addresses that should only be used within the system. The restriction of incoming communications traffic provides determinations that source and destination address pairs represent authorized or allowed communications. Determinations can be based on several factors, including the presence of such address pairs in the lists of authorized or allowed communications, the absence of such address pairs in lists of unauthorized or disallowed pairs, or meeting more general rules for authorized or allowed source and destination pairs.

Strong authentication of network addresses is not possible without the use of explicit security protocols and, thus, addresses can often be spoofed. Furthermore, identity-based incoming traffic restriction methods can be employed, including router access control lists and firewall rules.

Related controls and activities: AC-03.

(12) **Boundary protection: Host-based protection**

Implement [Assignment: organization-defined host-based boundary protection mechanisms] at [Assignment: organization-defined system components].

Discussion: Host-based boundary protection mechanisms include host-based firewalls. System components that employ host-based boundary protection mechanisms include servers, workstations, notebook computers, and mobile devices.

Related controls and activities: None.

(13) **Boundary protection: Isolation of security tools, mechanisms, and support components**

Isolate [Assignment: organization-defined information security tools, mechanisms, and support components] from other internal system components by implementing physically separate subnetworks with managed interfaces to other components of the system.

Discussion: Physically separate subnetworks with managed interfaces are useful in isolating computer network defences from critical operational processing networks to prevent adversaries from discovering the analysis and forensics techniques employed by organizations.

Related controls and activities: SC-02, SC-03.

(14) **Boundary protection: Protect against unauthorized physical connections**

Protect against unauthorized physical connections at [Assignment: organization-defined managed interfaces].

Discussion: Systems that operate at different security categories or classification levels may share common physical and environmental controls, since the systems may share space within the same facilities. In practice, it is possible that these separate systems may share common equipment rooms, wiring closets, and cable distribution paths. Protection against unauthorized physical connections can be achieved by using clearly identified and physically separated cable trays, connection frames, and patch panels for each side of managed interfaces with physical access controls that enforce limited authorized access to these items.

Related controls and activities: PE-04, PE-19.

(15) **Boundary protection: Network privileged accesses**

Route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.

Discussion: Privileged access provides greater accessibility to system functions, including security functions. Adversaries attempt to gain privileged access to systems through remote access to cause adverse mission or business impacts, such as by exfiltrating information or bringing down a critical system capability. Routing networked, privileged access requests through a dedicated, managed interface further restricts privileged access for increased access control and auditing.

Related controls and activities: AC-02, AC-03, AU-02, SI-04.

(16) **Boundary protection: Prevent discovery of system components**

Prevent the discovery of specific system components that represent a managed interface.

Discussion: Preventing the discovery of system components representing a managed interface helps protect network addresses of those components from discovery through common tools and techniques used to identify devices on networks. Network addresses are not available for discovery and require prior knowledge for access. Preventing the discovery of components and devices can be accomplished by not publishing network addresses, using network address translation, or not entering the addresses in domain name systems. Another prevention technique is to periodically change network addresses.

Related controls and activities: None.

(17) **Boundary protection: Automated enforcement of protocol formats**

Enforce adherence to protocol formats.

Discussion: System components that enforce protocol formats include deep packet inspection firewalls and XML gateways. The components verify adherence to protocol formats and specifications at the application layer and identify vulnerabilities that cannot be detected by devices operating at the network or transport layers.

Related controls and activities: SC-04.

(18) **Boundary protection: Fail secure**

Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device.

Discussion: Fail secure is a condition achieved by employing mechanisms to ensure that, in the event of operational failures of boundary protection devices at managed interfaces, systems do not enter into unsecure states where intended security properties no longer hold. Managed interfaces include routers, firewalls, and application gateways that reside on protected subnetworks (commonly referred to as DMZs). Failures of boundary protection devices cannot lead to or cause information external to the devices to enter the devices, nor can failures permit unauthorized information releases.

Related controls and activities: CP-02, CP-12, SC-24.

(19) **Boundary protection: Block communication from non-organizationally-configured hosts**

Block inbound and outbound communications traffic between [Assignment: organization-defined communication clients] that are independently configured by end users and external service providers.

Discussion: Communication clients independently configured by end users and external service providers include instant messaging clients and video conferencing software and applications. Traffic blocking does not apply to communication clients that are configured by organizations to perform authorized functions.

Related controls and activities: None.

(20) **Boundary protection: Dynamic isolation and segregation**

Provide the capability to dynamically isolate [Assignment: organization-defined system components] from other system components.

Discussion: The capability to dynamically isolate certain internal system components is useful when it is necessary to partition or separate system components of questionable origin from components that possess greater trustworthiness. Component isolation reduces the attack surface of organizational systems. Isolating selected system components can also limit the damage from successful attacks when such attacks occur.

Related controls and activities: None.

(21) **Boundary protection: Isolation of system components**

Employ boundary protection mechanisms to isolate [Assignment: organization-defined system components] supporting [Assignment: organization-defined missions and/or business functions].

Discussion: Organizations can isolate system components that perform different mission or business functions. Such isolation limits unauthorized information flows among system components and provides the opportunity to deploy greater levels of protection for selected system components.

Isolating system components with boundary protection mechanisms provides the capability for increased protection of individual system components and to control information flows more effectively between those components. Isolating system components provides enhanced protection that limits the potential harm from hostile cyber attacks and errors.

The degree of isolation varies depending on the mechanisms chosen. Boundary protection mechanisms include routers, gateways, and firewalls that separate system components into separate networks or subnetworks; cross-

domain devices that separate subnetworks; virtualization techniques; the encryption of information flows among system components using distinct encryption keys and complete physical/electrical isolation of the relevant network/system from all other networks (aka air gapping).

Related controls and activities: CA-09.

(22) **Boundary protection: Separate subnets for connecting to different security domains**

Implement separate network addresses to connect to systems in different security domains.

Discussion: The decomposition of systems into subnetworks (i.e., subnets) helps to provide the appropriate level of protection for network connections to different security domains that contain information with different security categories or classification levels.

Related controls and activities: None.

(23) **Boundary protection: Disable sender feedback on protocol validation failure**

Disable feedback to senders on protocol format validation failure.

Discussion: Disabling feedback to senders when there is a failure in protocol validation format prevents adversaries from obtaining information that would otherwise be unavailable.

Related controls and activities: None.

(24) **Boundary protection: Personal information**

For systems that handle personal information:

- a. apply the following handling rules to data elements of personal information: [Assignment: organization-defined handling rules]
- b. monitor for permitted handling at the external interfaces to the system and at key internal boundaries within the system
- c. document each handling exception
- d. review and remove exceptions that are no longer supported

Discussion: Managing the handling of personal information is an important aspect of protecting an individual's privacy. Applying, monitoring for, and documenting exceptions to handling rules ensure that personal information is handled only in accordance with established privacy requirements.

GC discussion: Uses and disclosures of information without the consent of the individual are listed in subsection 8(2) of the *Privacy Act*.

Related controls and activities: PT-02, SI-15.

(25) **Boundary protection: Unclassified national security system connections**

Prohibit the direct connection of [Assignment: organization-defined unclassified national security system] to an external network without the use of [Assignment: organization-defined boundary protection device].

Discussion: None.

GC discussion: A direct connection is a dedicated physical or virtual connection between 2 or more systems. Organizations typically do not have complete control over external networks, including the Internet. Boundary protection devices (e.g., firewalls, gateways, and routers) mediate communications and information flows between unclassified national security systems and external networks.

Related controls and activities: None.

(26) **Boundary protection: Classified national security system connections**

Prohibit the direct connection of a classified national security system to an external network without the use of [Assignment: organization-defined boundary protection device].

Discussion: None.

GC discussion: A direct connection is a dedicated physical or virtual connection between 2 or more systems. Organizations typically do not have complete control over external networks, including the Internet. Boundary protection devices (e.g., firewalls, gateways, and routers) mediate communications and information flows between classified national security systems and external networks. In addition, approved boundary protection devices (typically managed interface or cross-domain systems) provide information flow enforcement from systems to external networks.

Related controls and activities: None.

(27) **Boundary protection: Unclassified non-national security system connections**

Prohibit the direct connection of [Assignment: organization-defined unclassified non-national security system] to an external network without the use of [Assignment: organization-defined boundary protection device].

Discussion: None.

GC discussion: A direct connection is a dedicated physical or virtual connection between 2 or more systems. Organizations typically do not have complete control over external networks, including the Internet. Boundary protection devices (e.g., firewalls, gateways, and routers) mediate communications and information flows between unclassified non-national security systems and external networks.

Related controls and activities: None.

(28) **Boundary protection: Connections to public networks**

Prohibit the direct connection of [Assignment: organization-defined system] to a public network.

Discussion: A direct connection is a dedicated physical or virtual connection between 2 or more systems. A public network is a network accessible to the public, including the Internet and organizational extranets with public access.

Related controls and activities: None.

(29) **Boundary protection: Separate subnets to isolate functions**

Implement [Selection (1): physically; logically] separate subnetworks to isolate the following critical system components and functions: [Assignment: organization-defined critical system components and functions].

Discussion: Separating critical system components and functions from other non-critical system components and functions through separate subnetworks may be necessary to reduce susceptibility to a catastrophic or debilitating breach or compromise that results in system failure. For example, physically separating the command-and-control function from the in-flight entertainment function through separate subnetworks in a commercial aircraft provides an increased level of assurance in both the trustworthiness and robustness of critical system functions.

Related controls and activities: None.

References:

- [Baseline security requirements for network security zones \(ITSP.80.022\)](#)
- [Network security zoning – Design considerations for placement of services within zones \(ITSG-38\)](#)
- [Guidance on securely configuring network protocols \(ITSP.40.062\)](#)
- [NIST SP 800-189 Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation](#)
- [TBS Directive on Service and Digital, Appendix F: Standard on Enterprise Information Technology Usage Restrictions](#)
- [TBS Directive on Service and Digital, Appendix G: Standard on Enterprise Information Technology Service Common Configurations](#)

SC-08 Transmission confidentiality and integrity

Control: Protect the [Selection (1 or more): confidentiality; integrity] of transmitted information.

Discussion: Protecting the confidentiality and integrity of transmitted information applies to internal and external networks, as well as to any system components that can transmit information, including servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, facsimile machines, and radios. Unprotected communication paths are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of information can be accomplished by physical or logical means. Physical protection can be achieved by using protected distribution systems. A protected distribution system is a wireline or fibre-optics telecommunications system that includes terminals and adequate electromagnetic, acoustical, electrical, and physical controls to permit its use for the unencrypted transmission of classified information. Logical protection can be achieved by employing encryption techniques.

Organizations that rely on commercial providers who offer transmission services as commodity services rather than as fully dedicated services may find it difficult to obtain the necessary assurances regarding the implementation of needed controls for transmission confidentiality and integrity. In such situations, organizations determine what types of confidentiality or integrity services are available in standard, commercial telecommunications service packages. If it is not feasible to obtain the necessary controls and assurances of control effectiveness through appropriate contracting vehicles, organizations can implement appropriate compensating controls.

Related controls and activities: AC-17, AC-18, AU-10, IA-03, IA-08, IA-09, MA-04, PE-04, SA-04, SA-08, SA-400, SC-07, SC-16, SC-20, SC-23, SC-28, SI-400.

Enhancements:

(01) Transmission confidentiality and integrity: Cryptographic protection

Implement cryptographic mechanisms to [Selection (1 or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.

Discussion: Encryption protects information from unauthorized disclosure and modification during transmission. Cryptographic mechanisms that protect the confidentiality and integrity of information during transmission include TLS and Internet Protocol Security (IPsec). Cryptographic mechanisms used to protect information integrity include cryptographic hash functions that have applications in digital signatures, checksums, and message authentication codes.

Related controls and activities: SC-12, SC-13.

(02) Transmission confidentiality and integrity: Pre- and post-transmission handling

Maintain the [Selection (1 or more): confidentiality; integrity] of information during preparation for transmission and during reception.

Discussion: Information can be unintentionally or maliciously disclosed or modified during preparation for transmission or during reception, including during aggregation, at protocol transformation points, and during packing and unpacking. Such unauthorized disclosures or modifications compromise the confidentiality or integrity of the information.

Related controls and activities: None.

(03) Transmission confidentiality and integrity: Cryptographic protection for message externals

Implement cryptographic mechanisms to protect message externals unless otherwise protected by [Assignment: organization-defined alternative physical controls].

Discussion: Cryptographic protection for message externals addresses protection from the unauthorized disclosure of information. Message externals include message headers and routing information. Cryptographic protection prevents the exploitation of message externals and applies to internal and external networks or links that may be

visible to individuals who are not authorized users. Header and routing information is sometimes transmitted in clear text (i.e., unencrypted) because the information is not identified by organizations as having significant value or because encrypting the information can result in lower network performance or higher costs. Alternative physical controls include protected distribution systems.

Related controls and activities: SC-12, SC-13.

(04) **Transmission confidentiality and integrity: Conceal or randomize communications**

Implement cryptographic mechanisms to conceal or randomize communication patterns unless otherwise protected by [Assignment: organization-defined alternative physical controls].

Discussion: Concealing or randomizing communication patterns addresses protection from unauthorized disclosure of information. Communication patterns include frequency, periods, predictability, and amount. Changes to communications patterns can reveal information with intelligence value, especially when combined with other available information related to the mission and business functions of the organization. Concealing or randomizing communications prevents the derivation of intelligence based on communications patterns and applies to both internal and external networks or links that may be visible to individuals who are not authorized users. Encrypting the links and transmitting in continuous, fixed, or random patterns prevents the derivation of intelligence from the system communications patterns. Alternative physical controls include protected distribution systems.

Related controls and activities: SC-12, SC-13.

(05) **Transmission confidentiality and integrity: Protected distribution system**

Implement [Assignment: organization-defined protected distribution system] to [Selection (1 or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.

Discussion: The purpose of a protected distribution system is to deter, detect, and/or make difficult physical access to the communication lines that carry national security information.

Related controls and activities: None.

References:

- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [Guidance on securely configuring network protocols \(ITSP.40.062\)](#)
- [Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B information \(ITSP.40.111\)](#)

SC-09 Transmission confidentiality

Withdrawn: Incorporated into SC-08.

SC-10 Network disconnect

Control: Terminate the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.

Discussion: Network disconnect applies to internal and external networks. Terminating network connections associated with specific communications sessions includes de-allocating TCP/IP address or port pairs at the operating system level and de-allocating the networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. Periods of inactivity may be established by organizations and include time periods by type of network access or for specific network accesses.

Related controls and activities: AC-17, SC-23.

Enhancements: None.

References: None.

SC-11 Trusted path

Control:

- A. Provide a [Selection (1): physically; logically] isolated trusted communications path for communications between the user and the trusted components of the system
- B. Permit users to invoke the trusted communications path for communications between the user and the following security functions of the system, including at a minimum, authentication and re-authentication: [Assignment: organization-defined security functions]

Discussion: Trusted paths are mechanisms by which users can communicate (using input devices such as keypads or smart card readers with a built-in PIN pad) directly with the security functions of systems with the requisite assurance to support security policies. Trusted path mechanisms can only be activated by users or the security functions of organizational systems. User responses that occur via trusted paths are protected from modification by and disclosure to untrusted applications.

Organizations employ trusted paths for trustworthy, high-assurance connections between security functions of systems and users, including during system logons. The original implementations of trusted paths employed an out-of-band signal to initiate the path, such as using the <BREAK> key, which does not transmit characters that can be spoofed. In later implementations, a key combination that could not be hijacked was used (e.g., the <CTRL> + <ALT> + <DEL> keys). Such key combinations, however, are platform-specific and may not provide a trusted path implementation in every case. The enforcement of trusted communications paths is provided by a specific implementation that meets the reference monitor concept.

Related controls and activities: AC-16, AC-25, SC-12, SC-23.

Enhancements:

(01) Trusted path: Irrefutable communications path

- a. Provide a trusted communications path that is irrefutably distinguishable from other communications paths
- b. Initiate the trusted communications path for communications between the [Assignment: organization-defined security functions] of the system and the user

Discussion: An irrefutable communications path permits the system to initiate a trusted path, which necessitates that the user can unmistakably recognize the source of the communication as a trusted system component. For example, the trusted path may appear in an area of the display that other applications cannot access or be based on the presence of an identifier that cannot be spoofed.

Related controls and activities: None.

References: None.

SC-12 Cryptographic key establishment and management

Control: Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

Discussion: Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define key management requirements in accordance with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines and specify appropriate options, parameters, and levels. Organizations manage trust stores to ensure that only approved trust anchors are part of such trust stores. This includes certificates with visibility external to organizational systems and certificates related to the internal operations of systems. The joint NIST-CSE CMVP provides additional information on validated cryptographic modules and algorithms that can be used in cryptographic key management and establishment.

GC discussion: The use of NIST-CSE CMVP-validated commercial cryptographic modules is recommended for all national security systems.

Related controls and activities: AC-17, AU-09, AU-10, CM-03, IA-03, IA-07, IA-13, SA-04, SA-08, SA-09, SC-08, SC-11, SC-12, SC-13, SC-17, SC-20, SC-37, SC-40, SI-03, SI-07.

Enhancements:

(01) Cryptographic key establishment and management: Availability

Maintain availability of information in the event of the loss of cryptographic keys by users.

Discussion: Escrowing of encryption keys is a common practice for ensuring availability in the event of key loss. A forgotten passphrase is an example of losing a cryptographic key.

Related controls and activities: None.

(02) Cryptographic key establishment and management: Symmetric keys

Produce, control, and distribute symmetric cryptographic keys using [Selection (1): CMVP-validated; Cyber Centre-approved; prepositioned keying material] key management technology and processes.

Discussion: The Cyber Centre publication ITSP.40.111 provides recommendations for cryptographic key establishment schemes and key derivation functions that can be used to produce symmetric keys shared between 2 parties. These schemes are to be used in a network security protocol, such as those listed in the Cyber Centre's ITSP.40.062 with further configuration guidance therein.

GC discussion: For national security systems, the use of Cyber Centre-approved key management technology and processes is mandatory.

Related controls and activities: None.

(03) Cryptographic key establishment and management: Asymmetric keys

Produce, control, and distribute asymmetric cryptographic keys using [Selection (1): Cyber Centre-approved key management technology and processes; prepositioned keying material; Cyber Centre-approved or Cyber Centre-issued Medium Assurance PKI certificates; Cyber Centre-approved or Cyber Centre-issued Medium Hardware Assurance PKI certificates and hardware security tokens that protect the user's private key; certificates issued in accordance with organization-defined requirements].

Discussion: ITSP.40.111 provides recommendations for approved specifications of asymmetric cryptography and recommends that implementations, including key generation, execute within CMVP-validated cryptographic modules. ITSP.40.062 provides guidance on asymmetric key management within a PKI.

GC discussion: For national security systems, the use of Cyber Centre-approved key management technology and processes is mandatory.

Related controls and activities: None.

(04) Cryptographic key establishment and management: PKI certificates

Withdrawn: Incorporated into SC-12(03).

(05) Cryptographic key establishment and management: PKI certificates/hardware tokens

Withdrawn: Incorporated into SC-12(03).

(06) **Cryptographic key establishment and management: Physical control of keys**

Maintain physical control of cryptographic keys when stored information is encrypted by external service providers.

Discussion: For organizations that use external service providers (e.g., cloud service or data centre providers), physical control of cryptographic keys provides additional assurance that information stored by such external providers is not subject to unauthorized disclosure or modification.

Related controls and activities: None.

References:

- [Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B information \(ITSP.40.111\)](#)
- [Guidance on cloud service cryptography \(ITSP.50.106\)](#)
- [Guidance on securely configuring network protocols \(ITSP.40.062\)](#)
- [Cryptographic Module Validation Program \(CMVP\)](#)
- Directive for the control of COMSEC material in the Government of Canada (ITSD-03A) (upon request to the Cyber Centre)
- IT Security Directive for Cryptographic Key Ordering (ITSD-09) (upon request to the Cyber Centre)

SC-13 Cryptographic protection

Control:

- Determine the [Assignment: organization-defined cryptographic uses]
- Implement the following types of cryptography required for each specified cryptographic use: [Assignment: organization-defined types of cryptography for each specified cryptographic use]

Discussion: Cryptography can be employed to support a variety of security solutions, including the protection of classified information and protected information, the provision and implementation of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances but lack the necessary formal access approvals.

Cryptography can also be used to support random number and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and Cyber Centre-approved cryptography. For example, organizations that need to protect classified information may specify the use of Cyber Centre-approved cryptography. Organizations that need to provision and implement digital signatures may specify the use of FIPS-validated cryptography. Cryptography is implemented in accordance with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines.

Related controls and activities: AC-02, AC-03, AC-07, AC-17, AC-18, AC-19, AU-09, AU-10, CM-11, CP-09, IA-03, IA-05, IA-07, IA-13, MA-04, MP-02, MP-04, MP-05, SA-04, SA-08, SA-09, SA-400, SC-08, SC-12, SC-20, SC-23, SC-28, SC-40, SI-03, SI-07.

Enhancements:

(01) **Cryptographic protection: FIPS-validated cryptography**

Withdrawn: Incorporated into SC-13.

(02) **Cryptographic protection: National Security Agency (NSA)-approved cryptography**

Withdrawn: Incorporated into SC-13.

(03) **Cryptographic protection: Individuals without formal access approvals**

Withdrawn: Incorporated into SC-13.

(04) Cryptographic protection: Digital signatures

Withdrawn: Incorporated into SC-13.

(400) Cryptographic protection: PROTECTED A data in transit

Withdrawn: Incorporated into SC-13.

(401) Cryptographic protection: PROTECTED B data in transit

Withdrawn: Incorporated into SC-13.

(402) Cryptographic protection: PROTECTED C data in transit

Withdrawn: Incorporated into SC-13.

(403) Cryptographic protection: PROTECTED data at rest

Withdrawn: Incorporated into SC-13.

(404) Cryptographic protection: National security systems

Withdrawn: Incorporated into SC-13.

References:

- [Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B information \(ITSP.40.111\)](#)
- Directives for the application of communications security in the Government of Canada (ITSD-01A) (upon request to the Cyber Centre)
- [NIST FIPS 140-3 Security Requirements for Cryptographic Modules](#)

SC-14 Public access protections

Withdrawn: Incorporated into AC-02, AC-03, AC-05, AC-06, SI-03, SI-04, SI-05, SI-07, and SI-10.

