Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada

Canada

Security Playbook for Information System Solutions

Published: 2020-04-28

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT22-245/2020E-PDF
ISBN or ISSN: 978-0-660-34754-7

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Guide de sécurité pour les solutions de système d’information

Government of Canada   Gouvernement du Canada

Security Playbook for Information System Solutions

From Treasury Board of Canada Secretariat

On this page

1. Introduction

▼ In this section

1.1 Purpose

This document is a “playbook” for federal departments and agencies and outlines a set of security tasks for consideration when designing and implementing solutions for Government of Canada (GC) information systems in cloud environments.

The goal of this playbook is to:

- help projects develop a reasonable level of security assurance when implementing an information system solution
- help facilitate security assessment and authorization (SA&A) activities
- ensure that projects implement security considerations that conform with:
  - the *Directive on Security Management*
  - the Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice (SPIN) 2017-01

This playbook:

- focuses on a set of preliminary baseline security controls as a starting point
- is built around **agile** and **lean** principles
- is aligned with the guidance in *IT Security Risk Management: A Lifecycle Approach (ITSG-33)*
- does not prescribe a system development methodology

1.2 Scope

This playbook:

- focuses on software information system solutions being deployed in cloud environments
- addresses the specific scope of responsibility for the application components of information system solutions that projects are implementing in addition to cloud services
- assumes that security controls at the infrastructure layers have been implemented, in addition to the cloud service provider (CSP) environment, and are therefore inherited by the information system solution

Project teams should validate any assumption of security control inheritance with their departmental IT security authorities.

1.3 Stakeholders

This playbook is to be used by individuals who act in the following roles and participate in the project activities outlined in this playbook:

- the product owner [1]
- the authorizer (if different than the product owner)
- the project team lead
- the architecture owner
- the security architecture owner (if different than the architecture owner)
- project team members
- the security assessor
- the operations manager

Definitions of these roles can be found on the Disciplined Agile website and in Annex 1 of ITSG-33.

2. Considerations

▼ In this section

2.1 Baseline security controls

This playbook focuses on a preliminary set of baseline security controls that are suitable for application components of information system solutions that have a security category up to and including Protected B, medium integrity and medium availability (PBMM). This selection of security controls, listed in the appendix, provides a starting point for project teams and was selected to achieve the following objectives:

- comply with the applicable mandatory procedures in the *Directive on Security Management*
- meet the requirements of the Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice (SPIN)
- address the Communications Security Establishment’s (CSE’s) Top 10 Security Actions

- align with *Government of Canada Security Control Profile for Cloud-Based GC Services*
- focus on the selection of security controls to those implemented in software components of information system solutions
- achieve threat protection objectives specified in the ITSG-33 generic PBMM profile and the *Government of Canada Security Control Profile for Cloud-Based GC Services*

Project teams will need to tailor the applicable profile for their information system solution. This tailoring may result in the selection and implementation of additional security controls or enhancements to satisfy departmental security requirements or increase mitigation of specific threats.

In the security control catalogue, increasing levels of strength in security mechanisms can be achieved by implementing enhancements to base security controls. As a general rule, for a given security control, the more enhancements are implemented, the stronger the security mechanism. For example, implementing enhancement 1 of base security control IA-2 increases the strength of the identification and authentication mechanism, such as enforcing a second factor of authentication for privileged accounts.

2.2 Inherited security controls

The US National Institute of Standards and Technology defines common security controls as “security controls whose implementation results in a security capability that is inheritable by one or more organizational information systems.” Security controls are deemed inheritable by information systems or information system components when systems or components receive protection from implemented controls that were developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the systems or components. Examples of security controls that information systems and components could inherit include:

- IT security policies
- security awareness and training
- incident response plans
- physical access to facilities
- personnel security
- rules of behaviour

There are also a variety of technology-based security controls, which are typically implemented as common security controls and which can be used in information systems. Examples of technology-based, common security controls include:

- public key infrastructure (PKI) systems
- access control systems
- boundary protection systems

2.3 System development lifecycle process

Project teams using agile or more traditional waterfall methodologies should be able to use this playbook. Regardless of the methodology used, this playbook supports the integration of security activities within a project and throughout the system development lifecycle (SDLC) process by providing a set of tasks that project teams can add to their work items backlog or schedule.