SC-15 Collaborative computing devices and applications

Control:

- Prohibit remote activation of collaborative computing devices and applications with the following exceptions:
[Assignment: organization-defined exceptions where remote activation is to be allowed]
- Provide an explicit indication of use to users physically present at the devices

Discussion: Collaborative computing devices and applications include remote meeting devices and applications, networked whiteboards, cameras, and microphones. The explicit indication of use includes signals to users when collaborative computing devices and applications are activated.

Related controls and activities: AC-21, SC-42.

Enhancements:**(01) Collaborative computing devices and applications: Physical or logical disconnect**

Provide [Selection (1 or more): physical; logical] disconnect of collaborative computing devices in a manner that supports ease of use.

Discussion: Failing to disconnect from collaborative computing devices can result in subsequent compromises of organizational information. Providing easy methods to disconnect from such devices after a collaborative computing session ensures that participants carry out the disconnect activity without having to go through complex and tedious procedures. Disconnect from collaborative computing devices can be manual or automatic.

Related controls and activities: None.

(02) **Collaborative computing devices and applications: Blocking inbound and outbound communications traffic**

Withdrawn: Incorporated into SC-07.

(03) **Collaborative computing devices and applications: Disabling and removal in secure work areas**

Disable or remove collaborative computing devices and applications from [Assignment: organization-defined systems or system components] in [Assignment: organization-defined secure work areas].

Discussion: Failing to disable or remove collaborative computing devices and applications from systems or system components can result in compromises of information, including eavesdropping on conversations. A sensitive compartmented information facility (SCIF) is an example of a secure work area.

Related controls and activities: None.

(04) **Collaborative computing devices and applications: Explicitly indicate current participants**

Provide an explicit indication of current participants in [Assignment: organization-defined online meetings and teleconferences].

Discussion: Explicitly indicating current participants prevents unauthorized individuals from participating in collaborative computing sessions without the explicit knowledge of other participants.

Related controls and activities: None.

References: None.

SC-16 Transmission of security and privacy attributes

Control: Associate [Assignment: organization-defined security and privacy attributes] with information exchanged between systems and between system components.

Discussion: Security and privacy attributes can be explicitly or implicitly associated with the information contained in organizational systems or system components. Attributes are abstractions that represent the basic properties or characteristics of an entity with respect to protecting information or the management of personal information. Attributes are typically associated with internal data structures, including records, buffers, and files within the system.

Security and privacy attributes are used to implement access control and information flow control policies; reflect special dissemination, management, or distribution instructions, including permissible uses or disclosures of personal information; or support other aspects of the information security and privacy policies. Privacy attributes may be used independently or in conjunction with security attributes.

Related controls and activities: AC-03, AC-04, AC-16.

Enhancements:

(01) **Transmission of security and privacy attributes: Integrity verification**

Verify the integrity of transmitted security and privacy attributes.

Discussion: Part of verifying the integrity of transmitted information is ensuring that security and privacy attributes that are associated with such information have not been modified in an unauthorized manner. Unauthorized modification of security or privacy attributes can result in a loss of integrity for transmitted information.

Related controls and activities: AU-10, SC-08.

(02) **Transmission of security and privacy attributes: Anti-spoofing mechanisms**

Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes indicating the successful application of the security process.

Discussion: Some attack vectors operate by altering the security attributes of an information system to intentionally and maliciously implement an insufficient level of security within the system. The alteration of attributes leads organizations to believe that a greater number of security functions are in place and operational than were actually implemented.

Related controls and activities: SI-03, SI-04, SI-07.

(03) **Transmission of security and privacy attributes: Cryptographic binding**

Implement [Assignment: organization-defined mechanisms or techniques] to bind security and privacy attributes to transmitted information.

Discussion: Cryptographic mechanisms and techniques can provide strong security and privacy attribute binding to transmitted information to help ensure the integrity of such information.

Related controls and activities: AC-16, SC-12, SC-13.

References: None.

SC-17 Public key infrastructure certificates

Control:

- A. Issue public key certificates under an [Assignment: organization-defined certificate policy] or obtain public key certificates from an approved service provider
- B. Include only approved trust anchors in trust stores or certificate stores managed by the organization

Discussion: PKI certificates are certificates with visibility external to organizational systems and certificates related to the internal operations of systems, such as application-specific time services. In cryptographic systems with a hierarchical structure, a trust anchor is an authoritative source (i.e., a certificate authority) for which trust is assumed and not derived. A root certificate for a PKI system is an example of a trust anchor. A trust store or certificate store maintains a list of trusted root certificates.

Related controls and activities: AU-10, IA-05, SC-12.

Enhancements: None.

References:

- [TBS Public Key Infrastructure Configuration Requirements](#)
- [TBS X.509 Public Key Infrastructure Certificate Policy for Person Entity](#) (restricted to GC)

SC-18 Mobile code

Control:

- A. Define acceptable and unacceptable mobile code and mobile code technologies
- B. Authorize, monitor, and control the use of mobile code within the system

Discussion: Mobile code includes any program, application, or content that can be transmitted across a network (e.g., embedded in an email, document, or website) and executed on a remote system. Decisions regarding the use of mobile code within organizational systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include Java applets, JavaScript, HTML5, WebGL, and VBScript. Usage restrictions and implementation guidelines apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices, including notebook computers and smart phones. Mobile code policy and procedures address specific actions taken to prevent the development, acquisition, and introduction of

unacceptable mobile code within organizational systems, including requiring mobile code to be digitally signed by a trusted source.

Related controls and activities: AU-02, AU-12, CM-02, CM-06, SI-03.

Enhancements:

(01) Mobile code: Identify unacceptable code and take corrective actions

Identify [Assignment: organization-defined unacceptable mobile code] and take [Assignment: organization-defined corrective actions].

Discussion: Corrective actions when unacceptable mobile code is detected include blocking, quarantining, or alerting administrators. Blocking includes preventing the transmission of word-processing files with embedded macros when such macros have been determined to be unacceptable mobile code.

Related controls and activities: None.

(02) Mobile code: Acquisition, development, and use

Verify that the acquisition, development, and use of mobile code to be deployed in the system meets [Assignment: organization-defined mobile code requirements].

Discussion: None.

Related controls and activities: None.

(03) Mobile code: Prevent downloading and execution

Prevent the download and execution of [Assignment: organization-defined unacceptable mobile code].

Discussion: None.

Related controls and activities: None.

(04) Mobile code: Prevent automatic execution

Prevent the automatic execution of mobile code in [Assignment: organization-defined software applications] and enforce [Assignment: organization-defined actions] prior to executing the code.

Discussion: Actions enforced before executing mobile code include prompting users prior to opening email attachments or clicking on web links. Preventing the automatic execution of mobile code includes disabling auto-execute features on system components that employ any removable media technology.

Related controls and activities: None.

(05) Mobile code: Allow execution only in confined environments

Allow execution of permitted mobile code only in confined virtual machine environments.

Discussion: Permitting the execution of mobile code only in confined virtual machine environments helps prevent the introduction of malicious code into other systems and system components.

Related controls and activities: SC-44, SI-07.

References: None.

SC-19 Voice over Internet Protocol

Control:

- A. The organization establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously

- B.** The organization authorizes, monitors, and controls the use of VoIP within the information system

Discussion: None.

GC discussion: This control is used in any physical security zone that contains a National Security System (NSS) at the Secret or Top Secret level.

Enhancements:

(400) Voice over Internet Protocol: Protocol conversion

Unclassified VoIP is not permitted within classified facilities unless the VoIP is converted to plain old telephone systems (POTS) before exiting the facility boundary.

Discussion: None.

GC discussion: VoIP in classified facilities should comply with the US Committee on National Security Systems Instruction (CNSSI) No. 5000. Some authorizers may require CNSSI-5000 compliance.

Related controls and activities: None.

(401) Voice over Internet Protocol: No public network access

Unclassified VoIP over a Local Area Network (LAN) with access to a public data network is not permitted within classified facilities.

Discussion: None.

GC discussion: VoIP in classified facilities should comply with CNSSI-5000. Some authorizers may require CNSSI-5000 compliance.

Related controls and activities: None.

References: [CNSSI 5000 Voice Over Internet Protocol \(VoIP\) Telephony](#)

SC-20 Secure name/address resolution service (authoritative source)

Control:

- A.** Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries.
- B.** Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

Discussion: Providing authoritative source information enables external clients, including remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. Systems that provide name and address resolution services include DNS servers.

Additional artifacts include DNS Security Extensions (DNSSEC), digital signatures, and cryptographic keys. Authoritative data includes DNS resource records. The means for indicating the security status of child zones include the use of delegation signer resource records in the DNS. Systems that use technologies other than the DNS to map between host and service names and network addresses provide other means to assure the authenticity and integrity of response data.

Related controls and activities: AU-10, SC-08, SC-12, SC-13, SC-21, SC-22.

Enhancements:

(01) Secure name/address resolution service (authoritative source): Child subspaces

Withdrawn: Incorporated into SC-20.

(02) Secure name/address resolution service (authoritative source): Data origin and integrity

Provide data origin and integrity protection artifacts for internal name/address resolution queries.

Discussion: None.

Related controls and activities: None.

References:

- [Protective domain name system \(ITSAP.40.019\)](#)
- [NIST FIPS 140-3 Security Requirements for Cryptographic Modules](#)
- [NIST FIPS 186-5 Digital Signature Standard \(DSS\)](#)

SC-21 Secure name/address resolution service (recursive or caching resolver)

Control: Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

Discussion: Each client of name resolution services either performs this validation on its own or has authenticated channels to trusted validation providers. Systems that provide name and address resolution services for local clients include recursive resolving or caching DNS servers. DNS client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations. Systems that use technologies other than the DNS to map between host and service names and network addresses provide some other means to enable clients to verify the authenticity and integrity of response data.

Related controls and activities: SC-20, SC-22.

Enhancements:**(01) Secure name/address resolution service (recursive or caching resolver): Data origin/integrity**

Withdrawn: Incorporated into SC-21.

References: [Protective domain name system \(ITSAP.40.019\)](#)

SC-22 Architecture and provisioning for name/address resolution service

Control: Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.

Discussion: Systems that provide name and address resolution services include DNS servers. To eliminate single points of failure in systems and enhance redundancy, organizations employ at least 2 authoritative DNS servers – one configured as the primary server and the other configured as the secondary server. Additionally, organizations typically deploy the servers in 2 geographically separated network subnetworks (i.e., not located in the same physical facility).

For role separation, DNS servers with internal roles only process name and address resolution requests from within organizations (i.e., from internal clients). DNS servers with external roles only process name and address resolution information requests from clients external to organizations (i.e., on external networks, including the Internet). Organizations specify clients that can access authoritative DNS servers in certain roles (e.g., by address ranges and explicit lists).

Related controls and activities: SC-02, SC-20, SC-21, SC-24.

Enhancements: None.

References: [Protective domain name system \(ITSAP.40.019\)](#)

SC-23 Session authenticity

Control: Protect the authenticity of communications sessions.

Discussion: Protecting session authenticity addresses communications protection at the session level, not at the packet level. Such protection establishes grounds for confidence at both ends of communications sessions in the ongoing identities of other parties and the validity of transmitted information. Authenticity protection includes protecting against adversary-in-the-middle attacks, session hijacking, and the insertion of false information into sessions.

Related controls and activities: AU-10, SC-08, SC-10, SC-11.

Enhancements:

(01) Session authenticity: Invalidate session identifiers at logout

Invalidate session identifiers upon user logout or other session termination.

Discussion: Invalidating session identifiers at logout curtails the ability of adversaries to capture and continue to employ previously valid session IDs.

Related controls and activities: None.

(02) Session authenticity: User-initiated logouts/message displays

Withdrawn: Incorporated into AC-12(01).

(03) Session authenticity: Unique system-generated session identifiers

Generate a unique session identifier for each session with [Assignment: organization-defined randomness requirements] and recognize only session identifiers that are system-generated.

Discussion: Generating unique session identifiers curtails the ability of adversaries to reuse previously valid session IDs. Employing the concept of randomness in the generation of unique session identifiers protects against brute-force attacks to determine future session identifiers.

Related controls and activities: AC-10, SC-12, SC-13.

(04) Session authenticity: Unique session identifiers with randomization

Withdrawn: Incorporated into SC-23(03).

(05) Session authenticity: Allowed certificate authorities

Only allow the use of [Assignment: organization-defined certificate authorities] for verification of the establishment of protected sessions.

Discussion: Reliance on certificate authorities for the establishment of secure sessions includes the use of TLS certificates. These certificates, after verification by their respective certificate authorities, facilitate the establishment of protected sessions between web clients and web servers.

Related controls and activities: SC-12, SC-13.

References:

- [Guidance on securely configuring network protocols \(ITSP.40.062\)](#)
- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)

SC-24 Fail in known state

Control: Fail to a [Assignment: organization-defined known system state] for the following failures on the indicated components while preserving [Assignment: organization-defined system state information] in failure: [Assignment: list of organization-defined types of system failures on organization-defined system components].

Discussion: Failure in a known state addresses security concerns in accordance with the mission and business needs of organizations. Failure in a known state prevents the loss of confidentiality, integrity, or availability of information in the event of failures of organizational systems or system components. Failure in a known safe state helps to prevent systems from failing to a state that may cause injury to individuals or destruction to property. Preserving system state information facilitates system restart and return to the operational mode with less disruption of mission and business processes.

Related controls and activities: CP-02, CP-04, CP-10, CP-12, SA-08, SC-07, SC-22, SI-13.

Enhancements: None.

References: None.

SC-25 Thin nodes

Control: Employ minimal functionality and information storage on the following system components: [Assignment: organization-defined system components].

Discussion: The deployment of system components with minimal functionality reduces the need to secure every endpoint and may reduce the exposure of information, systems, and services to attacks. Reduced or minimal functionality includes diskless nodes and thin client technologies.

Related controls and activities: SC-30, SC-44, SI-400.

Enhancements: None.

References: None.

SC-26 Decoys

Control: Include components within organizational systems specifically designed to be the target of malicious attacks for detecting, deflecting, and analyzing such attacks.

Discussion: Decoys (i.e., honeypots, honeynets, or deception nets) are established to attract adversaries and deflect attacks away from the operational systems that support organizational mission and business functions. Use of decoys requires some supporting isolation measures to ensure that any deflected malicious code does not infect organizational systems. Depending on the specific usage of the decoy, consultation with the departmental legal team before deployment may be needed.

Related controls and activities: RA-05, SC-07, SC-30, SC-35, SC-44, SI-03, SI-04.

Enhancements:

(01) **Decoys: Detection of malicious code**

Withdrawn: Incorporated into SC-35.

References: None.

SC-27 Platform-independent applications

Control: Include within organizational systems the following platform-independent applications: [Assignment: organization-defined platform-independent applications].

Discussion: Platforms are combinations of hardware, firmware, and software components used to execute software applications. Platforms include operating systems, the underlying computer architectures, or both. Platform-independent applications are applications with the capability to execute on multiple platforms. Such applications promote portability and reconstitution on different platforms. Application portability and the ability to reconstitute on different platforms increase the availability of mission-essential functions within organizations in situations where systems with specific operating systems are under attack.

Related controls and activities: SC-29.

Enhancements: None.

References: None.

SC-28 Protection of information at rest

Control: Protect the [Selection (1 or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].

Discussion: Information at rest refers to the state of information when it is not in process or in transit and is located on system components. Such components include internal or external hard disk drives, storage area network devices, or databases. However, the focus of protecting information at rest is not on the type of storage device or frequency of access but rather on the state of the information.

Information at rest addresses the confidentiality and integrity of information and covers user information and system information. System-related information that requires protection includes configurations or rule sets for firewalls, intrusion detection and prevention systems, filtering routers, and authentication information. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning.

Integrity protection can be achieved, for example, by implementing write-once-read-many (WORM) technologies. When adequate protection of information at rest cannot otherwise be achieved, organizations may employ other controls, including frequent scanning to identify malicious code at rest and secure offline storage in lieu of online storage.

Related controls and activities: AC-03, AC-04, AC-06, AC-19, CA-07, CM-03, CM-05, CM-06, CP-09, MP-04, MP-05, PE-03, SA-400, SC-08, SC-12, SC-13, SC-34, SI-03, SI-07, SI-16.

Enhancements:

(01) Protection of information at rest: Cryptographic protection

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].

Discussion: The selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of organizational information. The strength of mechanism is commensurate with the security category or classification of the information. Organizations have the flexibility to encrypt information on system components or media or encrypt data structures, including files, records, or fields.

Related controls and activities: AC-19, SC-12, SC-13.

(02) Protection of information at rest: Offline storage

Remove the following information from online storage and store offline in a secure location: [Assignment: organization-defined information].

Discussion: Removing organizational information from online storage to offline storage eliminates the possibility of individuals gaining unauthorized access to the information through a network. Therefore, organizations may choose to move information to offline storage in lieu of protecting such information in online storage.

Related controls and activities: None.

(03) **Protection of information at rest: Cryptographic keys**

Provide protected storage for cryptographic keys [Selection (1): [Assignment: organization-defined safeguards]; hardware-protected key store].

Discussion: A Trusted Platform Module (TPM) is an example of a hardware-protected data store that can be used to protect cryptographic keys.

Related controls and activities: SC-12, SC-13.

References: [Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information \(ITSP.40.111\)](#)

SC-29 Heterogeneity

Control: Employ a diverse set of information technologies for the following system components in the implementation of the system: [Assignment: organization-defined system components].

Discussion: Increasing the diversity of information technologies within organizational systems reduces the impact of potential exploitations or compromises of specific technologies. Such diversity protects against common mode failures, including those failures induced by supply chain attacks. Diversity in information technologies also reduces the likelihood that the means adversaries use to compromise one system component will be effective against other system components, thus further increasing the adversary work factor to successfully complete planned attacks. An increase in diversity may add complexity and management overhead that could ultimately lead to mistakes and unauthorized configurations.

Related controls and activities: AU-09, PL-08, SC-27, SC-30, SI-400, SR-03.

Enhancements:

(01) **Heterogeneity:Virtualization techniques**

Employ virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed [Assignment: organization-defined frequency].

Discussion: While frequent changes to operating systems and applications can pose significant configuration management challenges, the changes can result in an increased work factor for adversaries to conduct successful attacks. Changing virtual operating systems or applications, as opposed to changing actual operating systems or applications, provides virtual changes that impede attacker success while reducing configuration management efforts. Virtualization techniques can assist in isolating untrustworthy software or software of dubious provenance into confined execution environments.

Related controls and activities: None.

References: None.

SC-30 Concealment and misdirection

Control: Employ the following concealment and misdirection techniques for [Assignment: organization-defined systems] at [Assignment: organization-defined time periods] to confuse and mislead adversaries: [Assignment: organization-defined concealment and misdirection techniques].

Discussion: Concealment and misdirection techniques can significantly reduce the targeting capabilities of adversaries (i.e., the window of opportunity and available attack surface) to initiate and complete attacks. For example, virtualization techniques provide organizations with the ability to disguise systems, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms.

The increased use of concealment and misdirection techniques and methods—including randomness, uncertainty, and virtualization—may sufficiently confuse and mislead adversaries and subsequently increase the risk of discovery and/or exposing tradecraft. Concealment and misdirection techniques may provide additional time to perform core mission and business functions. The implementation of concealment and misdirection techniques may add to the complexity and management overhead required for the system.

Related controls and activities: AC-06, SC-25, SC-26, SC-29, SC-44, SI-14.

Enhancements:

(01) **Concealment and misdirection: Virtualization techniques**

Withdrawn: Incorporated into SC-29(01).

(02) **Concealment and misdirection: Randomness**

Employ [Assignment: organization-defined techniques] to introduce randomness into organizational operations and assets.

Discussion: Randomness introduces increased levels of uncertainty for adversaries regarding the actions that organizations take to defend their systems against attacks. Such actions may impede the ability of adversaries to correctly target information resources of organizations that support critical missions or business functions.

Uncertainty may also cause adversaries to hesitate before initiating or continuing attacks. Misdirection techniques that involve randomness include performing certain routine actions at different times of day, employing different information technologies, using different suppliers, and rotating roles and responsibilities of organizational personnel.

Related controls and activities: None.

(03) **Concealment and misdirection: Change processing and storage locations**

Change the location of [Assignment: organization-defined processing and/or storage] [Selection (1): [Assignment: organization-defined time frequency]; at random time intervals]].

Discussion: Adversaries target critical mission and business functions and the systems that support those mission and business functions while also trying to minimize the exposure of their existence and tradecraft. The static, homogeneous, and deterministic nature of organizational systems targeted by adversaries make such systems more susceptible to attacks with less adversary cost and effort to be successful.

Changing processing and storage locations (also referred to as moving target defence) addresses the advanced persistent threat using techniques such as virtualization, distributed processing, and replication. This enables organizations to relocate the system components (i.e., processing, storage) that support critical mission and business functions.

Changing the locations of processing activities and/or storage sites introduces a degree of uncertainty into the targeting activities of adversaries. The targeting uncertainty increases the work factor of adversaries and makes compromises or breaches of the organizational systems more difficult and time-consuming. It also increases the chances that adversaries may inadvertently disclose certain aspects of their tradecraft while attempting to locate critical organizational resources.

Related controls and activities: None.

(04) **Concealment and misdirection: Misleading information**

Employ realistic, but misleading information in [Assignment: organization-defined system components] about its security state or posture.

Discussion: Employing misleading information is intended to confuse potential adversaries regarding the nature and extent of controls deployed by organizations. Thus, adversaries may employ incorrect and ineffective attack techniques. One technique for misleading adversaries is for organizations to place misleading information regarding the specific controls deployed in external systems that are known to be targeted by adversaries. Another technique is the use of deception nets that mimic actual aspects of organizational systems but use, for example, out-of-date software configurations.

Related controls and activities: None.

(05) **Concealment and misdirection: Concealment of system components**

Employ the following techniques to hide or conceal [Assignment: organization-defined system components]: [Assignment: organization-defined techniques].

Discussion: By hiding, disguising, or concealing critical system components, organizations may be able to decrease the probability that adversaries target and successfully compromise those assets. Potential means to hide, disguise, or conceal system components include the configuration of routers or the use of encryption or virtualization techniques.

Related controls and activities: None.

References: None.