If personal information is involved, project teams must ensure that privacy requirements are identified and appropriately addressed in their solutions in consultation with their departmental access to information and privacy (ATIP) office.

Project teams can learn more about security in IT projects in *Applying ITSG-33 guidance to IT projects* (ITSG-33 Primer for IT Projects), which is available on the ESA Tools and Templates GCpedia page (accessible only on the Government of Canada network).

2.4 Enterprise alignment

Project teams should consult with their departmental IT security and enterprise architecture or enterprise security architecture teams to:

- identify applicable security standards and opportunities for security solution reuse
- ensure enterprise alignment

2.5 Threat modelling

Project teams need to perform threat modelling to ensure that all threat exposures within their information system solutions are covered by appropriate designs and security mechanisms. The following links are resources that provide an introduction to threat modelling:

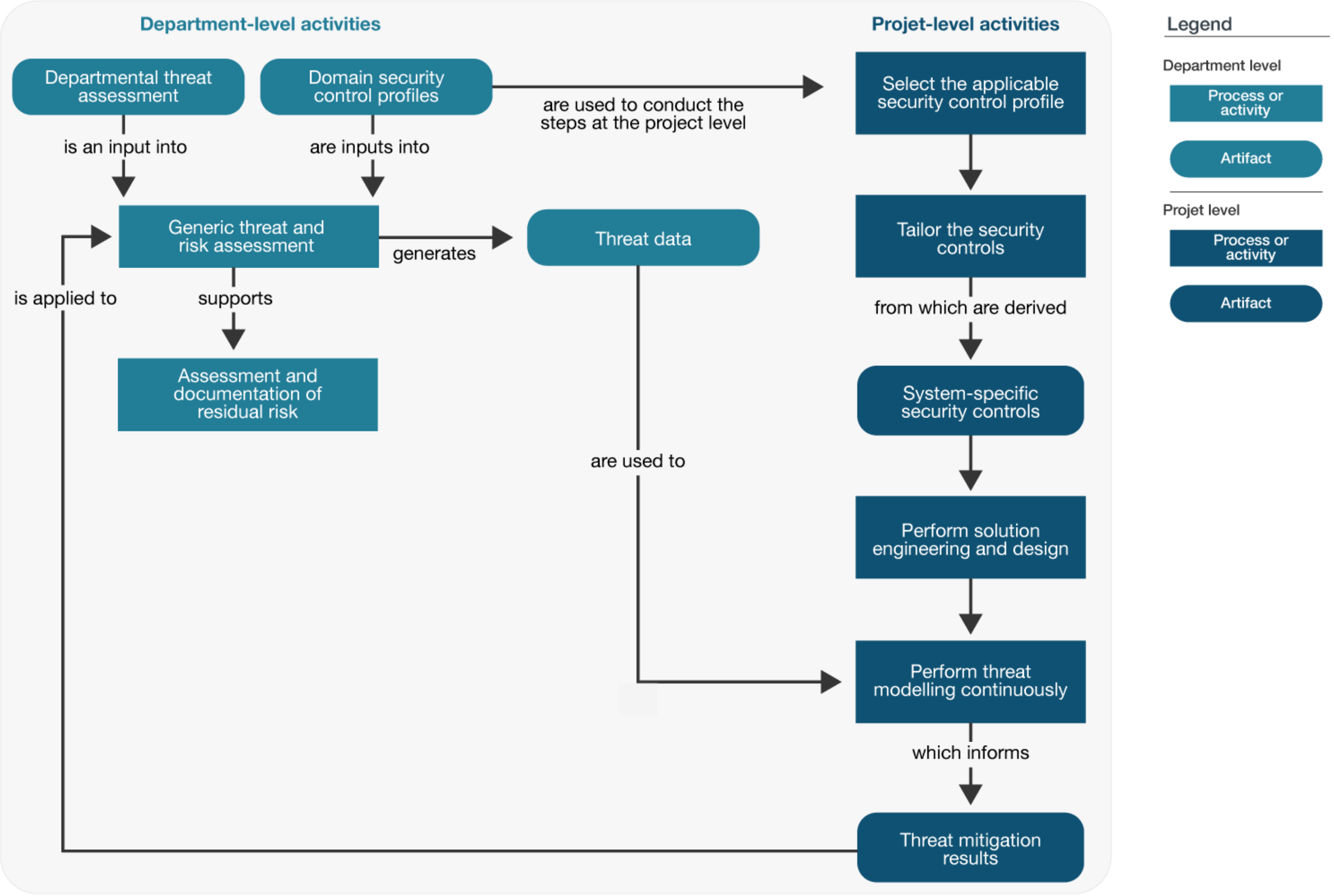
- Security Threat Models: An Agile Introduction from Agile Modeling
- Introduction to Microsoft's Security development Lifecycle (SDL) Threat Modelling presentation