SC-31 Covert channel analysis

Control:

- A. Perform a covert channel analysis to identify those aspects of communications within the system that are potential avenues for covert [Selection (1 or more): storage; timing] channels
- B. Estimate the maximum bandwidth of those channels

Discussion: Developers are in the best position to identify potential areas within systems that might lead to covert channels. Covert channel analysis is a meaningful activity when there is the potential for unauthorized information flows across security domains, such as in the case of systems that contain export-controlled information and have connections to external networks (i.e., networks that are not controlled by organizations). Covert channel analysis is also useful for multilevel secure systems, multiple security level systems, and cross-domain systems.

Related controls and activities: AC-03, AC-04, SA-08, SI-11.

Enhancements:

(01) **Covert channel analysis: Test covert channels for exploitability**

Test a subset of the identified covert channels to determine the channels that are exploitable.

Discussion: None.

Related controls and activities: None.

(02) **Covert channel analysis: Maximum bandwidth**

Reduce the maximum bandwidth for identified covert [Selection (1 or more): storage; timing] channels to [Assignment: organization-defined values].

Discussion: The complete elimination of covert channels, especially covert timing channels, is usually not possible without significant performance impacts.

Related controls and activities: None.

(03) **Covert channel analysis: Measure bandwidth in operational environments**

Measure the bandwidth of [Assignment: organization-defined subset of identified covert channels] in the operational environment of the system.

Discussion: Measuring covert channel bandwidth in specified operational environments helps organizations determine how much information can be covertly leaked before such leakage adversely affects mission or business functions. Covert channel bandwidth may be significantly different when measured in settings that are independent of the specific environments of operation, including laboratories or system development environments.

Related controls and activities: None.

References: None.

SC-32 System partitioning

Control: Partition the system into [Assignment: organization-defined system components] residing in separate [Selection (1): physical; logical] domains or environments based on [Assignment: organization-defined circumstances for physical or logical separation of components].

Discussion: System partitioning is part of a defence-in-depth protection strategy. Organizations determine the degree of physical separation of system components. Physical separation options include physically distinct components in separate racks in the same room, critical components in separate rooms, and geographical separation of critical components. Security categorization can guide the selection of candidates for domain partitioning. Managed interfaces restrict or prohibit network access and information flow among partitioned system components.

Related controls and activities: AC-04, AC-06, SA-08, SC-02, SC-03, SC-07, SC-36, SI-400.

Enhancements:

(01) **System partitioning: Separate physical domains for privileged functions**

Partition privileged functions into separate physical domains.

Discussion: Privileged functions that operate in a single physical domain may represent a single point of failure if that domain becomes compromised or experiences a denial of service.

Related controls and activities: None.

References:

- [TBS Directive on Security Management, Appendix J: Standard on Security Categorization](#)
- [Guidance on defence in depth for cloud-based services \(ITSP.50.104\)](#)

SC-33 Transmission preparation integrity

Withdrawn: Incorporated into SC-08.

SC-34 Non-modifiable executable programs

Control: For [Assignment: organization-defined system components], load and execute:

- the operating environment from hardware-enforced, read-only media
- the following applications from hardware-enforced, read-only media: [Assignment: organization-defined applications]

Discussion: The operating environment for a system contains the code that hosts applications, including operating systems, executives, or virtual machine monitors (i.e., hypervisors). It can also include certain applications that run directly on hardware platforms. Hardware-enforced, read-only media and write-once recordable media include Compact Disc-Recordable (CD-R) Digital Versatile Disc-Recordable (DVD-R), and Blu-Ray (BD-R) disk drives as well as one-time, programmable read-only memory (PROM). The use of non-modifiable storage ensures the integrity of software from the point of creation of the read-only image. The use of reprogrammable read-only memory can be accepted as read-only media provided that integrity can be adequately protected from the point of initial writing to the insertion of the memory into the system, and there are reliable hardware protections against reprogramming the memory while installed in organizational systems.

Related controls and activities: AC-03, SI-07, SI-14.

Enhancements:

(01) **Non-modifiable executable programs: No writeable storage**

Employ [Assignment: organization-defined system components] with no writeable storage that is persistent across component restart or power on/off.

Discussion: Disallowing writeable storage eliminates the possibility of malicious code insertion via persistent, writeable storage within the designated system components. The restriction applies to fixed and removable storage, with the latter being addressed either directly or as specific restrictions imposed through access controls for mobile devices.

Related controls and activities: AC-19, MP-07.

(02) **Non-modifiable executable programs: Integrity protection and read-only media**

Protect the integrity of information prior to storage on read-only media and control the media after such information has been recorded onto the media.

Discussion: Security safeguards prevent the substitution of media into information systems or the reprogramming of programmable read-only media prior to installation into the systems. Security safeguards include, for example, a combination of prevention, detection, and response.

Related controls and activities: AC-05, CM-03, CM-05, CM-09, MP-02, MP-04, MP-05, SA-12, SC-28, SI-03.

(03) **Non-modifiable executable programs: Hardware-based protection**

Withdrawn: Moved to SC-51.

References: None.

SC-35 External malicious code identification

Control: Include system components that proactively seek to identify network-based malicious code or malicious websites.

Discussion: External malicious code identification differs from decoys in SC-26 in that the components actively probe networks, including the Internet, in search of malicious code contained on external websites. Like decoys, the use of external malicious code identification techniques requires some supporting isolation measures to ensure that any malicious code discovered during the search and subsequently executed does not infect organizational systems. Virtualization is a common technique for achieving such isolation.

Related controls and activities: SC-07, SC-26, SC-44, SI-03, SI-04.

Enhancements: None.

References: None.

SC-36 Distributed processing and storage

Control: Distribute the following processing and storage components across multiple [Selection (1): physical locations; logical domains]: [Assignment: organization-defined processing and storage components].

Discussion: Distributing processing and storage across multiple physical locations or logical domains provides a degree of redundancy or overlap for organizations. The redundancy and overlap increase the work factor of adversaries to adversely impact organizational operations, assets, and individuals. The use of distributed processing and storage does not assume a single primary processing or storage location. Therefore, it allows for parallel processing and storage.

Related controls and activities: CP-06, CP-07, PL-08, SC-32.

Enhancements:

(01) Distributed processing and storage: Polling techniques

- a. Employ polling techniques to identify potential faults, errors, or compromises to the following processing and storage components: [Assignment: organization-defined distributed processing and storage components]
- b. Take the following actions in response to identified faults, errors, or compromises: [Assignment: organization-defined actions]

Discussion: Distributed processing and/or storage may be used to reduce opportunities for adversaries to compromise the confidentiality, integrity, or availability of organizational information and systems. However, the distribution of processing and storage components does not prevent adversaries from compromising one or more of the components. Polling compares the processing results and/or storage content from the distributed components and subsequently votes on the outcomes. Polling identifies potential faults, compromises, or errors in the distributed processing and storage components.

Related controls and activities: SI-04.

(02) Distributed processing and storage: Synchronization

Synchronize the following duplicate systems or system components: [Assignment: organization-defined duplicate systems or system components].

Discussion: SC-36 and CP-09(06) require the duplication of systems or system components in distributed locations. The synchronization of duplicated and redundant services and data helps to ensure that information contained in the distributed locations can be used in the mission or business functions of organizations, as needed.

Related controls and activities: CP-09.

References: None.

SC-37 Out-of-band channels

Control: Employ the following out-of-band channels for the physical delivery or electronic transmission of [Assignment: organization-defined information, system components, or devices] to [Assignment: organization-defined individuals or systems]: [Assignment: organization-defined out-of-band channels].

Discussion: Out-of-band channels include local, non-network access to systems; network paths physically separate from network paths used for operational traffic; or non-electronic paths, such as Canada Post. The use of out-of-band channels contrasts with the use of in-band channels (i.e., the same channels) that carry routine operational traffic. Out-of-band channels do not have the same vulnerability or exposure as in-band channels. Therefore, the confidentiality, integrity, or availability compromises of in-band channels will not compromise or adversely affect the out-of-band channels.

Organizations may employ out-of-band channels in the delivery or transmission of organizational items, including authenticators and credentials; cryptographic key management information; system and data backups; configuration

management changes for hardware, firmware, or software; security updates; maintenance information; and malicious code protection updates. For example, cryptographic keys for encrypted files are delivered using a different channel than the file.

Related controls and activities: AC-02, CM-03, CM-05, CM-07, IA-02, IA-04, IA-05, MA-04, SC-12, SI-03, SI-04, SI-07.

Enhancements:

(01) Out-of-band channels: Ensure delivery and transmission

Employ [Assignment: organization-defined controls] to ensure that only [Assignment: organization-defined individuals or systems] receive the following information, system components, or devices: [Assignment: organization-defined information, system components, or devices].

Discussion: Techniques employed by organizations to ensure that only designated systems or individuals receive certain information, system components, or devices include sending authenticators via an approved courier service but requiring recipients to show some form of government-issued photographic identification as a condition of receipt.

Related controls and activities: None.

References: [RCMP GCPSPG-007 Transport, Transmittal and Storage of Protected and Classified Material](#) (restricted to GC)

SC-38 Operations security

Control: Employ the following operations security controls to protect key organizational information throughout the system development lifecycle: [Assignment: organization-defined operations security controls].

Discussion: Operations security (OPSEC) is a systematic process by which potential adversaries can be denied information about the capabilities and intentions of organizations by identifying, controlling, and protecting generally unclassified information that specifically relates to the planning and execution of sensitive organizational activities.

The OPSEC process involves 5 steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and the application of appropriate countermeasures. OPSEC controls are applied to organizational systems and the environments in which those systems operate. OPSEC controls protect the confidentiality of information, including limiting the sharing of information with suppliers, potential suppliers, and other non-organizational elements and individuals.

Information critical to organizational mission and business functions includes user identities, element uses, suppliers, supply chain processes, functional requirements, security requirements, system design specifications, testing and evaluation protocols, and security control implementation details.

Related controls and activities: CA-02, CA-07, PL-01, PM-09, PM-12, RA-02, RA-03, RA-05, SC-07, SR-03, SR-07.

Enhancements: None.

References: None.

SC-39 Process isolation

Control: Maintain a separate execution domain for each executing system process.

Discussion: Systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process.

Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces. Process isolation technologies, including sandboxing or virtualization, logically separate software and

firmware from other software, firmware, and data. Process isolation helps limit the access of potentially untrusted software to other system resources. The capability to maintain separate execution domains is available in commercial operating systems that employ multi-state processor technologies.

Related controls and activities: AC-03, AC-04, AC-06, AC-25, SA-08, SC-02, SC-03, SI-16.

Enhancements:

(01) **Process isolation: Hardware separation**

Implement hardware separation mechanisms to facilitate process isolation.

Discussion: Hardware-based separation of system processes is generally less susceptible to compromise than software-based separation, thus providing greater assurance that the separation will be enforced. Hardware separation mechanisms include hardware memory management.

Related controls and activities: None.

(02) **Process isolation: Separate execution domain per thread**

Maintain a separate execution domain for each thread in [Assignment: organization-defined multi-threaded processing].

Discussion: None.

Related controls and activities: None.

References: None.

SC-40 Wireless link protection

Control: Protect external and internal [Assignment: organization-defined wireless links] from the following signal parameter attacks: [Assignment: organization-defined types of signal parameter attacks or references to sources for such attacks].

Discussion: Wireless link protection applies to internal and external wireless communication links that may be visible to individuals who are not authorized system users. Adversaries can exploit the signal parameters of wireless links if such links are not adequately protected. There are many ways to exploit the signal parameters of wireless links to gain intelligence, deny service, or spoof system users. Protection of wireless links reduces the impact of attacks that are unique to wireless systems. If organizations rely on commercial service providers for transmission services as commodity items rather than as fully dedicated services, it may not be possible to implement wireless link protections to the extent necessary to meet organizational security requirements.

Related controls and activities: AC-18, SC-05.

Enhancements:

(01) **Wireless link protection: Electromagnetic interference**

Implement cryptographic mechanisms that achieve [Assignment: organization-defined level of protection] against the effects of intentional electromagnetic interference.

Discussion: The implementation of cryptographic mechanisms that mitigate electromagnetic interference protects systems against intentional jamming that might deny or impair communications by ensuring that wireless spread-spectrum waveforms used to provide anti-jam protection are not predictable by unauthorized individuals. The implementation of cryptographic mechanisms may also coincidentally mitigate the effects of unintentional jamming due to interference from legitimate transmitters that share the same spectrum. Mission requirements, projected threats, concepts of operations, and laws, Orders in Council, directives, regulations, policies, and standards determine the levels of wireless link availability, cryptography needed, and performance.

Related controls and activities: PE-21, SC-12, SC-13.

(02) Wireless link protection: Reduce detection potential

Implement cryptographic mechanisms to reduce the detection potential of wireless links to [Assignment: organization-defined level of reduction].

Discussion: The implementation of cryptographic mechanisms to reduce detection potential is used for covert communications and to protect wireless transmitters from geolocation. It also ensures that the spread-spectrum waveforms used to achieve a low probability of detection are not predictable by unauthorized individuals. Mission requirements, projected threats, concepts of operations, and applicable laws, Orders in Council, directives, regulations, policies, and standards determine the levels to which wireless links are undetectable.

Related controls and activities: SC-12, SC-13.

(03) Wireless link protection: Imitative or manipulative communications deception

Implement cryptographic mechanisms to identify and reject wireless transmissions that are deliberate attempts to achieve imitative or manipulative communications deception based on signal parameters.

Discussion: The implementation of cryptographic mechanisms to identify and reject imitative or manipulative communications ensures that the signal parameters of wireless transmissions are not predictable by unauthorized individuals. Such unpredictability reduces the probability of imitative or manipulative communications deception based on signal parameters alone.

Related controls and activities: SC-12, SC-13, SI-04.

(04) Wireless link protection: Signal parameter identification

Implement cryptographic mechanisms to prevent the identification of [Assignment: organization-defined wireless transmitters] by using the transmitter signal parameters.

Discussion: The implementation of cryptographic mechanisms to prevent the identification of wireless transmitters protects against the unique identification of wireless transmitters for the purposes of intelligence exploitation by ensuring that anti-fingerprinting alterations to signal parameters are not predictable by unauthorized individuals. It also provides anonymity when required. Radio fingerprinting techniques identify the unique signal parameters of transmitters to fingerprint such transmitters for purposes of tracking and mission or user identification.

Related controls and activities: SC-12, SC-13.

References: None.

SC-41 Port and input/output device access

Control: [Selection (1): Physically; Logically] disable or remove [Assignment: organization-defined connection ports or input/output devices] on the following systems or system components: [Assignment: organization-defined systems or system components].

Discussion: Disabling or removing connection ports and input/output (I/O) devices helps prevent the exfiltration of information from systems and the introduction of malicious code from those ports or devices. Physically disabling or removing ports and/or devices is the stronger action compared to logical approaches. Examples of connection ports include Universal Serial Bus (USB), Thunderbolt, and Firewire (IEEE 1394). Examples of I/O devices include optical disc drives, USB thumb drives, monitors, keyboards, and mice.

Related controls and activities: AC-20, MP-07.

Enhancements: None.

References: None.

SC-42 Sensor capability and data

Control:

- A. Prohibit [Selection (1 or more): the use of devices possessing [Assignment: organization-defined environmental sensing capabilities] in [Assignment: organization-defined facilities, areas, or systems]; the remote activation of environmental sensing capabilities on organizational systems or system components with the following exceptions: [Assignment: organization-defined exceptions where remote activation of sensors is allowed]]
- B. Provide an explicit indication of sensor use to [Assignment: organization-defined group of users]

Discussion: Sensor capability and data applies to types of systems or system components characterized as mobile devices, such as cellular telephones, smart phones, and tablets. Mobile devices often include sensors that can collect and record data regarding the environment where the system is in use. Sensors that are embedded within mobile devices include microphones, cameras, Global Positioning System (GPS) mechanisms, and accelerometers.

While the sensors on mobile devices provide an important function, such devices can potentially provide a means for adversaries to learn valuable information about individuals and organizations if activated covertly. For example, remotely activating the GPS function on a mobile device could provide an adversary with the ability to track the movements of an individual. Organizations may prohibit individuals from bringing cellular telephones or digital cameras into certain designated facilities or controlled areas within facilities where classified information is stored or sensitive conversations take place.

Related controls and activities: SC-15.

Enhancements:

(01) Sensor capability and data: Reporting to authorized individuals or roles

Verify that the system is configured so that data or information collected by the [Assignment: organization-defined sensors] is only reported to authorized individuals or roles.

Discussion: In situations where sensors are activated by authorized individuals, it is still possible that the data or information collected by the sensors will be sent to unauthorized entities. Organizations should make sure appropriate controls are in place to ensure sensor data is protected.

Related controls and activities: None.

(02) Sensor capability and data: Authorized use

Employ the following measures so that data or information collected by [Assignment: organization-defined sensors] is used only for authorized purposes: [Assignment: organization-defined measures].

Discussion: Organizations should ensure lawful authority for any use or disclosure of sensor data. Information collected by sensors for a specific authorized purpose could be misused for some unauthorized purpose. For example, GPS sensors that are used to support traffic navigation could be misused to track the movements of individuals. Measures to mitigate such activities include additional training to help ensure that authorized individuals do not abuse their authority and, in the case where sensor data is maintained by external parties, contractual restrictions on the use of such data exist.

Related controls and activities: PT-02.

(03) Sensor capability and data: Prohibit use of devices

Withdrawn: Incorporated into SC-42.

(04) Sensor capability and data: Notice of collection

Employ the following measures to facilitate an individual's awareness that personal information is being collected by [Assignment: organization-defined sensors]: [Assignment: organization-defined measures].

Discussion: Obtain legal advice before collecting sensor data on employer-issued devices. When individuals are aware that organizational sensors are collecting data, they can engage more effectively in managing their privacy. Measures can include conventional written notices or sensor configurations that make individuals directly or indirectly aware through other devices that the sensor is collecting information. The clarity of the notice is an important consideration.

GC discussion: There are both privacy and Charter implications with the use of sensor technology, and further assessment by organizational counsel may be required. It is important to notify users of employer-issued technologies about the potential infringement of their personal information and that users acknowledge these risks before using the device.

Related controls and activities: PT-01, PT-04, PT-05.

(05) **Sensor capability and data: Collection minimization**

Employ [Assignment: organization-defined sensors] that are configured to minimize the collection of information about individuals that is not needed.

Discussion: Although policies that constrain authorized use can be applied to information once it is collected, minimizing the collection of information that is not needed mitigates privacy and Charter risk and mitigates the risk of policy control failures.

GC discussion: In addition, for the use of the technologies that can be considered privacy-invasive, the OPC asks that Charter implications be considered, in line with the R. vs. Oakes Supreme Court decision. Bearing in mind the concept of unreasonable search and seizure, organizations should assess collection of information that may infringe on Charter rights against the principles set out in the aforementioned Oakes decision.

Related controls and activities: SA-08, SI-12.

(400) **Sensor capability and data: Disablement in security/high-security zones**

Ensure that the organization disables all sensors on all devices when they are not approved to process information at the highest classification level in the security or high-security zone they are in.

Discussion: None.

GC discussion: Organizations must ensure that device sensors are disabled. For example, cameras and microphones on Protected B-approved workstations must be physically disabled if they are not used. If they are used, they must be situated in such ways as to prevent compromise of Protected C or classified information discussed or presented in the security or high-security zones.

Related controls and activities: None.

References:

- [Security considerations for exposure of classified IT systems to mobile devices and wireless signals \(ITSB-104\)](#)
- [Using your mobile device securely \(ITSAP.00.001\)](#)
- [Security considerations for mobile device deployments \(ITSAP.70.002\)](#)

SC-43 Usage restrictions

Control:

- A. Establish usage restrictions and implementation guidelines for the following system components: [Assignment: organization-defined system components]
- B. Authorize, monitor, and control the use of such components within the system

Discussion: Usage restrictions apply to all system components including, but not limited to, mobile code, mobile devices, wireless access, and wired and wireless peripheral components (e.g., copiers, printers, scanners, optical devices, and other similar technologies). The usage restrictions and implementation guidelines are based on the potential for system components to cause damage to the system and help to ensure that only authorized system use occurs.

Related controls and activities: AC-18, AC-19, CM-06, SC-07, SC-18.

Enhancements: None.

References: [TBS Directive on Service and Digital, Appendix F: Standard on Enterprise Information Technology Usage Restrictions](#)

SC-44 Detonation chambers

Control: Employ a detonation chamber capability within [Assignment: organization-defined system, system component, or location].

Discussion: Detonation chambers, also known as dynamic execution environments, allow organizations to open email attachments, execute untrusted or suspicious applications, and execute URL requests in the safety of an isolated environment or a virtualized sandbox. Protected and isolated execution environments provide a means of determining whether the associated attachments or applications contain malicious code.

While detonation chambers are related to the concept of deception nets, they are not intended to maintain a long-term environment in which adversaries can operate and their actions can be observed. Rather, detonation chambers are intended to quickly identify malicious code and either reduce the likelihood that the code is propagated to user environments of operation or prevent such propagation completely.

Related controls and activities: SC-07, SC-18, SC-25, SC-26, SC-30, SC-35, SC-39, SI-03, SI-07.

Enhancements: None.

References: [Top 10 IT security actions to protect Internet-connected networks and information \(ITSM.10.089\)](#)

SC-45 System time synchronization

Control: Synchronize system clocks within and between systems and system components.

Discussion: Time synchronization of system clocks is essential for the correct execution of many system services, including identification and authentication processes that involve certificates and time-of-day restrictions as part of access control. Denial of service or failure to deny expired credentials may result if clocks are not properly synchronized within and between systems and system components.

Time is commonly expressed in UTC or local time with an offset from UTC. The granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks, such as clocks synchronizing within hundreds of milliseconds or tens of milliseconds. Organizations may define different time granularities for system components. Time service can be critical to other security capabilities—such as access control and identification and authentication—depending on the nature of the mechanisms used to support the capabilities.

Related controls and activities: AC-03, AU-08, IA-02, IA-08.

Enhancements:

(01) System time synchronization: Synchronization with authoritative time source

- a. Compare the internal system clocks [Assignment: organization-defined frequency] with [Assignment: organization-defined authoritative time source]

- b. Synchronize the internal system clocks to the authoritative time source when the time difference is greater than [Assignment: organization-defined time period]

Discussion: Synchronization of internal system clocks with an authoritative source provides uniformity of time stamps for systems with multiple system clocks and systems connected over a network.

Related controls and activities: None.

(02) **System time synchronization: Secondary authoritative time source**

- a. Identify a secondary authoritative time source that is in a different geographic region than the primary authoritative time source
- b. Synchronize the internal system clocks to the secondary authoritative time source if the primary authoritative time source is unavailable

Discussion: It may be necessary to employ geolocation information to determine that the secondary authoritative time source is in a different geographic region.

Related controls and activities: None.

References: [IETF RFC 5905 Network Time Protocol Version 4: Protocol and Algorithms Specification](#)

SC-46 Cross-domain policy enforcement

Control: Implement a policy enforcement mechanism [Selection (1): physically; logically] between the physical and/or network interfaces for the connecting security domains.

Discussion: For logical policy enforcement mechanisms, organizations should avoid creating a logical path between interfaces to prevent the ability to bypass the policy enforcement mechanism. For physical policy enforcement mechanisms, the robustness of physical isolation afforded by the physical implementation of policy enforcement may be needed to preclude the presence of logical covert channels penetrating the security domain.

GC discussion: Only Cyber Centre-approved CDS should be used for Protected C and classified information. Contact cyber@cyber.gc.ca for more information.

Related controls and activities: AC-04, SC-07.

Enhancements:

(400) **Cross-domain policy enforcement: Manual data transfer**

Limit the use of manual data transfer.

Discussion: A transfer CDS allows information to be transferred securely and automatically between different security domains. The use of manual data transfer should be limited to specific requirements. Circumventing the proper transfer procedures and choosing to transfer information using removable media is generally inappropriate user behaviour.

If transferring information using removable media becomes an operational necessity, procedures must conform with the Cyber Centre's ITSB-112. An authorized user may do a manual data transfer using removable media such as a USB memory stick. If available, an offline CDS can be used to scan and sanitize the media. Such a transfer can be used when there is a requirement to transfer a software patch or anti-virus update from a removable media device to an isolated security domain, for example.

Related controls and activities: None.

References:

- [Cross domain security primer \(ITSB-120\)](#)

- [Security considerations for the use of removable media devices for Protected C and Classified Information \(ITSB-112\)](#)

SC-47 Alternate communications paths

Control: Establish [Assignment: organization-defined alternate communications paths] for system operations organizational command and control.

Discussion: An incident, whether adversarial or non-adversarial, can disrupt established communications paths used for system operations and organizational command and control. Alternate communications paths reduce the risk of all communications paths being affected by the same incident. Moreover, the inability of organizational officials to obtain timely information about disruptions or to provide timely direction to operational elements after a communications path incident can impact the ability of the organization to respond to such incidents in a timely manner. Establishing alternate communications paths for command-and-control purposes, including designating alternative decision-makers if primary decision-makers are unavailable and establishing the extent and limitations of their actions, can greatly facilitate the organization's ability to continue to operate and take appropriate actions during an incident.

Related controls and activities: CP-02, CP-08.

Enhancements: None.

References: [TBS Directive on Security Management, Appendix D: Mandatory Procedures for Business Continuity Management Control](#)

SC-48 Sensor relocation

Control: Relocate [Assignment: organization-defined sensors and monitoring capabilities] to [Assignment: organization-defined locations] under the following conditions or circumstances: [Assignment: organization-defined conditions or circumstances].

Discussion: Adversaries may take various paths and use different approaches as they move laterally through an organization (including its systems) to reach their target or as they attempt to exfiltrate information from the organization. Organizations often only have a limited set of monitoring and detection capabilities, and they may be focused on the critical or likely infiltration or exfiltration paths.

By using communications paths that an organization typically does not monitor, an adversary can increase its chances of achieving its desired goals. By relocating its sensors or monitoring capabilities to new locations, an organization can impede the adversary's ability to achieve its goals. Sensors or monitoring capabilities might be relocated based on threat information that the organization has acquired or relocated randomly to confuse the adversary and make its lateral transition through the system or organization more challenging.

Related controls and activities: AU-02, SC-07, SI-04.

Enhancements:

(01) Sensor relocation: Dynamic relocation of sensors or monitoring capabilities

Dynamically relocate [Assignment: organization-defined sensors and monitoring capabilities] to [Assignment: organization-defined locations] under the following conditions or circumstances: [Assignment: organization-defined conditions or circumstances].

Discussion: None.

Related controls and activities: None.

References: [NIST SP 800-160 Vol. 2 Rev. 1 Developing Cyber Resilient Systems: A Systems Security Engineering Approach](#)

SC-49 Hardware-enforced separation and policy enforcement

Control: Implement hardware-enforced separation and policy enforcement mechanisms between [Assignment: organization-defined security domains].

Discussion: System owners may require additional strength of mechanism and robustness to ensure domain separation and policy enforcement for specific types of threats and environments of operation. Hardware-enforced separation and policy enforcement provide greater strength of mechanism than software-enforced separation and policy enforcement.

Related controls and activities: AC-04, SA-08, SC-50.

Enhancements: None.

References: System lifecycle cyber security and privacy risk management activities (ITSP.10.037)

SC-50 Software-enforced separation and policy enforcement

Control: Implement software-enforced separation and policy enforcement mechanisms between [Assignment: organization-defined security domains].

Discussion: System owners may require additional strength of mechanism to ensure domain separation and policy enforcement for specific types of threats and environments of operation.

Related controls and activities: AC-03, AC-04, SA-08, SC-02, SC-03, SC-49.

Enhancements: None.

References: System lifecycle cyber security and privacy risk management activities (ITSP.10.037)

SC-51 Hardware-based protection

Control:

- A. Employ hardware-based write-protect for [Assignment: organization-defined system firmware components]
- B. Implement specific procedures for [Assignment: organization-defined authorized individuals] to manually disable hardware write-protect for firmware modifications and re-enable the write-protect prior to returning to operational mode

Discussion: None.

Related controls and activities: None.

Enhancements: None.

References: None.

SC-400 Entity source authentication

Control: The information system allows a message recipient to verify the claimed source identifier in a message.

Discussion: Source authentication prevents an unauthorized entity from sending a message impersonating another entity. This control applies to non-session-based communications and can be implemented in protocols at any layer, from IP packets to electronic mail. A message is any communication between 2 entities.

Related controls and activities: IA-01, IA-02, IA-03, IA-04, IA-05, SC-08, SC-13

Enhancements:

(01) Entity source authentication: Claimed identifier authentication

Authentication of the claimed identifier in the message is cryptographically based.

Discussion: None.

Related controls and activities: None.

(02) Entity source authentication: Digital signature

The organization employs CMVP-certified cryptography for digital signature generation and verification.

Discussion: None.

Related controls and activities: SC-13.

(03) Entity source authentication: Authentication implementation

The organization employs Cyber Centre-approved cryptography and protocols to implement the authentication.

Discussion: None.

Related controls and activities: SC-13.

References:

- [Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B information \(ITSP.40.111\)](#)
- [NIST FIPS 140-3 Security Requirements for Cryptographic Modules](#)
- [Cryptographic Module Validation Program \(CMVP\)](#)

SC-401 Unclassified telecommunications in secure facilities

Control:

- A.** Unclassified telecommunications systems in secure facilities must not pass/transmit sensitive audio discussions when they are idle and not in use. Additionally, these telecommunications systems must be configured to prevent external control or activation. The concepts of on-hook audio protection outlined in CNSSI 5002 and 5006 must be incorporated into secure facilities' telecommunications systems
- B.** Unclassified telephone systems and services must be configured to prevent technical exploitation or penetration. In addition, these systems must incorporate physical and software access controls to prevent disclosure or manipulation of system programming and stored data
- C.** The organization must ensure that the following specific requirements are applied to unclassified telecommunications systems
 1. provide on-hook audio protection by the use of CNSSI 5006 equipment, CNSSI 5006-approved disconnect devices, or equivalent CNSSI 5002 system configuration
 2. provide isolation by using a computerized telephone system (CTS) with control of software and hardware configuration control and of audit reports (such as station message detail reporting, call detail reporting, etc.). System programming will not include the ability to place, or keep, a handset off-hook. Configuration of the system must ensure that all on-hook and off-hook vulnerabilities are identified and mitigated
 3. ensure that equipment used for the administration of telephone systems is installed inside an area where access is limited to authorized personnel. When local administration terminals (for a CTS) are not or cannot be contained within the controlled area or safeguarded against unauthorized manipulation, then the use of CNSSI 5006-approved telephone equipment must be required, regardless of the CTS configuration
 4. ensure that remote maintenance is not used outside the secure facility

5. ensure that speakerphones and audio-conferencing systems are not used on unclassified telecommunications systems in secure facilities. CSE may approve exceptions to this requirement when these systems have sufficient audio isolation from other classified discussion areas in the secure facility, and when there are established procedures to prevent inadvertent transmission of classified information
 6. ensure that features used for voicemail or unified messaging services are configured to prevent unauthorized access to remote diagnostic ports or internal dial tone
 7. ensure that telephone answering devices (TAD) and facsimile machines do not contain features that introduce security vulnerabilities, for example, remote room monitoring, remote programming, or other similar features that may permit off-premises access to room audio. Prior CSE approval is required before installation or use
- D. All unclassified telecommunications systems and associated infrastructure must be electrically and physically isolated from any classified information/telecommunications systems in accordance with CNSS requirements or any other separation standards applied to the classified information system on site
- E. The security requirements and installation guidelines contained in the CNSSI 5000 shall be followed for VoIP systems installed in any physical security zone processing classified information

Discussion: None.

GC discussion: A secure facility is any physical security zone that processes classified information. Secure facility may mean SCIF at the Top Secret level, or any secure facility of lower level (e.g. Secret, Confidential).

Related controls and activities: None.

Enhancements: None.

References: To access these resources, please search for the title or issue number of the publication in the [CNSS library](#):

- CNSSI 5000 Voice Over Internet Protocol (VoIP) Telephony
- CNSSI 5002 Telephony isolation used for unified communications implementations within physically protected spaces
- CNSSI 5006 National Instruction for Approved Telephone Equipment

Family: System and information integrity

The controls and activities in the System and information integrity (SI) family support the protection of the integrity of the system components and the data that is processes. They enable an organization to identify, report and correct data and system flaws in a timely manner, to provide protection against malicious code, and to monitor system security alerts and advisories in order to take appropriate actions in response.

SI-01 System and information integrity policy and procedures

Activity:

- A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]
 - 1. [Selection (1 or more): Organization-level; Mission/business process-level; System-level] system and information integrity policy that
 - a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
 - b. is consistent with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines
 - 2. procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls
- B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and information integrity policy and procedures
- C. Review and update the current system and information integrity
 - 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]
 - 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]

Discussion: System and information integrity policy and procedures address the controls in the SI family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of system and information integrity policy and procedures.

In general, security and privacy program policies and procedures at the organization level are preferable and may remove the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations.

Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.

Events that may precipitate an update to system and information integrity policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related controls and activities: PM-09, PS-08, SA-08, SI-02, SI-12.

Enhancements: None.

References: [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)

SI-02 Flaw remediation

Control:

- A. Identify, report, and correct system flaws
- B. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation
- C. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates
- D. Incorporate flaw remediation into the organizational configuration management process

Discussion: The need to remediate system flaws applies to all types of software and firmware. Organizations identify systems affected by software flaws, including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security and privacy responsibilities. Organizations consider establishing a controlled patching environment for mission-critical systems.

Security-relevant updates include patches, service packs, and malicious code signatures. Organizations also address flaws discovered during assessments, continuous monitoring, incident response activities, and system error handling. By incorporating flaw remediation into configuration management processes, required remediation actions can be tracked and verified.

Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of risk factors, including the security category of the system, the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw), the organizational risk tolerance, the mission supported by the system, or the threat environment.

Some types of flaw remediation may require more testing than others. Organizations determine the type of testing needed for the specific type of flaw remediation activity under consideration and the types of changes that are to be configuration-managed. Flaw remediation testing analyzes both the effectiveness of addressing security issues and any potential side-effects on functionality, system and system component performance, and operations. When implementing remediation activities, organizations consider the order and timing of updates to validate correct execution within the system environment and to support system and component availability needs (i.e., implementing a staggered deployment strategy). Organizations verify that software and firmware updates come from authorized sources prior to downloading. In testing decisions, organizations consider whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures.

Related controls and activities: CA-05, CM-03, CM-04, CM-05, CM-06, CM-08, MA-02, RA-05, SA-08, SA-10, SA-11, SI-03, SI-05, SI-07, SI-11.

Enhancements:

(01) Flaw remediation: Central management

Withdrawn: Incorporated into PL-09.

(02) Flaw remediation: Automated flaw remediation status

Determine if system components have applicable security-relevant software and firmware updates installed using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency].

Discussion: Automated mechanisms can track and determine the status of known flaws for system components.

Related controls and activities: CA-07, SI-04.

(03) Flaw remediation: Time to remediate flaws and benchmarks for corrective actions

- a. Measure the time between flaw identification and flaw remediation
- b. Establish the following benchmarks for taking corrective actions: [Assignment: organization-defined benchmarks]

Discussion: Organizations determine the time it takes on average to correct system flaws after such flaws have been identified and subsequently establish organizational benchmarks (i.e., timeframes) for taking corrective actions. Benchmarks can be established by the type of flaw or the severity of the potential vulnerability if the flaw can be exploited.

Related controls and activities: None.

(04) **Flaw remediation: Automated patch management tools**

Employ automated patch management tools to facilitate flaw remediation to the following system components: [Assignment: organization-defined system components].

Discussion: Using automated tools to support patch management helps to ensure the timeliness and completeness of system patching operations.

Related controls and activities: None.

(05) **Flaw remediation: Automatic software and firmware updates**

Install [Assignment: organization-defined security-relevant software and firmware updates] automatically to [Assignment: organization-defined system components].

Discussion: Due to system integrity and availability concerns, organizations consider the methodology used to carry out automatic updates. Organizations balance the need to ensure that the updates are installed as soon as possible with the need to maintain configuration management and control with any mission or operational impacts that automatic updates might impose (i.e., implementing a staggered deployment strategy).

Related controls and activities: None.

(06) **Flaw remediation: Removal of previous versions of software and firmware**

Remove previous versions of [Assignment: organization-defined software and firmware components] after updated versions have been installed.

Discussion: Previous versions of software or firmware components that are not removed from the system after updates have been installed may be exploited by adversaries. Some products may automatically remove previous versions of software and firmware from the system.

Related controls and activities: None.

(07) **Flaw remediation: Root cause analysis**

- a. Conduct root cause analysis to identify the underlying causes of issues or failures
- b. Develop actions to address the root cause of the issue or failure
- c. Implement the actions and monitor the implementation for effectiveness

Discussion: Root cause analysis includes a wide range of approaches, tools, and techniques to systematically identify the underlying causes of issues or failures in systems and systems components (i.e., hardware, software, and firmware). Organizations consider the severity of the incident to determine what root cause analysis method should be used and how quickly to implement remediation actions. The root cause analysis includes a timeline, missed warning signs, key decisions, gaps, mitigations, and verification of effectiveness. The actions identified to address the source of the issue are implemented and integrated into applicable organizational policies, procedures, and control implementations.

Related controls and activities: AC-01, AT-01, AU-01, AU-02, CA-01, CM-01, CP-01, IA-01, IR-01, IR-04, MA-01, MP-01, PE-01, PL-01, PM-01, PS-01, PT-01, RA-01, SA-01, SA-15, SC-01, SI-01, SR-01.

References:

- [TBS Patch Management Guidance](#)
- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [NIST FIPS 140-3 Security Requirements for Cryptographic Modules](#)

SI-03 Malicious code protection

Control:

- Implement [Selection (1 or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code
- Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures
- Configure malicious code protection mechanisms to
 - perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (1 or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy
 - [Selection (1 or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection
- Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system

Discussion: System entry and exit points include firewalls, remote access servers, workstations, email servers, web servers, proxy servers, notebook computers, and mobile devices. Malicious code includes viruses, worms, trojans, and spyware. Malicious code can also be encoded in various formats contained within compressed or hidden files or hidden in files using techniques such as steganography.

Malicious code can be inserted into systems in a variety of ways, including by email, web browsing, and portable storage devices. Malicious code insertions occur through the exploitation of system vulnerabilities. A variety of technologies and methods exist to limit or eliminate the effects of malicious code.

Malicious code protection mechanisms include both signature- and non-signature-based technologies. Non-signature-based detection mechanisms include AI techniques that use heuristics to detect, analyze, and describe the characteristics or behaviour of malicious code and to provide controls against such code for which signatures do not yet exist or for which existing signatures may not be effective.

Malicious code for which active signatures do not yet exist or may be ineffective includes polymorphic malicious code (i.e., code that changes signatures when it replicates). Non-signature-based mechanisms also include reputation-based technologies.

In addition to the above technologies, pervasive configuration management, comprehensive software integrity controls, and anti-exploitation software may be effective in preventing the execution of unauthorized code. Malicious code may be present in COTS software and custom-built software and could include logic bombs, backdoors, and other types of attacks that could affect organizational mission and business functions.

In situations where malicious code cannot be detected by detection methods or technologies, organizations rely on other types of controls, including secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices, to ensure that software does not perform functions other than the functions intended.

Organizations may determine that, in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, the detection of malicious downloads, or the detection of maliciousness when attempting to open or execute files.

Related controls and activities: AC-04, AC-19, CM-03, CM-08, IR-04, MA-03, MA-04, PL-09, RA-05, SC-07, SC-23, SC-26, SC-28, SC-44, SI-02, SI-04, SI-07, SI-08, SI-15.

Enhancements:

(01) **Malicious code protection: Central management**

Withdrawn: Incorporated into PL-09.

(02) **Malicious code protection: Automatic updates**

Withdrawn: Incorporated into SI-03.

(03) **Malicious code protection: Non-privileged users**

Withdrawn: Incorporated into AC-06(10).

(04) **Malicious code protection: Updates only by privileged users**

Update malicious code protection mechanisms only when directed by a privileged user.

Discussion: Protection mechanisms for malicious code are typically categorized as security-related software and, as such, are only updated by organizational personnel with appropriate access privileges.

Related controls and activities: CM-05.

(05) **Malicious code protection: Portable storage devices**

Withdrawn: Incorporated into MP-07.

(06) **Malicious code protection: Testing and verification**

- a. Test malicious code protection mechanisms [Assignment: organization-defined frequency] by introducing known benign code into the system
- b. Verify that the detection of the code and the associated incident reporting occur

Discussion: None.

Related controls and activities: CA-02, CA-07, RA-05.

(07) **Malicious code protection: Non-signature-based detection**

Withdrawn: Incorporated into SI-03.

(08) **Malicious code protection: Detect unauthorized commands**

- a. Detect the following unauthorized operating system commands through the kernel application programming interface on [Assignment: organization-defined system hardware components]: [Assignment: organization-defined unauthorized operating system commands]
- b. [Selection (1 or more): issue a warning; audit the command execution; prevent the execution of the command]

Discussion: Detecting unauthorized commands can be applied to critical interfaces other than kernel-based interfaces, including interfaces with virtual machines and privileged applications. Unauthorized operating system commands include commands for kernel functions from system processes that are not trusted to initiate such

commands as well as commands for kernel functions that are suspicious even though commands of that type are reasonable for processes to initiate.

Organizations can define the malicious commands to be detected by a combination of command types, command classes, or specific instances of commands. Organizations can also define hardware components by component type, component, component location in the network, or a combination thereof. Organizations may select different actions for different types, classes, or instances of malicious commands.

Related controls and activities: AU-02, AU-06, AU-12.

(09) **Malicious code protection: Authenticate remote commands**

Withdrawn: Moved to AC-17(10).

(10) **Malicious code protection: Malicious code analysis**

- a. Employ the following tools and techniques to analyze the characteristics and behaviour of malicious code: [Assignment: organization-defined tools and techniques]
- b. Incorporate the results from malicious code analysis into organizational incident response and flaw remediation processes

Discussion: The use of malicious code analysis tools provides organizations with a more in-depth understanding of adversary tradecraft (i.e., tactics, techniques, and procedures) and the functionality and purpose of specific instances of malicious code. Understanding the characteristics of malicious code facilitates effective organizational responses to current and future threats. Organizations can conduct malicious code analyses by employing reverse engineering techniques or by monitoring the behaviour of executing code.

Related controls and activities: None.

References:

- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [Protect your organization from malware \(ITSAP.00.057\)](#)
- [Spotting malicious email messages \(ITSAP.00.100\)](#)

SI-04 System monitoring

Control:

- A. Monitor the system to detect
 1. attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]
 2. unauthorized local, network, and remote connections
- B. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods]
- C. Invoke internal monitoring capabilities or deploy monitoring devices
 1. strategically within the system to collect organization-determined essential information
 2. at ad hoc locations within the system to track specific types of transactions of interest to the organization
- D. Analyze detected events and anomalies
- E. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or Canada
- F. Obtain legal opinion regarding system monitoring activities

- G. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (1 or more): as needed; [Assignment: organization-defined frequency]]

Discussion: System monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at external interfaces to the system. Internal monitoring includes the observation of events occurring within the system. Organizations monitor systems by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives guide and inform the determination of the events. System monitoring capabilities are achieved through a variety of tools and techniques, including intrusion detection and prevention systems, malicious code protection software, scanning tools, audit record monitoring software, and network monitoring software.

Depending on the security architecture, the distribution and configuration of monitoring devices may impact throughput at key internal and external boundaries, as well as at other locations across a network due to the introduction of network throughput latency. If throughput management is needed, such devices are strategically located and deployed as part of an established organization-wide security architecture. Strategic locations for monitoring devices include selected perimeter locations and near key servers and server farms that support critical applications.

Monitoring devices are typically employed at the managed interfaces associated with controls SC-07 and AC-17. The information collected is a function of the organizational monitoring objectives and the capability of systems to support such objectives. Specific types of transactions of interest include Hypertext Transfer Protocol (HTTP) traffic that bypasses HTTP proxies.

System monitoring is an integral part of organizational continuous monitoring and incident response programs, and output from system monitoring serves as input to those programs. System monitoring requirements, including the need for specific types of system monitoring, may be referenced in other controls (e.g., AC-02G, AC-02(07), AC-02(12)a, AC-17(01), AU-13, AU-13(01), AU-13(02), CM-03F, CM-06D, MA-03A, MA-04A, SC-05(03)b, SC-07A, SC-07(24)b, SC-18B, SC-43B).

Adjustments to levels of system monitoring are based on law enforcement information, intelligence information, or other sources of information. The legality of system monitoring activities is based on applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines.

Related controls and activities: AC-02, AC-03, AC-04, AC-08, AC-17, AU-02, AU-06, AU-07, AU-09, AU-12, AU-13, AU-14, CA-07, CM-03, CM-06, CM-08, CM-11, IA-10, IR-04, MA-03, MA-04, PL-09, PM-12, RA-05, RA-10, SC-05, SC-07, SC-18, SC-26, SC-31, SC-35, SC-36, SC-37, SC-43, SI-03, SI-06, SI-07, SR-09, SR-10.

Enhancements:

(01) **System monitoring: System-wide intrusion detection system**

Connect and configure individual intrusion detection tools into a system-wide intrusion detection system.

Discussion: Linking individual intrusion detection tools into a system-wide intrusion detection system provides additional coverage and effective detection capabilities. The information contained in one intrusion detection tool can be shared widely across the organization, making the system-wide detection capability more robust and powerful.

Related controls and activities: None.

(02) **System monitoring: Automated tools and mechanisms for real-time analysis**

Employ automated tools and mechanisms to support near real-time analysis of events.

Discussion: Automated tools and mechanisms include host-based, network-based, transport-based, or storage-based event monitoring tools and mechanisms or SIEM technologies that provide real-time analysis of alerts and notifications generated by organizational systems. Automated monitoring techniques can create unintended privacy risks because automated controls may connect to external or otherwise unrelated systems. The matching of records between these systems may create linkages with unintended consequences. Organizations assess and document these risks in their PIA and make determinations that are in alignment with their privacy program plan.

Related controls and activities: PM-23, PM-25.

(03) **System monitoring: Automated tool and mechanism integration**

Employ automated tools and mechanisms to integrate intrusion detection tools and mechanisms into access control and flow control mechanisms.

Discussion: Using automated tools and mechanisms to integrate intrusion detection tools and mechanisms into access and flow control mechanisms facilitates a rapid response to attacks by enabling the reconfiguration of mechanisms in support of attack isolation and elimination.

Related controls and activities: PM-23, PM-25.

(04) **System monitoring: Inbound and outbound communications traffic**

- a. Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic
- b. Monitor inbound and outbound communications traffic [Assignment: organization-defined frequency] for [Assignment: organization-defined unusual or unauthorized activities or conditions]

Discussion: Unusual or unauthorized activities or conditions related to system inbound and outbound communications traffic includes internal traffic that indicates the presence of malicious code or unauthorized use of legitimate code or credentials within organizational systems or propagating among system components, signaling to external systems, and the unauthorized exporting of information. Evidence of malicious code or unauthorized use of legitimate code or credentials is used to identify potentially compromised systems or system components.

Related controls and activities: None.

(05) **System monitoring: System-generated alerts**

Alert [Assignment: organization-defined personnel or roles] when the following system-generated indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].

Discussion: Alerts may be generated from a variety of sources, including audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be automated and may be transmitted by telephone, email, or text message.

Organizational personnel on the alert notification list can include system administrators, mission or business owners, system owners, information owners/stewards, senior officials in the department's security governance, appropriate privacy senior officials or executives, system security officers, or privacy officers. In contrast to alerts generated by the system, alerts generated by organizations in SI-04(12) focus on information sources external to the system, such as suspicious activity reports and reports on potential insider threats.

Related controls and activities: AU-04, AU-05, PE-06.

(06) **System monitoring: Restrict non-privileged users**

Withdrawn: Incorporated into AC-06(10).

(07) **System monitoring: Automated response to suspicious events**

- a. Notify [Assignment: organization-defined incident response personnel (identified by name and/or by role)] of detected suspicious events
- b. Take the following actions upon detection: [Assignment: organization-defined least-disruptive actions to terminate suspicious events]

Discussion: Least-disruptive actions include initiating requests for human responses.

Related controls and activities: None.

(08) System monitoring: Protection of monitoring information

Withdrawn: Incorporated into SI-04.

(09) System monitoring: Testing of monitoring tools and mechanisms

Test intrusion monitoring tools and mechanisms [Assignment: organization-defined frequency].

Discussion: It is necessary to test intrusion monitoring tools and mechanisms to ensure that they are operating correctly and continue to satisfy the monitoring objectives of organizations. The frequency and depth of testing depends on the types of tools and mechanisms used by organizations and the methods of deployment.

Related controls and activities: None.

(10) System monitoring: Visibility of encrypted communications

Make provisions so that [Assignment: organization-defined encrypted communications traffic] is visible to [Assignment: organization-defined system monitoring tools and mechanisms].

Discussion: Organizations balance the need to encrypt communications traffic to protect data confidentiality with the need to maintain visibility into such traffic from a monitoring perspective. Organizations determine whether the visibility requirement applies to internal encrypted traffic, encrypted traffic intended for external destinations, or a subset of the traffic types.

Related controls and activities: None.

(11) System monitoring: Analyze communications traffic anomalies

Analyze outbound communications traffic at the external interfaces to the system and selected [Assignment: organization-defined internal points within the system] to discover anomalies.

Discussion: Organization-defined internal points include subnetworks and subsystems. Anomalies within organizational systems include large file transfers, long-time persistent connections, attempts to access information from unexpected locations, the use of unusual protocols and ports, the use of unmonitored network protocols (e.g., IPv6 usage during IPv4 transition), and attempted communications with suspected malicious external addresses.

Related controls and activities: None.

(12) System monitoring: Automated organization-generated alerts

Alert [Assignment: organization-defined personnel or roles] using [Assignment: organization-defined automated mechanisms] when the following indications of inappropriate or unusual activities with security or privacy implications occur: [Assignment: organization-defined activities that trigger alerts].

Discussion: Organizational personnel on the system alert notification list include system administrators, mission or business owners, system owners, the senior agency information security officer, the appropriate privacy senior official or executive, system security officers, or privacy officers.

Automated organization-generated alerts are the security alerts generated by organizations and transmitted using automated means. The sources for organization-generated alerts are focused on other entities such as suspicious activity reports and reports on potential insider threats. In contrast to alerts generated by the organization, alerts generated by the system in SI-04(05) focus on information sources that are internal to the systems, such as audit records.

Related controls and activities: None.

(13) System monitoring: Analyze traffic and event patterns

- a. Analyze communications traffic and event patterns for the system
- b. Develop profiles representing common traffic and event patterns

- c. Use the traffic and event profiles to tune system monitoring devices

Discussion: Identifying and understanding common communications traffic and event patterns helps organizations provide useful information to system monitoring devices to more effectively identify suspicious or anomalous traffic and events when they occur. Such information can help reduce the number of false positives and false negatives during system monitoring.

Related controls and activities: None.

(14) **System monitoring: Wireless intrusion detection**

Employ a wireless intrusion detection system (WIDS) to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system.

Discussion: Wireless signals may radiate beyond organizational facilities. Organizations proactively search for unauthorized wireless connections, including by conducting thorough scans for unauthorized wireless access points. Wireless scans are not limited to those areas within facilities containing systems but also include areas outside of facilities to verify that unauthorized wireless access points are not connected to organizational systems.

Related controls and activities: AC-18, IA-03.

(15) **System monitoring: Wireless to wireline communications**

Employ an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.

Discussion: Wireless networks are inherently less secure than wired networks. For example, wireless networks are more susceptible to eavesdroppers or traffic analysis than wireline networks. When wireless to wireline communications exist, the wireless network could become a port of entry into the wired network. Given that it is easier to gain unauthorized network access from wireless access points than from wired access points, it may be necessary to conduct additional monitoring of traffic transitioning between wireless and wired networks to detect malicious activities. Employing intrusion detection systems to monitor wireless communications traffic helps ensure that the traffic does not contain malicious code prior to transitioning to the wireline network.

Related controls and activities: AC-18.

(16) **System monitoring: Correlate monitoring information**

Correlate information from monitoring tools and mechanisms employed throughout the system.

Discussion: Correlating information from different system monitoring tools and mechanisms can provide a more comprehensive view of system activity. Correlating system monitoring tools and mechanisms that typically work in isolation—including malicious code protection software, host monitoring, and network monitoring—can provide an organization-wide monitoring view and may reveal otherwise unseen attack patterns. Understanding the capabilities and limitations of diverse monitoring tools and mechanisms and how to maximize the use of information generated by those tools and mechanisms can help organizations develop, operate, and maintain effective monitoring programs. The correlation of monitoring information is especially important during the transition from older to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols).

Related controls and activities: AU-06.

(17) **System monitoring: Integrated situational awareness**

Correlate information from monitoring physical, cyber, and supply chain activities to achieve integrated, organization-wide situational awareness.

Discussion: Correlating monitoring information from a more diverse set of information sources helps to achieve integrated situational awareness. Integrated situational awareness from a combination of physical, cyber, and supply chain monitoring activities enhances the capability of organizations to more quickly detect sophisticated attacks and investigate the methods and techniques employed to carry out such attacks.

In contrast to SI-04(16), which correlates with the various cyber monitoring information, integrated situational awareness is intended to correlate monitoring beyond the cyber domain. Correlation of monitoring information from multiple activities may help reveal attacks on organizations from threat actors that are operating across multiple attack vectors.

Related controls and activities: AU-16, PE-06, SR-02, SR-04, SR-06.

(18) **System monitoring: Analyze traffic and covert exfiltration**

Analyze outbound communications traffic at external interfaces to the system and at the following internal points to detect covert exfiltration of information: [Assignment: organization-defined interior points within the system].

Discussion: Organization-defined internal points include subnetworks and subsystems. Covert means that can be used to exfiltrate information include steganography.

Related controls and activities: None.

(19) **System monitoring: Risk for individuals**

Implement [Assignment: organization-defined additional monitoring] of individuals who have been identified by [Assignment: organization-defined sources] as posing an increased level of risk.

Discussion: Indications of increased risk from individuals can be obtained from different sources, including personnel records, intelligence agencies, law enforcement organizations, and other sources. The monitoring of individuals is coordinated with the management, legal, security, privacy, and human resources officials who conduct such monitoring. Monitoring is conducted in accordance with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines.

Related controls and activities: None.

(20) **System monitoring: Privileged user**

Implement the following additional monitoring of privileged users: [Assignment: organization-defined additional monitoring].

Discussion: Privileged users have access to more sensitive information, including security-related information, than the general user population. Access to such information means that privileged users can potentially do greater damage to systems and organizations than non-privileged users. Therefore, implementing additional monitoring on privileged users helps to ensure that organizations can identify malicious activity at the earliest possible time and take appropriate actions.

Related controls and activities: AC-18.

(21) **System monitoring: Probationary periods**

Implement the following additional monitoring of individuals during [Assignment: organization-defined probationary period]: [Assignment: organization-defined additional monitoring].

Discussion: During probationary periods, employees do not have permanent employment status within organizations. Without such status or access to information that is resident on the system, additional monitoring can help identify any potentially malicious activity or inappropriate behaviour.

Related controls and activities: AC-18.

(22) **System monitoring: Unauthorized network services**

- a. Detect network services that have not been authorized or approved by [Assignment: organization-defined authorization or approval processes]
- b. [Selection (1 or more): Audit; Alert [Assignment: organization-defined personnel or roles]] when detected

Discussion: Unauthorized or unapproved network services include services in service-oriented architectures that lack organizational verification or validation and may therefore be unreliable or serve as malicious rogues for valid services.

Related controls and activities: CM-07.

(23) **System monitoring: Host-based devices**

Implement the following host-based monitoring mechanisms at [Assignment: organization-defined system components]: [Assignment: organization-defined host-based monitoring mechanisms].

Discussion: Host-based monitoring collects information about the host (or system in which it resides). System components in which host-based monitoring can be implemented include servers, notebook computers, and mobile devices. Organizations may consider employing host-based monitoring mechanisms from multiple product developers or vendors.

Related controls and activities: AC-18, AC-19.

(24) **System monitoring: Indicators of compromise**

Discover, collect, and distribute to [Assignment: organization-defined personnel or roles], indicators of compromise (IOCs) provided by [Assignment: organization-defined sources].

Discussion: IOCs are forensic artifacts from intrusions that are identified on organizational systems at the host or network level. IOCs provide valuable information on systems that have been compromised. IOCs can include the creation of registry key values. IOCs for network traffic include Universal Resource Locator (URL) or protocol elements that indicate malicious code command-and-control (C2) servers. The rapid distribution and adoption of IOCs can improve information security by reducing the time that systems and organizations are vulnerable to the same exploit or attack. Threat indicators, signatures, tactics, techniques, procedures, and other IOCs may be available via governmental and non-governmental cooperatives, including the Forum of Incident Response and Security Teams (FIRST), the Canadian Cyber Threat Exchange (CCTX), and the Cyber Centre as the Computer Emergency Readiness Team (CERT-CA).

Related controls and activities: AC-18.

(25) **System monitoring: Optimize network traffic analysis**

Provide visibility into network traffic at external and key internal system interfaces to optimize the effectiveness of monitoring devices.

Discussion: Encrypted traffic, asymmetric routing architectures, capacity and latency limitations, and transitioning from older to newer technologies (e.g., IPv4 to IPv6 network protocol transition) may result in blind spots for organizations when analyzing network traffic. Collecting, decrypting, pre-processing, and distributing only relevant traffic to monitoring devices can streamline the effectiveness and use of devices and optimize traffic analysis.

Related controls and activities: None.

References:

- [TBS Policy on Government Security](#)
- [TBS Policy on Service and Digital](#)
- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [TBS Directive on Security Management, Appendix G: Mandatory Procedures for Security Event Management Control](#)
- [TBS Government of Canada Cyber Security Event Management Plan \(GC CSEMP\)](#)
- [TBS Event Logging Guidance](#)

SI-05 Security alerts, advisories, and directives

Control:

- A. Receive system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis
- B. Generate internal security alerts, advisories, and directives as necessary
- C. Disseminate security alerts, advisories, and directives to: [Selection (1 or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]
- D. Implement security directives in accordance with established timeframes or notify the issuing organization of the degree of non-compliance

Discussion: The Cyber Centre generates security alerts and advisories to maintain situational awareness throughout the GC. Security directives are issued by TBS or other designated organizations with the responsibility and authority to issue such directives. Compliance with security directives is essential due to the critical nature of many of these directives and the potential (immediate) adverse effects on organizational operations and assets, individuals, other organizations, and Canada should the directives not be implemented in a timely manner. External organizations include supply chain partners, external mission or business partners, external service providers, and other peer or supporting organizations.

Related controls and activities: PM-15, RA-05, SI-02.

Enhancements:

(01) Security alerts, advisories, and directives: Automated alerts and advisories

Broadcast security alert and advisory information throughout the organization using [Assignment: organization-defined automated mechanisms].

Discussion: The significant number of changes to organizational systems and operational environments requires the dissemination of security-related information to a variety of organizational entities that have a direct interest in the success of organizational mission and business functions. Based on information provided by security alerts and advisories, changes may be required at one or more of the 3 levels related to risk management, including the governance level, mission and business process level, and the information system level.

Related controls and activities: None.

References: [TBS Policy on Government Security](#)

SI-06 Security and privacy function verification

Control:

- A. Verify the correct operation of [Assignment: organization-defined security and privacy functions]
- B. Perform the verification of the functions specified in SI-06A [Selection (1 or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; [Assignment: organization-defined frequency]]
- C. Alert [Assignment: organization-defined personnel or roles] to failed security and privacy verification tests
- D. [Selection (1 or more): Shut the system down; Restart the system; [Assignment: organization-defined alternative action(s)]] when anomalies are discovered

Discussion: Transitional states for systems include system start-up, restart, shutdown, and abort. System notifications include hardware indicator lights, electronic alerts to system administrators, and messages to local computer consoles. In contrast to security function verification, privacy function verification ensures that privacy functions operate as expected

and are approved by the appropriate privacy senior official or executive or that privacy attributes are applied or used as expected.

Related controls and activities: CA-07, CM-04, CM-06, SI-07.

Enhancements:

(01) **Security and privacy function verification: Notification of failed security tests**

Withdrawn: Incorporated into SI-06.

(02) **Security and privacy function verification: Automation support for distributed testing**

Implement automated mechanisms to support the management of distributed security and privacy function testing.

Discussion: The use of automated mechanisms to support the management of distributed function testing helps ensure the integrity, timeliness, completeness, and efficacy of such testing.

Related controls and activities: SI-02.

(03) **Security and privacy function verification: Report verification results**

Report the results of security and privacy function verification to [Assignment: organization-defined personnel or roles].

Discussion: Organizational personnel with potential interest in the results of the verification of security and privacy functions include systems security officers, senior officials in the department's security governance, and appropriate privacy senior officials or executives.

Related controls and activities: SI-04, SR-04, SR-05.

References: None.

SI-07 Software, firmware, and information integrity

Control:

- A. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]
- B. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined actions]

Discussion: Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity. Software includes operating systems (with key internal components, such as kernels or drivers), middleware, and applications. Firmware interfaces include Unified Extensible Firmware Interface (UEFI) and Basic Input/Output System (BIOS). Information includes personal information and metadata that contains security and privacy attributes associated with information. Integrity checking mechanisms—including parity checks, cyclical redundancy checks, cryptographic hashes, and associated tools—can automatically monitor the integrity of systems and hosted applications.

Related controls and activities: AC-04, CM-03, CM-07, CM-08, MA-03, MA-04, RA-05, SA-08, SA-09, SA-10, SC-08, SC-12, SC-13, SC-28, SC-37, SI-03, SR-03, SR-04, SR-05, SR-06, SR-09, SR-10, SR-11.

Enhancements:

(01) **Software, firmware, and information integrity: Integrity checks**

Perform an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (1 or more): at start-up; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization-defined frequency]].

Discussion: Security-relevant events include the identification of new threats to which organizational systems are susceptible and the installation of new hardware, software, or firmware. Transitional states include system start-up, restart, shutdown, and abort.

Related controls and activities: None.

(02) **Software, firmware, and information integrity: Automated notifications of integrity violations**

Employ automated tools that notify [Assignment: organization-defined personnel or roles] upon discovering discrepancies during integrity verification.

Discussion: Using automated tools to report system and information integrity violations and to notify organizational personnel in a timely matter is essential for effective risk response. Personnel with an interest in system and information integrity violations include mission and business owners, system owners, senior officials in the department's security governance, the appropriate privacy senior official or executive, system administrators, software developers, systems integrators, information security officers, and privacy officers.

Related controls and activities: None.

(03) **Software, firmware, and information integrity: Centrally managed integrity tools**

Employ centrally managed integrity verification tools.

Discussion: Centrally managed integrity verification tools provide greater consistency in the application of such tools and can facilitate more comprehensive coverage of integrity verification actions.

Related controls and activities: AU-03, SI-02, SI-08.

(04) **Software, firmware, and information integrity: Tamper-evident packaging**

Withdrawn: Incorporated into SA-12.

(05) **Software, firmware, and information integrity: Automated response to integrity violations**

Automatically [Selection (1 or more): shut the system down; restart the system; implement [Assignment: organization-defined controls]] when integrity violations are discovered.

Discussion: Organizations may define different integrity checking responses by type of information, specific information, or a combination of both. Types of information include firmware, software, and user data. Specific information includes boot firmware for certain types of machines. The automatic implementation of controls within organizational systems includes reversing the changes, halting the system, or triggering audit alerts when unauthorized modifications to critical security files occur.

Related controls and activities: None.

(06) **Software, firmware, and information integrity: Cryptographic protection**

Implement cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.

Discussion: Cryptographic mechanisms used to protect integrity include digital signatures and the computation and application of signed hashes using asymmetric cryptography, protecting the confidentiality of the key used to generate the hash, and using the public key to verify the hash information. Organizations that employ cryptographic mechanisms should also consider cryptographic key management solutions.

Related controls and activities: SC-12, SC-13.

(07) **Software, firmware, and information integrity: Integration of detection and response**

Incorporate the detection of the following unauthorized changes into the organizational incident response capability: [Assignment: organization-defined security-relevant changes to the system].

Discussion: Integrating detection and response helps ensure that detected events are tracked, monitored, corrected, and available for historical purposes. It is important to maintain historical records to identify and discern adversary actions over an extended period and for possible legal actions. Security-relevant changes include unauthorized changes to established configuration settings or the unauthorized elevation of system privileges.

Related controls and activities: AU-02, AU-06, IR-04, IR-05, SI-04.

(08) **Firmware and information integrity: Auditing capability for significant events**

Upon detection of a potential integrity violation, provide the capability to audit the event and initiate the following actions: [Selection (1 or more): generate an audit record; alert current user; alert [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined other actions]].

Discussion: Organizations select response actions based on types of software, specific software, or information for which there are potential integrity violations.

Related controls and activities: AU-02, AU-06, AU-12.

(09) **Software, firmware, and information integrity: Verify boot process**

Verify the integrity of the boot process of the following system components: [Assignment: organization-defined system components].

Discussion: Ensuring the integrity of boot processes is critical to starting system components in known, trustworthy states. Integrity verification mechanisms provide a level of assurance that only trusted code is executed during boot processes.

Related controls and activities: SI-06.

(10) **Software, firmware, and information integrity: Protection of boot firmware**

Implement the following mechanisms to protect the integrity of boot firmware in [Assignment: organization-defined system components]: [Assignment: organization-defined mechanisms].

Discussion: Unauthorized modifications to boot firmware may indicate a sophisticated, targeted attack. These types of targeted attacks can result in a permanent denial of service or a persistent malicious code presence. These situations can occur if the firmware is corrupted or if the malicious code is embedded within the firmware. System components can protect the integrity of boot firmware in organizational systems by verifying the integrity and authenticity of all updates to the firmware prior to applying changes to the system component and preventing unauthorized processes from modifying the boot firmware.

Related controls and activities: SI-06.

(11) **Software, firmware, and information integrity: Confined environments with limited privileges**

Withdrawn: Moved to CM-07(06).

(12) **Software, firmware, and information integrity: Integrity verification**

Require that the integrity of the following software be verified prior to execution: [Assignment: organization-defined software].

Discussion: Organizations verify the integrity of software prior to execution to reduce the likelihood of executing malicious code or programs that contain errors from unauthorized modifications. Organizations consider the source of the software, ensuring the software and updates come from authorized sources and/or sites, and the practicality of approaches for verifying software integrity, including the availability of trustworthy checksums from software developers and vendors.

Related controls and activities: CM-11, SI-02.

(13) **Software, firmware, and information integrity: Code execution in protected environments**

Withdrawn: Moved to CM-07(07).

(14) **Software, firmware, and information integrity: Binary or machine-executable code**

Withdrawn: Moved to CM-07(08).

(15) **Software, firmware, and information integrity: Code authentication**

Implement cryptographic mechanisms to authenticate the following software or firmware components prior to installation: [Assignment: organization-defined software or firmware components].

Discussion: Cryptographic authentication includes verifying that software or firmware components have been digitally signed using certificates recognized and approved by organizations. Code signing is an effective method to protect against malicious code. Organizations that employ cryptographic mechanisms should also consider cryptographic key management solutions.

Related controls and activities: CM-05, SC-12, SC-13.

(16) **Software, firmware, and information integrity: Time limit on process execution without supervision**

Prohibit processes from executing without supervision for more than [Assignment: organization-defined time period].

Discussion: Placing a time limit on process execution without supervision is intended to apply to processes for which typical or normal execution periods can be determined and situations in which organizations exceed such periods. Supervision includes timers on operating systems, automated responses, and manual oversight and response when system process anomalies occur.

Related controls and activities: None.

(17) **Software, firmware, and information integrity: Runtime application self-protection**

Implement [Assignment: organization-defined controls] for application self-protection at runtime.

Discussion: Runtime application self-protection employs runtime instrumentation to detect and block the exploitation of software vulnerabilities by taking advantage of information from the software in execution. Runtime exploit prevention differs from traditional perimeter-based protections such as guards and firewalls which can only detect and block attacks by using network information without contextual awareness.

Runtime application self-protection technology can reduce the susceptibility of software to attacks by monitoring its inputs and blocking those inputs that could allow attacks. It can also help protect the runtime environment from unwanted changes and tampering. When a threat is detected, runtime application self-protection technology can prevent exploitation and take other actions (e.g., sending a warning message to the user, terminating the user's session, terminating the application, or sending an alert to organizational personnel). Runtime application self-protection solutions can be deployed in either monitor or protection mode.

Related controls and activities: SI-16.

References:

- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [NIST FIPS 140-3 Security Requirements for Cryptographic Modules](#)
- [NIST FIPS 180-4: Secure Hash Standard \(SHS\)](#)
- [NIST FIPS 186-5 Digital Signature Standard \(DSS\)](#)
- [NIST FIPS 202 SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions](#)

SI-08 Spam protection

Control:

- A. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages
- B. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures

Discussion: System entry and exit points include firewalls, remote-access servers, email servers, web servers, proxy servers, workstations, notebook computers, and mobile devices. Spam can be transported by different means, including email, email attachments, and web access. Spam protection mechanisms include signature definitions.

Related controls and activities: PL-09, SC-05, SC-07, SC-38, SI-03, SI-04.

Enhancements:

(01) Spam protection: Central management

Withdrawn: Incorporated into PL-09.

(02) Spam protection: Automatic updates

Automatically update spam protection mechanisms [Assignment: organization-defined frequency].

Discussion: Using automated mechanisms to update spam protection mechanisms helps ensure that updates occur on a regular basis and provide the latest content and protection capabilities.

Related controls and activities: None.

(03) Spam protection: Continuous learning capability

Implement spam protection mechanisms with a learning capability to identify legitimate communications traffic more effectively.

Discussion: Learning mechanisms include Bayesian filters that respond to user inputs that identify specific traffic as spam or legitimate by updating algorithm parameters and thereby separating types of traffic more accurately.

Related controls and activities: None.

References: [Implementation guidance: email domain protection \(ITSP.40.065\)](#)

SI-09 Information input restrictions

Withdrawn: Incorporated into AC-02, AC-03, AC-05, and AC-06.

SI-10 Information input validation

Control: Check the validity of the following information inputs: [Assignment: organization-defined information inputs to the system].

Discussion: Checking the valid syntax and semantics of system inputs—including character set, length, numerical range, and acceptable values—verifies that inputs match specified definitions for format and content. For example, if the organization specifies that numerical values between 1 and 100 are the only acceptable inputs for a field in a given application, inputs of “387”, “abc”, or “%K%” are invalid inputs and are not accepted as input to the system.

Valid inputs are likely to vary from field to field within a software application. Applications typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information.

If software applications use attacker-supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata. Consequently, the module or component that receives the corrupted output will perform the wrong operations or otherwise interpret the data incorrectly.

Pre-screening inputs prior to passing them to interpreters prevents the content from being unintentionally interpreted as commands. Input validation ensures accurate and correct inputs and prevents attacks such as cross-site scripting and a variety of injection attacks.

Related controls and activities: None.

Enhancements:

(01) Information input validation: Manual override capability

- a. Provide a manual override capability for input validation of the following information inputs: [Assignment: organization-defined inputs defined in the base control (SI-10)]
- b. Restrict the use of the manual override capability to only [Assignment: organization-defined authorized individuals]
- c. Audit the use of the manual override capability

Discussion: In certain situations, such as during events that are defined in contingency plans, a manual override capability for input validation may be needed. Manual overrides are used only in limited circumstances and with the inputs defined by the organization.

Related controls and activities: AC-03, AU-02, AU-12.

(02) Information input validation: Review and resolution of errors

Review and resolve input validation errors within [Assignment: organization-defined time period].

Discussion: Resolution of input validation errors includes correcting systemic causes of errors and resubmitting transactions with corrected input. Input validation errors are those related to the information inputs defined by the organization in the base control (SI-10).

Related controls and activities: None.

(03) Information input validation: Predictable behaviour

Verify that the system behaves in a predictable and documented manner when invalid inputs are received.

Discussion: A common vulnerability in organizational systems is unpredictable behaviour when invalid inputs are received. Verifying system predictability helps ensure that the system behaves as expected when invalid inputs are received. This occurs by specifying system responses that allow the system to transition to known states without adverse, unintended side effects. The invalid inputs are those related to the information inputs defined by the organization in the base control (SI-10).

Related controls and activities: None.

(04) Information input validation: Timing interactions

Account for timing interactions among system components in determining appropriate responses for invalid inputs.

Discussion: When addressing invalid system inputs received across protocol interfaces, timing interactions become relevant, where one protocol needs to consider the impact of the error response on other protocols in the protocol stack.

For example, 802.11 standard wireless network protocols do not interact well with Transmission Control Protocols (TCP) when packets are dropped (which could be due to invalid packet input). TCP assumes packet losses are due

to congestion, while packets lost over 802.11 links are typically dropped due to noise or collisions on the link. If TCP makes a congestion response, it takes the wrong action in response to a collision event.

Adversaries may be able to use what appear to be acceptable individual behaviours of the protocols in concert to achieve adverse effects through suitable construction of invalid input. The invalid inputs are those related to the information inputs defined by the organization in the base control (SI-10).

Related controls and activities: None.

(05) **Information input validation: Restrict inputs to trusted sources and approved formats**

Restrict the use of information inputs to [Assignment: organization-defined trusted sources] and/or [Assignment: organization-defined formats].

Discussion: Restricting the use of inputs to trusted sources and in trusted formats applies the concept of authorized or permitted software to information inputs. Specifying known trusted sources for information inputs and acceptable formats for such inputs can reduce the probability of malicious activity. The information inputs are those defined by the organization in the base control (SI-10).

Related controls and activities: AC-03, AC-06.

(06) **Information input validation: Injection prevention**

Prevent untrusted data injections.

Discussion: Untrusted data injections may be prevented using a parameterized interface or output escaping (output encoding). Parameterized interfaces separate data from code so that injections of malicious or unintended data cannot change the semantics of commands being sent. Output escaping uses specified characters to inform the interpreter's parser whether data is trusted. Preventing untrusted data injections refers to the information inputs defined by the organization in the base control (SI-10).

Related controls and activities: AC-03, AC-06.

References: None.

SI-11 Error handling

Control:

- A. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited
- B. Reveal error messages only to [Assignment: organization-defined personnel or roles]

Discussion: Organizations consider the structure and content of error messages. The extent to which systems can handle error conditions is guided and informed by organizational policy and operational requirements. Exploitable information includes stack traces and implementation details; erroneous logon attempts with passwords mistakenly entered as the username; mission or business information that can be derived from, if not stated explicitly by, the information recorded; and personal information, such as account numbers, social insurance numbers, and credit card numbers. Error messages may also provide a covert channel for transmitting information.

Related controls and activities: AU-02, AU-03, SC-31, SI-02, SI-15.

Enhancements: None.

References: None.

SI-12 Information management and retention

Control: Manage and retain information within the system and information output from the system in accordance with applicable laws, Orders in Council, directives, regulations, policies, standards, guidelines, and operational requirements.

Discussion: Information management and retention requirements cover the full lifecycle of information, in some cases extending beyond system disposal. Information to be retained may also include policies, procedures, plans, reports, data output from control implementation, and other types of administrative information.

Library and Archives Canada provides federal policy and guidance on records retention and schedules. The authority to dispose is granted through a disposition instrument signed by the Librarian and Archivist of Canada. Retention schedules are derived collaboratively between program officials and information management officials and are in line with the goal of retaining personal information for the least amount of time required.

If organizations have a records management office, consider coordinating with records management personnel. Records produced from the output of implemented controls that may require management and retention include, but are not limited to: All XX-01, AC-06(09), AT-04, AU-12, CA-02, CA-03, CA-05, CA-06, CA-07, CA-08, CA-09, CM-02, CM-03, CM-04, CM-06, CM-08, CM-09, CM-12, CM-13, CP-02, IR-06, IR-08, MA-02, MA-04, PE-02, PE-08, PE-16, PE-17, PL-02, PL-04, PL-07, PL-08, PM-05, PM-08, PM-09, PM-18, PM-21, PM-27, PM-28, PM-30, PM-31, PS-02, PS-06, PS-07, PT-02, PT-03, PT-07, RA-02, RA-03, RA-05, RA-08, SA-04, SA-05, SA-08, SA-10, SI-04, SR-02, SR-04, SR-08.

Related controls and activities: AC-16, AU-05, AU-11, CA-02, CA-03, CA-05, CA-06, CA-07, CA-09, CM-05, CM-09, CP-02, IR-08, MP-02, MP-03, MP-04, MP-06, PL-02, PL-04, PM-04, PM-08, PM-09, PS-02, PS-06, PT-02, PT-03, RA-02, RA-03, SA-05, SA-08, SR-02.

Enhancements:

(01) Information management and retention: Limit personal information elements

Limit personal information being processed in the information lifecycle to the following elements of personal information: [Assignment: organization-defined elements of personal information].

Discussion: Limiting the retention of personal information throughout the information lifecycle when the information is not needed for operational purposes helps reduce the level of privacy risk created by a system. The information lifecycle includes information creation, collection, use, handling, storage, maintenance, dissemination, disclosure, and disposition. Risk assessments, as well as applicable laws, regulations, and policies, can provide useful inputs to determine which elements of personal information may create risk.

GC discussion: The Privacy Regulations stipulate that personal information, if used to make administrative decisions, must be retained for 2 years past the last administrative action, to enable the individual to request access to their personal information. If personal information is aggregated and it is determined that the individual cannot be re-identified using the aggregate data, this information can be held for as long as necessary.

Related controls and activities: PM-25.

(02) Information management and retention: Minimize personal information in testing, training, and research

Use the following techniques to minimize the use of personal information for research, testing, or training: [Assignment: organization-defined techniques].

Discussion: Organizations can minimize the risk to an individual's privacy by employing techniques such as de-identification or synthetic data. Limiting the use of personal information throughout the information lifecycle when the information is not needed for research, testing, or training helps reduce the level of privacy risk created by a system. Risk assessments, as well as applicable laws, regulations, and policies, can provide useful inputs to determine the techniques to use and when to use them.

GC discussion: If personal information is to be used for research, testing or training, individuals should be provided prior notice about this use, and the associated (if applicable) PIB should reflect this use of the personal information.

If the use of the personal information for these purposes is not considered to be a use consistent with the purpose of collection, consent to use the personal information may be required.

Related controls and activities: PM-22, PM-25, SI-19.

(03) **Information management and retention: Information disposal**

Use the following techniques to dispose of, destroy, or erase information following the retention period:
[Assignment: organization-defined techniques].

Discussion: Organizations can minimize both security and privacy risks by disposing of information when it is no longer needed. The disposal or destruction of information applies to originals as well as copies and archived records, including system logs, that may contain personal information.

Related controls and activities: None.

References:

- [IT media sanitization \(ITSP.40.006\)](#)
- [RCMP GCPSP-001 Equipment Selection Guide for Paper Shredders](#)
- [TBS Directive on Security Management, Appendix E: Mandatory Procedures for Information Management Security Control](#)
- [TBS Directive on Security Management, Appendix J: Standard on Security Categorization](#)
- [TBS Directive on Privacy Practices](#)
- [Privacy Regulations SOR/83-508](#)

SI-13 Predictable failure prevention

Control:

- Determine mean time to failure (MTTF) for the following system components in specific environments of operation:
[Assignment: organization-defined system components]
- Provide substitute system components and a means to exchange active and standby components in accordance with the following criteria: [Assignment: organization-defined MTTF substitution criteria]

Discussion: While MTTF is primarily a reliability issue, predictable failure prevention is intended to address potential failures of system components that provide security capabilities. Failure rates reflect installation-specific considerations rather than the industry average. Organizations define the criteria for the substitution of system components based on the MTTF value with consideration for the potential harm from component failures. The transfer of responsibilities between active and standby components does not compromise safety, operational readiness, or security capabilities. The preservation of system state variables is also critical to help ensure a successful transfer process. Standby components remain available at all times except for maintenance issues or recovery failures in progress.

Related controls and activities: CP-02, CP-10, CP-13, MA-02, MA-06, SA-08, SC-06.

Enhancements:

(01) **Predictable failure prevention: Transferring component responsibilities**

Take system components out of service by transferring component responsibilities to substitute components no later than [Assignment: organization-defined fraction or percentage] of mean time to failure.

Discussion: Transferring primary system component responsibilities to other substitute components prior to primary component failure is important to reduce the risk of degraded or debilitated mission or business functions. Making such transfers based on a percentage of MTTF allows organizations to be proactive based on their risk tolerance. However, the premature replacement of system components can result in the increased cost of system operations.

Related controls and activities: None.

(02) Predictable failure prevention: Time limit on process execution without supervision

Withdrawn: Incorporated into SI-07(16).

(03) Predictable failure prevention: Manual transfer between components

Manually initiate transfers between active and standby system components when the use of the active component reaches [Assignment: organization-defined percentage] of the MTTF.

Discussion: For example, if the MTTF for a system component is 100 days and the MTTF percentage defined by the organization is 90%, the manual transfer would occur after 90 days.

Related controls and activities: None.

(04) Predictable failure prevention: Standby component installation and notification

If system component failures are detected:

- a. ensure that the standby components are successfully and transparently installed within [Assignment: organization-defined time period]
- b. [Selection (1 or more): Activate [Assignment: organization-defined alarm]; Automatically shut down the system; [Assignment: organization-defined action]]

Discussion: Automatic or manual transfer of components from standby to active mode can occur upon the detection of component failures.

Related controls and activities: None.

(05) Predictable failure prevention: Failover capability

Provide [Selection (1): real-time; near real-time] [Assignment: organization-defined failover capability] for the system.

Discussion: Failover refers to the automatic switchover to an alternate system upon the failure of the primary system. Failover capability includes incorporating mirrored system operations at alternate processing sites or periodic data mirroring at regular intervals defined by the recovery time periods of organizations.

Related controls and activities: CP-06, CP-07, CP-09.

References: None.

SI-14 Non-persistence

Control: Implement non-persistent [Assignment: organization-defined system components and services] that are initiated in a known state and terminated [Selection (1 or more): upon end of session of use; periodically at [Assignment: organization-defined frequency]].

Discussion: Implementation of non-persistent components and services mitigates risk from advanced persistent threats (APTs) by reducing the targeting capability of adversaries (i.e., window of opportunity and available attack surface) to initiate and complete attacks. By implementing the concept of non-persistence for selected system components, organizations can provide a trusted, known-state computing resource for a specific time period that does not give adversaries sufficient time to exploit vulnerabilities in organizational systems or operating environments.

Since the APT is a high-end, sophisticated threat with regard to capability, intent, and targeting, organizations assume that, over an extended period, a percentage of attacks will be successful. Non-persistent system components and services are activated as required using protected information and are terminated periodically or at the end of sessions. Non-persistence increases the work factor of adversaries attempting to compromise or breach organizational systems.

Non-persistence can be achieved by refreshing system components, periodically reimaging components, or using a variety of common virtualization techniques. Non-persistent services can be implemented by using virtualization techniques as part of virtual machines or as new instances of processes on physical machines (either persistent or non-persistent).

The benefit of periodic refreshes of system components and services is that it does not require organizations to first determine whether compromises of components or services have occurred (something that may often be difficult to determine). The refresh of selected system components and services occurs with sufficient frequency to prevent the spread or intended impact of attacks, but not with such frequency that it makes the system unstable. Refreshes of critical components and services may be done periodically to hinder the ability of adversaries to exploit optimum windows of vulnerabilities.

Related controls and activities: SC-30, SC-34, SI-21.

Enhancements:

(01) Non-persistence: Refresh from trusted sources

Obtain software and data employed during system component and service refreshes from the following trusted sources: [Assignment: organization-defined trusted sources].

Discussion: Trusted sources include software and data from write-once, read-only media or from selected offline secure storage facilities.

Related controls and activities: None.

(02) Non-persistence: Non-persistent information

- a. [Selection (1): Refresh [Assignment: organization-defined information] [Assignment: organization-defined frequency]; Generate [Assignment: organization-defined information] on demand]
- b. Delete information when no longer needed

Discussion: Retaining information longer than it is needed makes the information a potential target for advanced adversaries searching for high-value assets to compromise through unauthorized disclosure, unauthorized modification, or exfiltration. For system-related information, unnecessary retention provides advanced adversaries with information that can assist in their reconnaissance and lateral movement through the system.

Related controls and activities: None.

(03) Non-persistence: Non-persistent connectivity

Establish connections to the system on demand and terminate connections after [Selection (1): completion of a request; a period of non-use].

Discussion: Persistent connections to systems can provide advanced adversaries with paths to move laterally through systems and potentially position themselves closer to high-value assets. Limiting the availability of such connections impedes the adversary's ability to move freely through organizational systems.

Related controls and activities: SC-10.

References: None.

SI-15 Information output filtering

Control: Validate information output from the following software programs and/or applications to ensure that the information is consistent with the expected content: [Assignment: organization-defined software programs and/or applications].

Discussion: Certain types of attacks, including Structured Query Language (SQL) injections, produce output results that are unexpected or inconsistent with the output results that would be expected from software programs or applications.

Information output filtering focuses on detecting extraneous content, preventing such extraneous content from being displayed, and then alerting monitoring tools that anomalous behaviour has been discovered.

Related controls and activities: SI-03, SI-04, SI-11.

Enhancements: None.

References: None.

SI-16 Memory protection

Control: Implement the following controls to protect the system memory from unauthorized code execution: [Assignment: organization-defined controls].

Discussion: Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Controls employed to protect memory include data execution prevention and address space layout randomization. Data execution prevention controls can either be hardware-enforced or software-enforced, with hardware enforcement providing the greater strength of mechanism.

Related controls and activities: AC-25, SC-03, SI-07.

Enhancements: None.

References: None.

SI-17 Fail-safe procedures

Control: Implement the indicated fail-safe procedures when the indicated failures occur: [Assignment: organization-defined list of failure conditions and associated fail-safe procedures].

Discussion: Failure conditions include the loss of communications among critical system components or between system components and operational facilities. Fail-safe procedures include alerting operator personnel and providing specific instructions on subsequent steps to take. Subsequent steps may include doing nothing, re-establishing system settings, shutting down processes, restarting the system, or contacting designated organizational personnel.

Related controls and activities: CP-12, CP-13, SC-24, SI-13.

Enhancements: None.

References: None.

SI-18 Personal information quality operations

Control:

- A. Ensure the accuracy, relevance, timeliness, and completeness of personal information used for an administrative purpose by the organization across the information lifecycle [Assignment: organization-defined frequency]
- B. Correct or delete inaccurate or outdated personal information

Discussion: Personal information quality operations include the steps that organizations take to confirm the accuracy and relevance of personal information throughout the information lifecycle. The information lifecycle includes the creation, collection, use, handling, storage, maintenance, dissemination, disclosure, and disposal of personal information. Personal information quality operations include editing and validating addresses as they are collected or entered into systems using automated address verification look-up APIs.

Checking personal information quality includes the tracking of updates or changes to data over time, which enables organizations to know how and what personal information was changed should erroneous information be identified. The measures taken to protect personal information quality are based on the nature and context of the personal information, how it is to be used, how it was obtained, and the potential de-identification methods employed.

GC discussion: If the personal information is used or intended to be used as part of an administrative purpose, organizations need to ensure its accuracy. The measures taken to validate the accuracy of personal information used to make determinations about the rights, benefits, or privileges of individuals covered under federal programs may be more comprehensive than the measures used to validate personal information used for less sensitive purposes.

Individuals have the right to request that incorrect information be corrected in government records where they believe there is an error or omission. Organizations must notify the individuals of the correction or notation. Organizations use discretion when determining if personal information is to be corrected or deleted based on the scope of requests, the changes sought, the impact of the changes, and laws, regulations, and policies. Organizational personnel consult with the appropriate privacy senior official or executive and legal counsel regarding appropriate instances of correction or deletion.

Related controls and activities: PM-22, PM-24, PT-02, SI-04.

Enhancements:

(01) **Personal information quality operations: Automation support**

Correct or delete personal information that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified using [Assignment: organization-defined automated mechanisms].

Discussion: The use of automated mechanisms to improve data quality may inadvertently create privacy risks. Automated tools may connect to external or otherwise unrelated systems, and the matching of records between these systems may create linkages with unintended consequences. Organizations assess and document these risks in their PIAs and make determinations that align with their privacy program plans.

As data is obtained and used across the information lifecycle, it is important to confirm the accuracy and relevance of personal information. Automated mechanisms can augment existing data quality processes and procedures and enable an organization to better identify and manage personal information in large-scale systems.

For example, automated tools can greatly improve efforts to consistently normalize data or identify malformed data. Automated tools can also be used to improve the auditing of data and to detect errors that may incorrectly alter personal information or incorrectly associate such information with the wrong individual. Automated capabilities backstop processes and procedures at-scale and enable more fine-grained detection and correction of data quality errors.

Related controls and activities: PM-18, RA-08.

(02) **Personal information quality operations: Data tags**

Employ data tags to automate the correction or deletion of personal information across the information lifecycle within organizational systems.

Discussion: Data tagging personal information includes tags that note handling permissions, authority to collect, de-identification, impact level, information lifecycle stage, and retention or last updated dates. Employing data tags for personal information can support the use of automation tools to correct or delete personal information.

Related controls and activities: AC-03, AC-16, SC-16.

(03) **Personal information quality operations: Collection**

Collect personal information directly from the individual, wherever possible.

Discussion: Individuals or their designated representatives can be sources of correct personal information. Organizations consider contextual factors that may result in individuals providing incorrect personal information. Additional steps may be necessary to validate personal information, depending on how it is to be used, and how it

was obtained. The measures taken to validate the accuracy of personal information used to make determinations about the rights, benefits, or privileges of individuals under federal programs may be more comprehensive than the measures taken to validate less sensitive personal information.

GC discussion: Organizations shall, wherever possible, collect personal information that is intended to be used for an administrative purpose directly from the individual to whom it relates except where the individual authorizes otherwise or where personal information may be disclosed to the institution from another credible source, unless it would result in inaccurate information; or defeat the purpose or prejudice the use for which information is collected.

Related controls and activities: None.

(04) **Personal information quality operations: Individual requests**

Correct or delete personal information upon request by individuals or their designated representatives.

Discussion: Inaccurate personal information maintained by organizations may cause problems for individuals, especially in those business functions where inaccurate information may result in inappropriate decisions or the denial of benefits and services to individuals. Even correct information, in certain circumstances, can cause problems for individuals that outweigh the benefits of an organization maintaining the information. Organizations use discretion when determining if personal information is to be corrected or deleted based on the scope of requests, the changes sought, the impact of the changes, and laws, regulations, and policies. Organizational personnel consult with the appropriate privacy senior official or executive and legal counsel regarding appropriate instances of correction or deletion.

Related controls and activities: None.

(05) **Personal information quality operations: Notice of correction or deletion**

Notify [Assignment: organization-defined recipients of personal information] and individuals that the personal information has been corrected or deleted.

Discussion: When personal information is corrected or deleted, organizations take steps to ensure that all authorized recipients of such information, and the individual with whom the information is associated or their designated representatives, are informed of the corrected or deleted information.

Related controls and activities: None.

References:

- [Privacy Act](#)
- [TBS Policy on Privacy Protection](#)
- [TBS Directive on Privacy Practices](#)
- [TBS Directive on Personal Information Requests and Correction of Personal Information](#)

SI-19 De-identification

Control:

- A. Remove the following elements of personal information from datasets: [Assignment: organization-defined elements of personal information]
- B. Evaluate [Assignment: organization-defined frequency] for effectiveness of de-identification
- AA. Consider the privacy injury if information that may be available in the public enables re-identification of individuals

Discussion: At times, programs may have use for personal information but can achieve their objective without the use of personal identifiers. Where the objective can be achieved without direct identifiers, the information should be de-identified. De-identification is the general term for a process that removes the association between a set of identifying data and the data subject. Its objective is to prevent someone's personal information from being evident in uses or disclosures.

Many datasets contain personal information that can be used to distinguish or trace an individual's identity, such as name, social insurance number, date and place of birth, mother's maiden name, or biometric records. Datasets may also contain other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Disposition (deletion) of personal information is one method of de-identification and should be considered when such information is not (or no longer) necessary to satisfy the requirements envisioned for the data and should be removed from datasets by trained individuals. For example, if the dataset is only used to produce aggregate statistics, the identifiers that are not needed for producing those statistics are removed. Removing identifiers improves privacy protection since information that is removed cannot be inadvertently disclosed or improperly used.

Consideration should be given to the potential privacy injury if some information can enable re-identification of the individual, even without direct identifiers. Organizations may be subject to specific de-identification definitions or methods under applicable laws, regulations, or policies.

Re-identification is a residual risk with de-identified data. Re-identification attacks can vary, including combining new datasets or other improvements in data analytics. Maintaining awareness of potential attacks and evaluating for the effectiveness of the de-identification over time support the management of this residual risk. It is recommended to plan for regular, ongoing, and periodic assessment of re-identification risk by revisiting dissemination strategies and by amending the terms of information sharing agreements, where applicable, as circumstances change.

Related controls and activities: MP-06, PM-22, PM-23, PM-24, RA-02, SI-12.

Enhancements:

(01) De-identification: Collection

De-identify the dataset upon collection by not collecting personal information.

Discussion: If a dataset is being sourced from another program or entity, limit the information sought to only the personal information that is required. For example, if an organization does not intend to use the social insurance number of an applicant, then the social insurance number should not be collected. Organizations should document the collection, use or disclosure of datasets in an information sharing arrangement or agreement.

Related controls and activities: None.

(02) De-identification: Archiving

Prohibit archiving of personal information elements if those elements in a dataset will not be needed after the dataset is archived.

Discussion: Datasets can be archived for many reasons. Unless there is a requirement to retain personal information, datasets should be de-identified prior to archiving. If deletion of the personal information is considered, ensure there is a records disposition standard in place and that deletion of the personal information meets the organization's retention standards.

Related controls and activities: None.

(03) De-identification: Release

Remove personal information elements from a dataset prior to its release if those elements in the dataset do not need to be part of the data release.

Discussion: Prior to releasing a dataset, a data custodian considers the intended uses of the dataset and determines if it is necessary to release personal information. If the personal information is not necessary, the information can be removed using de-identification techniques.

GC discussion: Prior to releasing a dataset, a data custodian considers the intended uses of the dataset and determines the originating program's authority to release, the recipient's authority for collection and document the

use of each personal information data element against the express purpose of the recipient program. If the personal information is not necessary, the information should not be disclosed.

Related controls and activities: None.

(04) **De-identification: Removal, masking, encryption, hashing, or replacement of direct identifiers**

Remove, mask, encrypt, hash, or replace direct identifiers in a dataset.

Discussion: There are many possible processes for removing direct identifiers from a dataset. Columns in a dataset that contain a direct identifier can be removed. In masking, the direct identifier is transformed into a repeating character, such as XXXXXX or 999999. Identifiers can be encrypted or hashed so that the linked records remain linked.

In the case of encryption or hashing, algorithms are employed that require the use of a key, including the Advanced Encryption Standard or a Hash-based Message Authentication Code. Implementations may use the same key for all identifiers or use a different key for each identifier. Using a different key for each identifier provides a higher degree of security and privacy. Identifiers can alternatively be replaced with a keyword, including transforming “William Stephenson” to “PATIENT” or replacing it with a surrogate value, such as transforming “William Stephenson” to “Laura Secord.”

Related controls and activities: SC-12, SC-13.

(05) **De-identification: Statistical disclosure control**

Manipulate numerical data, contingency tables, and statistical findings so that no individual or organization is identifiable in the results of the analysis.

Discussion: Many types of statistical analyses can result in the disclosure of information about individuals even if only summary information is provided. For example, if a school that publishes a monthly table with the number of minority students enrolled, reports that it has 10 to 19 such students in January, and subsequently reports that it has 20 to 29 such students in March, then it can be inferred that the student who enrolled in February was a minority. Care should be taken to review all statistical information that is disclosed to ensure the protection of the individual’s personal information.

Related controls and activities: None.

(06) **De-identification: Differential privacy**

Prevent disclosure of personal information by adding non-deterministic noise to the results of mathematical operations before the results are reported.

Discussion: The mathematical definition for differential privacy holds that the result of a dataset analysis should be approximately the same before and after the addition or removal of a single data record (which is assumed to be the data from a single individual).

In its most basic form, differential privacy applies only to online query systems. However, it can also be used to produce machine-learning statistical classifiers and synthetic data. Differential privacy comes at the cost of decreased accuracy of results, forcing organizations to quantify the trade-off between privacy protection and the overall accuracy, usefulness, and utility of the de-identified dataset. Non-deterministic noise can include adding small, random values to the results of mathematical operations in dataset analysis.

Related controls and activities: SC-12, SC-13.

(07) **De-identification: Validated algorithms and software**

Perform de-identification using validated algorithms and software that is validated to implement the algorithms.

Discussion: Algorithms that appear to remove personal information from a dataset may in fact leave information that is personally identifiable or data that is re-identifiable. Software that is claimed to implement a validated

algorithm may contain bugs or implement a different algorithm. Software may de-identify one type of data, such as integers, but not de-identify another type of data, such as floating-point numbers. For these reasons, de-identification is performed using algorithms and software that are validated.

Related controls and activities: None.

(08) **De-identification: Motivated intruder**

Perform a motivated intruder test on the de-identified dataset to determine if the identified data remains or if the de-identified data can be re-identified.

Discussion: A motivated intruder test is a test in which an individual or group takes a data release and specified resources and attempts to re-identify one or more individuals in the de-identified dataset. Such tests specify the amount of inside knowledge, computational resources, financial resources, data, and skills that intruders possess to conduct the tests. A motivated intruder test can determine if the de-identification is insufficient. It can also be a useful diagnostic tool to assess if de-identification is likely to be sufficient. However, the test alone cannot prove that de-identification is sufficient.

Related controls and activities: None.

References:

- [Privacy Act](#)
- [Privacy Regulations SOR/83-508](#)
- [TBS Policy on Privacy Protection](#)
- [TBS Directive on Privacy Practices](#)
- [TBS Privacy Implementation Notice 2023-01: De-identification](#)
- [NIST SP 800-188 De-Identifying Government Datasets: Techniques and Governance](#)

SI-20 Tainting

Control: Embed data or capabilities in the following systems or system components to determine if organizational data has been exfiltrated or improperly removed from the organization: [Assignment: organization-defined systems or system components].

Discussion: Many cyber-attacks target organizational information, or information that the organization holds on behalf of other entities (e.g., personal information), and exfiltrate that data. In addition, insider attacks and erroneous user procedures can remove information from the system that is in violation of the organizational policies. Tainting approaches can range from passive to active. A passive tainting approach can be as simple as adding false email names and addresses to an internal database. If the organization receives an email at one of the false email addresses, it knows that the database has been compromised. Moreover, the organization knows that the email was sent by an unauthorized entity, so any packets it includes potentially contain malicious code, and that the unauthorized entity may have potentially obtained a copy of the database.

Another tainting approach can include embedding false data or steganographic data in files to enable the data to be found via open-source analysis. Finally, an active tainting approach can include embedding software in the data that is able to “call home,” thereby alerting the organization to its “capture,” and possibly its location, and the path by which it was exfiltrated or removed.

Related controls and activities: AU-13.

Enhancements: None.

References: [TBS Policy on Privacy Protection](#)

SI-21 Information refresh

Control: Refresh [Assignment: organization-defined information] at [Assignment: organization-defined frequencies] or generate the information on demand and delete the information when no longer needed.

Discussion: Retaining information for longer than it is needed makes the information an increasingly valuable and enticing target for adversaries. Keeping information available for the minimum period of time needed to support organizational missions or business functions reduces the opportunity for adversaries to compromise, capture, and exfiltrate that information.

Related controls and activities: SI-14.

Enhancements: None.

References:

- [TBS Policy on Privacy Protection](#)
- [TBS Directive on Privacy Practices](#)

SI-22 Information diversity

Control:

- A. Identify the following alternative sources of information for [Assignment: organization-defined essential functions and services]: [Assignment: organization-defined alternative information sources]
- B. Use an alternative information source for the execution of essential functions or services on [Assignment: organization-defined systems or system components] when the primary source of information is corrupted or unavailable

Discussion: Actions taken by a system service or a function are often driven by the information it receives. Corruption, fabrication, modification, or deletion of that information could impact the ability of the service function to properly carry out its intended actions. By having multiple sources of input, the service or function can continue operation if one source is corrupted or no longer available. It is possible that the alternative sources of information may be less precise or less accurate than the primary source of information. But having such sub-optimal information sources may still provide a sufficient level of quality that the essential service or function can be carried out, even in a degraded or debilitated manner.

Related controls and activities: None.

Enhancements: None.

References: None.

SI-23 Information fragmentation

Control: Based on [Assignment: organization-defined circumstances]:

- A. fragment the following information: [Assignment: organization-defined information]
- B. distribute the fragmented information across the following systems or system components: [Assignment: organization-defined systems or system components]

Discussion: One objective of the advanced persistent threat is to exfiltrate valuable information. Once exfiltrated, there is generally no way for the organization to recover the lost information. Therefore, organizations may consider dividing the information into disparate elements and distributing those elements across multiple systems or system components and locations. Such actions will increase the adversary's work factor to capture and exfiltrate the desired information and, in so

doing, increase the probability of detection. The fragmentation of information impacts the organization's ability to access the information in a timely manner. The extent of the fragmentation is dictated by the impact or classification level (and value) of the information, threat intelligence information received, and whether data tainting is used (i.e., data tainting-derived information about the exfiltration of some information could result in the fragmentation of the remaining information).

Related controls and activities: None.

Enhancements: None.

References: None.

SI-400 Dedicated administration workstation

Control: Require any administrative or superuser actions to be performed from a physical workstation that is dedicated to those specific tasks and isolated from all other functions and networks, and especially from any form of Internet access.

Discussion: A dedicated administration workstation (DAW) is typically comprised of a user terminal with a very small selection of software designed for interfacing with the target system. For the purpose of this control, workstation means the system from which you are performing the administration, as opposed to the target system of administration.

The DAW must be hardened for the role, to minimize the likelihood that a superuser's or administrator's endpoint may be compromised by any threat actor (which would logically lead to the compromise of the target system). Typical office productivity tools are not required on the DAW. All non-essential applications and services are removed. DAWs are not domain-joined, cannot download patches from the Internet, and cannot update documentation in networked applications.

Jump servers do not replace the requirement for DAWs. Connections through a jump server must be done from a DAW. Jump servers are used to centralize the logging of administrative activities, simplify the network isolation of critical servers, and provide a common handover point for administrators with separation of duties (e.g., where software patches are staged by one administrator for installation by another administrator).

If a VPN is being used to provide the network connectivity, the VPN must automatically exclude all other network access excepting the VPN. The DAW must not be able to access networks other than the network it is administering. The management interface of the target system must be restricted to a management network and must not be accessible to wider networks such as corporate workstation LANs or the Internet. If multiple target networks are administered by the same physical DAW, all networks must have the same security profile (e.g., a single DAW cannot administer both a network for Secret and a network for Protected B).

Virtual terminal software that emulates a simple terminal should also reside on a DAW.

Related controls and activities: AC-04(22), AC-17(400), CM-07, MA-04, SA-08, SC-02, SC-07, SC-08, SC-32.

Enhancements:

(01) Dedicated administration workstation: Thin client dedicated administration workstation

Implement virtualized DAW inside network-isolated physical thin client DAW.

Discussion: Administrators who have numerous infrastructures to manage may choose to have a physical thin client DAW which can run multiple virtualized DAWs for different networks.

The thin client may be employed in a virtual desktop infrastructure (VDI) fashion, where the physical DAW is the hypervisor host for a virtual DAW, or in a network booted thin client fashion, where the operating system of the thin client is loaded from the network to be administered.

The physical thin client must not have independent network access.

Related controls and activities: SA-08, SC-25.

(02) Dedicated administration workstation: VPN on carrier private network

Connect a DAW to a target network using carrier private networks (e.g., virtual private LAN service (VPLS) or multiprotocol label switching (MPLS)) with VPN encryption.

Discussion: When administering a network from a remote location, Internet-addressable VPN gateways and VPN endpoints are vulnerable to attacks by public network-based threat actors. Moving to a carrier private network will eliminate public Internet vulnerabilities and reduces the number of threat actors of concern. However, the network may still be vulnerable to confidentiality or integrity attacks from inside the carrier network. Hence, a VPN is still required inside the carrier network.

Related controls and activities: SC-08.

(03) **Dedicated administration workstation: Local area network**

Connect a DAW to a target network using only LAN.

Discussion: To further decrease the likelihood of a network attack, attach a DAW to the target system using only LAN. The target system can then deny administrative access except on the local segment.

Related controls and activities: SA-08.

(04) **Dedicated administration workstation: Console access only**

Connect a DAW to the target system using only direct console ports.

Discussion: To eliminate the likelihood of a network attack, connect a DAW to the target system directly through local serial ports. The system can then deny administrative access to all networks.

Related controls and activities: SA-08.

(05) **Dedicated administration workstation: Dedicated physical workstation**

Use a single-purpose physical workstation as the DAW.

Discussion: To reduce the possibility of attacks moving laterally between networks being administered, use a physical workstation for each target network, without sharing DAW resources.

Related controls and activities: SA-08.

(06) **Dedicated administration workstation: Heterogeneous administrative access**

Use a different operating system for the DAW relative to the target system.

Discussion: A vulnerability in either a DAW or the target system might be shared between the 2, providing a single attack route for both. If the DAW and target systems have different operating systems, it will require additional effort to compromise both.

Related controls and activities: SC-29.

References: None.

Family: Supply chain risk management

The controls in the Supply chain risk management (SR) family support the mitigation of cyber security risks within the supply chain at all levels of an organization.

SR-01 Supply chain risk management policy and procedures

Activity:

- A. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]
 - 1. [Selection (1 or more): Organization-level; Mission/business process-level; System-level] supply chain risk management (SCRM) policy that
 - a. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
 - b. is consistent with applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines
 - 2. procedures to facilitate the implementation of the SCRM policy and the associated SCRM controls
- B. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the SCRM policy and procedures
- C. Review and update the current SCRM
 - 1. policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]
 - 2. procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]

Discussion: SCRM policy and procedures address the controls in the SR family, as well as supply chain-related controls in other families, that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of SCRM policy and procedures.

In general, security and privacy program policies and procedures at the organization level are preferable and may remove the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations.

Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents.

Events that may precipitate an update to SCRM policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, Orders in Council, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related controls and activities: PM-09, PM-30, PS-08, SI-02, SI-12.

Enhancements: None.

References:

- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)

- [CSE-RCMP Harmonized Threat and Risk Assessment Methodology \(TRA-1\)](#)
- [TBS Guide to Integrated Risk Management](#)
- [Protecting your organization from software supply chain threats \(ITSM.10.071\)](#)
- [Cyber supply chain: An approach to assessing risk \(ITSAP.10.070\)](#)
- [Supply chain security for small and medium-sized organizations \(ITSAP.00.070\)](#)
- [Public Safety Canada Risk Management Guide for Critical Infrastructure Sectors](#)

SR-02 Supply chain risk management plan

Activity:

- Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: [Assignment: organization-defined systems, system components, or system services]
- Review and update the SCRM plan [Assignment: organization-defined frequency] or as required, to address threat, organizational or environmental changes
- Protect the SCRM plan from unauthorized disclosure and modification

Discussion: The dependence on products, systems, and services from external providers, as well as the nature of the relationships with those providers, present an increasing level of risk to an organization. Threat actions that may increase security or privacy risks include unauthorized production, the insertion or use of counterfeits, tampering, theft, insertion of malicious software and hardware, and poor manufacturing and development practices in the supply chain.

Supply chain risks can be endemic or systemic within a system element or component, a system, an organization, a sector, or Canada. Managing supply chain risk is a complex, multifaceted undertaking that requires a coordinated effort across an organization to build trust relationships and communicate with internal and external stakeholders.

SCRM activities include identifying and assessing risks, determining appropriate risk response actions, developing SCRM plans to document response actions, and monitoring performance against plans. The SCRM plan (at the system level) is implementation-specific and provides policy implementation, requirements, constraints, and implications. It can either be standalone or incorporated into system security and privacy plans. The SCRM plan addresses managing, implementing, and monitoring SCRM controls and the development/sustainment of systems across the software development lifecycle (SDLC) to support mission and business functions.

Because supply chains can differ significantly across and within organizations, SCRM plans are tailored to the individual program, organizational, and operational contexts. Tailored SCRM plans provide the basis for determining whether a technology, service, system component, or system is fit for purpose and, as such, the controls need to be tailored accordingly.

Tailored SCRM plans help organizations focus their resources on the most critical mission and business functions based on mission and business requirements and their risk environment. SCRM plans include an expression of the supply chain risk tolerance for the organization, acceptable supply chain risk mitigation strategies or controls, a process for consistently evaluating and monitoring supply chain risk, approaches for implementing and communicating the plan, a description of and justification for supply chain risk mitigation measures taken, and associated roles and responsibilities.

Finally, SCRM plans address requirements for developing trustworthy, secure, privacy-protective, and resilient system components and systems, including the application of the security design principles implemented as part of lifecycle-based systems security engineering processes (see SA-08).

Related controls and activities: CA-02, CP-04, IR-04, MA-02, MA-06, PE-16, PL-02, PM-09, PM-30, RA-03, RA-07, SA-08, SI-04.

Enhancements:

(01) Supply chain risk management plan: Establish a SCRM team

Establish a SCRM team consisting of [Assignment: organization-defined personnel, roles, and responsibilities] to lead and support the following SCRM activities: [Assignment: organization-defined SCRM activities].

Discussion: To implement SCRM plans, organizations should establish a coordinated, team-based approach to identify and assess supply chain risks and manage these risks by using programmatic and technical mitigation techniques. The team approach enables organizations to conduct an analysis of their supply chain, communicate with internal and external partners or stakeholders, and gain broad consensus regarding the appropriate resources for SCRM.

The SCRM team consists of organizational personnel with diverse roles and responsibilities for leading and supporting SCRM activities, including risk executive, IT, contracting, information security, privacy, mission or business, legal, supply chain and logistics, acquisition, business continuity, and other relevant functions. Members of the SCRM team are involved in various aspects of the SDLC and, collectively, have an awareness of and provide expertise in acquisition processes, legal practices, vulnerabilities, threats, and attack vectors, as well as an understanding of the technical aspects and dependencies of systems.

The SCRM team can be an extension of the security and privacy risk management processes or can be included as part of an organizational risk management team.

Related controls and activities: None.

References:

- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [TBS Directive on Security Management: Appendix F: Mandatory Procedures for Security in Contracts and Other Arrangements Control](#)
- [Protecting your organization from software supply chain threats \(ITSM.10.071\)](#)

SR-03 Supply chain controls and processes

Control:

- Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of [Assignment: organization-defined system or system component] in coordination with [Assignment: organization-defined supply chain personnel]
- Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events: [Assignment: organization-defined supply chain controls]
- Document the selected and implemented supply chain processes and controls in [Selection (1): security and privacy plans; SCRM plan; [Assignment: organization-defined document]]

Discussion: Supply chain elements include organizations, entities, or tools employed for the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of systems and system components. Supply chain processes include hardware, software, and firmware development processes; shipping and handling procedures; personnel security and physical security programs; configuration management tools, techniques, and measures to maintain provenance; or other programs, processes, or procedures associated with the development, acquisition, maintenance and disposal of systems and system components.

Supply chain elements and processes may be provided by organizations, system integrators, or external providers. Weaknesses or deficiencies in supply chain elements or processes represent potential vulnerabilities that can be exploited

by adversaries to cause harm to the organization and affect its ability to carry out its core missions or business functions. Supply chain personnel are individuals with roles and responsibilities in the supply chain.

Related controls and activities: CA-02, MA-02, MA-06, PE-03, PE-16, PL-08, PM-30, SA-02, SA-03, SA-04, SA-05, SA-08, SA-09, SA-10, SA-15, SC-07, SC-29, SC-30, SC-38, SI-07, SR-06, SR-09, SR-11.

Enhancements:

(01) Supply chain controls and processes: Diverse supply base

Employ a diverse set of sources for the following system components and services: [Assignment: organization-defined system components and services].

Discussion: Diversifying the supply of systems, system components, and services can reduce the probability that adversaries will successfully identify and target the supply chain and can reduce the impact of a supply chain event or compromise. Identifying multiple suppliers for replacement components can reduce the probability that the replacement component will become unavailable. Employing a diverse set of developers or logistics service providers can reduce the impact of a natural disaster or other supply chain event. Organizations should consider designing the system to include diverse materials and components.

Related controls and activities: None.

(02) Supply chain controls and processes: Limitation of harm

Employ the following controls to limit harm from potential adversaries identifying and targeting the organizational supply chain: [Assignment: organization-defined controls].

Discussion: Controls that can be implemented to reduce the probability of adversaries successfully identifying and targeting the supply chain include avoiding the purchase of custom or non-standardized configurations, employing approved vendor lists with standing reputations in industry, following pre-agreed maintenance schedules and update and patch delivery mechanisms, maintaining a contingency plan in case of a supply chain event, using procurement carve-outs that provide exclusions to commitments or obligations, using diverse delivery routes, and minimizing the time between purchase decisions and delivery.

Related controls and activities: None.

(03) Supply chain controls and processes: Sub-tier flow-down

Ensure that the controls included in the contracts of prime contractors are also included in the contracts of subcontractors.

Discussion: To manage supply chain risk effectively and holistically, it is important that organizations ensure that SCRM controls are included at all tiers in the supply chain. This includes ensuring that prime contractors have implemented processes to facilitate the flow-down of SCRM controls to subcontractors. The controls subject to flow-down are identified in SR-03B.

Related controls and activities: SR-05, SR-08.

References:

- [Protecting your organization from software supply chain threats \(ITSM.10.071\)](#)
- [Cyber supply chain: An approach to assessing risk \(ITSAP.10.070\)](#)
- [Public Safety Canada Risk Management Guide for Critical Infrastructure Sectors](#)
- [PSPC Contract Security Manual](#)
- [ISO 20243-1 Information technology – Open Trusted Technology Provider™ Standard \(O-TTPS\)–Part 1: Requirements and recommendations for mitigating maliciously tainted and counterfeit products](#)

SR-04 Provenance

Control: Document, monitor, and maintain valid provenance of the following systems, system components, and associated data: [Assignment: organization-defined systems, system components, and associated data].

Discussion: Every system and system component has a point of origin and may be changed throughout their existence. Provenance is the chronology of the origin, development, ownership, location, and changes to a system or system component and associated data. It may also include personnel and processes used to interact with or make modifications to the system, component, or associated data.

Organizations should consider developing procedures (see SR-01) for allocating responsibilities for the creation, maintenance, and monitoring of provenance for systems and system components; transferring provenance documentation and responsibility between organizations; and preventing and monitoring for unauthorized changes to the provenance records. Organizations should have methods to document, monitor, and maintain valid provenance baselines for systems, system components, and related data.

These actions help track, assess, and document any changes to the provenance, including changes in supply chain elements or configuration, and help ensure non-repudiation of provenance information and the provenance change records. Provenance considerations are addressed throughout the system development lifecycle and incorporated into contracts and other arrangements, as appropriate.

Related controls and activities: CM-08, MA-02, MA-06, RA-09, SA-03, SA-08, SI-04.

Enhancements:

(01) Provenance: Identity

Establish and maintain unique identification of the following supply chain elements, processes, and personnel associated with the identified system and critical system components: [Assignment: organization-defined supply chain elements, processes, and personnel associated with organization-defined systems and critical system components].

Discussion: Knowing who and what is in the supply chains of organizations is critical to gaining visibility into supply chain activities. Visibility into supply chain activities is also important for monitoring and identifying high-risk events and activities. Without reasonable visibility into supply chain elements, processes, and personnel, it is very difficult for organizations to understand and manage risk and reduce their susceptibility to adverse events.

Supply chain elements include organizations, entities, or tools used for the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of systems and system components. Supply chain processes include development processes for hardware, software, and firmware; shipping and handling procedures; configuration management tools, techniques, and measures to maintain provenance; personnel and physical security programs; or other programs, processes, or procedures associated with the production and distribution of supply chain elements.

Supply chain personnel are individuals with specific roles and responsibilities related to the secure the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of a system or system component. Identification methods are sufficient to support an investigation in case of a supply chain change (e.g., if a supply company is purchased), compromise, or event.

Related controls and activities: IA-02, IA-08, PE-16.

(02) Provenance: Track and trace

Establish and maintain unique identification of the following systems and critical system components for tracking through the supply chain: [Assignment: organization-defined systems and critical system components].

Discussion: Tracking the unique identification of systems and system components during development and transport activities provides a foundational identity structure for establishing and maintaining of provenance. For example, system components may be labelled using serial numbers or tagged using radio-frequency identification

tags. Labels and tags can help provide better visibility into the provenance of a system or system component. A system or system component may have more than one unique identifier. Identification methods are sufficient to support a forensic investigation after a supply chain compromise or event.

Related controls and activities: IA-02, IA-08, PE-16, PL-02.

(03) **Provenance: Validate as genuine and not altered**

Employ the following controls to validate that the system or system component received is genuine and has not been altered: [Assignment: organization-defined controls].

Discussion: For many systems and system components, especially hardware, there are technical means to determine if the items are genuine or have been altered, including optical and nanotechnology tagging, physically unclonable functions, side-channel analysis, cryptographic hash verifications or digital signatures, and visible anti-tamper labels or stickers. Controls can also include monitoring for out-of-specification performance, which can be an indicator of tampering or counterfeits.

Organizations may leverage supplier and contractor processes for validating that a system or component is genuine and has not been altered and for replacing a suspect system or component. Some indications of tampering may be visible and addressable before accepting delivery, such as inconsistent packaging, broken seals, and incorrect labels. When a system or system component is suspected of being altered or counterfeit, the supplier, contractor, or original equipment manufacturer may be able to replace the item or provide a forensic capability to determine the origin of the counterfeit or altered item. Organizations can provide training to personnel on how to identify suspicious system or component deliveries.

Related controls and activities: AT-03, SR-09, SR-10, SR-11.

(04) **Provenance: Supply chain integrity – pedigree**

Employ [Assignment: organization-defined controls] and conduct [Assignment: organization-defined analysis] to ensure the integrity of the system and system components by validating the internal composition and provenance of critical or mission-essential technologies, products, and services.

Discussion: Authoritative information regarding the internal composition of system components and the provenance of technology, products, and services provides a strong basis for trust. The validation of the internal composition and provenance of technologies, products, and services is referred to as the pedigree. For microelectronics, this includes material composition of components. For software, this includes the composition of open-source and proprietary code, including the version of the component at a given point in time.

Pedigrees increase the assurance that the claims suppliers assert about the internal composition and provenance of the products, services, and technologies they provide are valid. The validation of the internal composition and provenance can be achieved by various evidentiary artifacts or records that manufacturers and suppliers produce during the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of technology, products, and services.

Evidentiary artifacts include, but are not limited to, software identification (SWID) tags, software component inventory, the manufacturers' declarations of platform attributes (e.g., serial numbers, hardware component inventory), and measurements (e.g., firmware hashes) that are tightly bound to the hardware itself.

Related controls and activities: RA-03.

References:

- [Protecting your organization from software supply chain threats \(ITSM.10.071\)](#)
- [ISO 27036-1 Cybersecurity – Supplier relationships–Part 1: Overview and concepts](#)
- [ISO 27036-2 Cybersecurity – Supplier relationships–Part 2: Requirements](#)
- [ISO 20243-1 Information technology – Open Trusted Technology Provider™ Standard \(O-TTPS\)–Part 1: Requirements and recommendations for mitigating maliciously tainted and counterfeit products](#)

- [Cyber supply chain: An approach to assessing risk \(ITSAP.10.070\)](#)
- [Public Safety Canada Risk Management Guide for Critical Infrastructure Sectors](#)

SR-05 Acquisition strategies, tools, and methods

Control: Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: [Assignment: organization-defined acquisition strategies, contract tools, and procurement methods].

Discussion: Using an acquisition process provides an important vehicle to protect the supply chain. There are many useful tools and techniques available, including obscuring the end use of a system or system component, using blind or filtered buys, requiring tamper-evident packaging, or using trusted or controlled distribution. The results from a supply chain risk assessment can guide and inform the strategies, tools, and methods that are most applicable to the situation.

Tools and techniques may provide protection against unauthorized production, theft, tampering, insertion of counterfeits, insertion of malicious software or backdoors, and poor development practices throughout the system development lifecycle. Organizations should also consider providing incentives for suppliers who implement controls, promote transparency into their processes and security and privacy practices, provide contract language that addresses the prohibition of tainted or counterfeit components, and restrict purchases from untrustworthy suppliers.

Organizations should consider providing training, education, and awareness programs for personnel regarding supply chain risk, available mitigation strategies, and when the programs should be employed. Methods for reviewing and protecting development plans, documentation, and evidence are commensurate with the security and privacy requirements of the organization. Contracts may specify documentation protection requirements.

Related controls and activities: AT-03, SA-02, SA-03, SA-04, SA-05, SA-08, SA-09, SA-10, SA-15, SR-06, SR-09, SR-10, SR-11.

Enhancements:

(01) Acquisition strategies, tools, and methods: Adequate supply

Employ the following controls to ensure an adequate supply of [Assignment: organization-defined critical system components]: [Assignment: organization-defined controls].

Discussion: Adversaries can attempt to impede organizational operations by disrupting the supply of critical system components or corrupting supplier operations. Organizations may track systems and component mean time to failure to mitigate the loss of temporary or permanent system function. Controls to ensure that adequate supplies of critical system components include using multiple suppliers throughout the supply chain for the identified critical components, stockpiling spare components to ensure operation during mission-critical times, and identifying functionally identical or similar components that may be used, if necessary.

Related controls and activities: RA-09.

(02) Acquisition strategies, tools, and methods: Assessments prior to selection, acceptance, modification, or update

Assess the system, system component, or system service prior to selection, acceptance, modification, or update.

Discussion: Organizational personnel or independent, external entities should conduct assessments of systems, components, products, tools, and services to uncover evidence of tampering, unintentional and intentional vulnerabilities, or evidence of non-compliance with supply chain controls. These include malicious code, malicious processes, defective software, backdoors, and counterfeits.

Assessments can include evaluations; design proposal reviews; visual or physical inspections; static and dynamic analyses; visual, x-ray, or magnetic particle inspections; simulations; white-, grey-, or black-box testing; fuzz testing; stress testing; and penetration testing (see SR-06(01)). Evidence generated during assessments should be documented for follow-on actions by organizations.

The evidence generated during the organizational or independent assessments of supply chain elements may be used to improve supply chain processes and inform the SCRM process. The evidence can be leveraged in follow-on assessments. Evidence and other documentation may be shared in accordance with organizational agreements.

Related controls and activities: CA-08, RA-05, SA-11, SI-07.

References:

- [TBS Directive on Security Management: Appendix B: Mandatory Procedures for Information Technology Security Control](#)
- [TBS Directive on Security Management: Appendix F: Mandatory Procedures for Security in Contracts and Other Arrangements Control](#)
- [Protecting your organization from software supply chain threats \(ITSM.10.071\)](#)
- [PSPC Contract Security Manual](#)
- [ISO 27036-1 Cybersecurity – Supplier relationships–Part 1: Overview and concepts](#)
- [ISO 27036-2 Cybersecurity – Supplier relationships–Part 2: Requirements](#)
- [ISO 20243-1 Information technology – Open Trusted Technology Provider™ Standard \(O-TTPS\)–Part 1: Requirements and recommendations for mitigating maliciously tainted and counterfeit products](#)

SR-06 Supplier assessments and reviews

Control: Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide [Assignment: organization-defined frequency].

Discussion: An assessment and review of supplier risk includes security and SCRM processes, foreign ownership, control, or influence (FOCI), and the ability of the supplier to effectively assess subordinate second-tier and third-tier suppliers and contractors. The reviews may be conducted by the organization or by an independent third party. The reviews should consider documented processes, documented controls, all-source intelligence, and publicly available information related to the supplier or contractor.

Organizations can use open-source information to monitor for indications of stolen information, poor development and quality control practices, information spillage, or counterfeits. In some cases, it may be appropriate or required to share assessment and review results with other organizations in accordance with any applicable rules, policies, or inter-organizational agreements or contracts.

Related controls and activities: SR-03, SR-05.

Enhancements:

(01) Supplier assessments and reviews: Testing and analysis

Employ [Selection (1 or more): organizational analysis; independent third-party analysis; organizational testing; independent third-party testing] of the following supply chain elements, processes, and actors associated with the system, system component, or system service: [Assignment: organization-defined supply chain elements, processes, and actors].

Discussion: Relationships between entities and procedures within the supply chain, including development and delivery, are considered. Supply chain elements include organizations, entities, or tools that are used for the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of systems, system components, or system services.

Supply chain processes include SCRM programs; SCRM strategies and implementation plans; personnel and physical security programs; hardware, software, and firmware development processes; configuration management tools, techniques, and measures to maintain provenance; shipping and handling procedures; and programs, processes, or procedures associated with the production and distribution of supply chain elements.

Supply chain actors are individuals with specific roles and responsibilities in the supply chain. The evidence generated and collected during analyses and testing of supply chain elements, processes, and actors is documented and used to inform organizational risk management activities and decisions.

Related controls and activities: CA-08, SI-04.

References:

- [TBS Directive on Security Management: Appendix F: Mandatory Procedures for Security in Contracts and Other Arrangements Control](#)
- [Protecting your organization from software supply chain threats \(ITSM.10.071\)](#)
- [Cyber supply chain: An approach to assessing risk \(ITSAP.10.070\)](#)
- [ISO 27036-1 Cybersecurity – Supplier relationships–Part 1: Overview and concepts](#)
- [ISO 27036-2 Cybersecurity – Supplier relationships–Part 2: Requirements](#)
- [ISO 20243-1 Information technology – Open Trusted Technology Provider™ Standard \(O-TTPS\)–Part 1: Requirements and recommendations for mitigating maliciously tainted and counterfeit products](#)
- [NIST FIPS 140-3 Security Requirements for Cryptographic Modules](#)
- [NIST FIPS 186-5 Digital Signature Standard \(DSS\)](#)
- [NIST FIPS 202 SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions](#)

SR-07 Supply chain operations security

Control: Employ the following OPSEC controls to protect supply chain-related information for the system, system component, or system service: [Assignment: organization-defined OPSEC controls].

Discussion: Supply chain OPSEC expands the scope of OPSEC to include suppliers and potential suppliers. OPSEC is a process that includes identifying critical information; analyzing friendly actions related to operations and other activities to identify actions that can be observed by potential adversaries; determining indicators that potential adversaries might obtain that could be interpreted or pieced together to derive information in sufficient time to cause harm to organizations; implementing safeguards or countermeasures to eliminate or reduce exploitable vulnerabilities and risk to an acceptable level; and considering how aggregated information may expose users or specific uses of the supply chain.

Supply chain information includes user identities; uses for systems, system components, and system services; supplier identities; security and privacy requirements; system and component configurations; supplier processes; design specifications; and testing and evaluation results.

Supply chain OPSEC may require organizations to withhold mission or business information from suppliers and may include the use of intermediaries to hide the end use or users of systems, system components, or system services.

Related controls and activities: SC-38.

Enhancements: None.

References:

- [Protecting your organization from software supply chain threats \(ITSM.10.071\)](#)
- [ISO 27036-1 Cybersecurity – Supplier relationships–Part 1: Overview and concepts](#)
- [ISO 27036-2 Cybersecurity – Supplier relationships–Part 2: Requirements](#)

SR-08 Notification agreements

Control: Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the [Selection (1 or more): notification of supply chain compromises; results of assessments or audits; [Assignment: organization-defined information]].

Discussion: The establishment of agreements and procedures facilitates communication among supply chain entities. Early notification of compromises and potential compromises in the supply chain that can potentially adversely affect or have adversely affected organizational systems or system components is essential for organizations to effectively respond to such incidents. The results of assessments or audits may include open-source information that contributed to a decision or result and could be used to help the supply chain entity resolve a concern or improve its processes.

Related controls and activities: IR-04, IR-06, IR-08, SI-02.

Enhancements: None.

References:

- [Protecting your organization from software supply chain threats \(ITSM.10.071\)](#)
- [ISO 27036-1 Cybersecurity – Supplier relationships–Part 1: Overview and concepts](#)
- [ISO 27036-2 Cybersecurity – Supplier relationships–Part 2: Requirements](#)

SR-09 Tamper resistance and detection

Control: Implement a tamper protection program for the system, system component, or system service.

Discussion: Anti-tamper technologies, tools, and techniques provide a level of protection for systems, system components, and services against many threats, including reverse engineering, modification, and substitution. Strong identification combined with tamper resistance and/or tamper detection is essential to protecting systems and components during distribution and when in use.

Related controls and activities: PE-03, PM-30, SA-15, SI-04, SI-07, SR-03, SR-04, SR-05, SR-10, SR-11.

Enhancements:

(01) Tamper resistance and detection: Multiple stages of system development lifecycle

Employ anti-tamper technologies, tools, and techniques throughout the system development lifecycle.

Discussion: The system development lifecycle includes research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal. Organizations should use a combination of hardware and software techniques for tamper resistance and detection. Organizations should use obfuscation and self-checking to make reverse engineering and modifications more difficult, time-consuming, and expensive for adversaries. The customization of systems and system components can make substitutions easier to detect and therefore limit damage.

Related controls and activities: SA-03.

References: [ISO 20243-1 Information technology – Open Trusted Technology Provider™ Standard \(O-TTPS\)–Part 1: Requirements and recommendations for mitigating maliciously tainted and counterfeit products](#)

SR-10 Inspection of systems or components

Control: Inspect the following systems or system components [Selection (1 or more): at random; at [Assignment: organization-defined frequency]], upon [Assignment: organization-defined indications of need for inspection]] to detect tampering: [Assignment: organization-defined systems or system components].

Discussion: The inspection of systems or systems components for tamper resistance and detection addresses physical and logical tampering and is applied to systems and system components removed from organization-controlled areas. Indications of a need for inspection include changes in packaging, specifications, factory location, or entity in which the part is purchased, and when individuals return from travel to high-risk locations.

Related controls and activities: AT-03, PM-30, SI-04, SI-07, SR-03, SR-04, SR-05, SR-09, SR-11.

Enhancements: None.

References: [ISO 20243-1 Information technology – Open Trusted Technology Provider™ Standard \(O-TTPS\)–Part 1: Requirements and recommendations for mitigating maliciously tainted and counterfeit products](#)

SR-11 Component authenticity

Control:

- A. Develop and implement anti-counterfeiting policy and procedures that include the means to detect and prevent counterfeit components from entering the system
- B. Report counterfeit system components to [Selection (1 or more): source of counterfeit component; [Assignment: organization-defined external reporting organizations]; [Assignment: organization-defined personnel or roles]]

Discussion: Sources of counterfeit components include manufacturers, developers, vendors, and contractors. Anti-counterfeiting policies and procedures support tamper resistance and provide a level of protection against the introduction of malicious code. External reporting organizations include the Cyber Centre.

Related controls and activities: PE-03, SA-04, SI-07, SR-09, SR-10.

Enhancements:

(01) Component authenticity: Anti-counterfeit training

Train [Assignment: organization-defined personnel or roles] to detect counterfeit system components (including hardware, software, and firmware).

Discussion: None.

Related controls and activities: AT-03.

(02) Component authenticity: Configuration control for component service and repair

Maintain configuration control over the following system components awaiting service or repair and over serviced or repaired components awaiting return to service: [Assignment: organization-defined system components].

Discussion: None.

Related controls and activities: CM-03, MA-02, MA-04, SA-10.

(03) Component authenticity: Anti-counterfeit scanning

Scan for counterfeit system components [Assignment: organization-defined frequency].

Discussion: The type of component determines the type of scanning to be conducted (e.g., web application scanning if the component is a web application).

Related controls and activities: RA-05.

References: [ISO 20243-1 Information technology – Open Trusted Technology Provider™ Standard \(O-TTPS\)–Part 1: Requirements and recommendations for mitigating maliciously tainted and counterfeit products](#)

SR-12 Component disposal

Control: Dispose of [Assignment: organization-defined data, documentation, tools, or system components] using the following techniques and methods: [Assignment: organization-defined techniques and methods].

Discussion: Data, documentation, tools, or system components can be disposed of at any time during the system development lifecycle (not only in the disposal or retirement phase of the lifecycle). For example, disposal can occur during

research and development, design, prototyping, or operations/maintenance and can include methods such as disk cleaning, removal of cryptographic keys, and partial reuse of components.

Opportunities for compromise during disposal affect physical and logical data, including system documentation in paper-based or digital files; shipping and delivery documentation; memory sticks with software code; or complete routers or servers that include permanent media, which contain sensitive or proprietary information. Additionally, proper disposal of system components helps prevent such components from entering the grey market.

Related controls and activities: MP-06.

Enhancements: None.

References: None.

Works Cited

Lampson, B. W. (1973, October). A note on the confinement problem. *Communications of the ACM*, 16(10), 613-615.
doi:10.1145/362375.362389

Popek, G. J. (1974). *The Principle of Kernel Design*. Proceedings of the May 6-10, 1974, National Computer Conference and Exposition (pp. 977-978). Chicago: Association for Computing Machinery.
doi:https://doi.org/10.1145/1500175.1500361

Saltzer, J., & Schroeder, M. (1975). The protection of information in computer systems. *Proceedings of the IEEE*, 63(9), 1278-1308. doi:10.1109/PROC.1975.9939