In addition, departmental security authorities may want to document residual risks associated with the information system solution that a project is implementing against departmental threats. In the GC, the methodology of choice for that purpose is the Harmonized TRA Methodology (TRA-1). Threat modelling methodologies are typically not suited for assessing residual risks because they:

- tend to focus on threats and their mitigation
- do not include the qualification or quantification of risks

However, risk assessments and threat modelling can work together to satisfy both project-level and department-level requirements. Figure 1 presents an example of these methods working together in alignment with the guidance in ITSG-33.

Figure 1: notional integration of threat modelling and residual risk assessment


Department-level activities
Projet-level activities
Departmental threat assessment
Domain security control profiles
are used to conduct the steps at the project level
Select the applicable security control profile
is an input into
are inputs into
Generic threat and risk assessment
generates
Threat data
Tailor the security controls
is applied to
supports
from which are derived
Assessment and documentation of residual risk
System-specific security controls
are used to
Perform solution engineering and design
Perform threat modelling continuously
which informs
Threat mitigation results
Legend
Department level
Process or activity
Artifact
Projet level
Process or activity
Artifact

▼ Figure 1 - Text version

Figure 1 shows the relationship between department-level and project-level activities for threat assessments.

At the department level, the departmental threat assessment and the domain security control profiles are inputs into a generic threat and risk assessment.

The generic threat and risk assessment:

- generates threat data, which are used to perform threat modelling at the project level
- supports the assessment and documentation of residual risk
- is applied to the threat mitigation results

The domain security control profiles are used to conduct the steps at the project level. These steps are:

- select the applicable security control profile
- tailor the security controls, from which are derived the system-specific security controls
- perform solution engineering and design
- perform threat modelling, which informs the threat mitigation results

In Figure 1, departmental security authorities use a generic threat and risk assessment (TRA) to assess residual risks associated with the information system. The project team:

- selects an applicable security control profile and tailors the security controls for the information system
- models threats as part of the solution engineering and design processes to ensure that secure design patterns are adopted and appropriate security mechanisms are selected and implemented

- adjusts its threat model based on the threat data in the generic TRA

As the solution engineering and design processes progress:

- the project team informs departmental security authorities of threat mitigation results
- departmental security authorities use these results to assess and document residual risks

The right threat modelling method to use and exactly when threat modelling occurs in a project is the subject of debate. Project teams should use a method that they understand and that works well with their SDLC process.

2.6 Security assurance

Project teams need to be concerned with security assurance [2] for the:

- information system solutions that they implement
- underlying cloud services

For information system solutions, project teams can establish assurance by:

- incorporating security in project documentation
- completing security verification and validation tasks

Projects teams also need to produce verifiable outputs, such as testing plans and results, to support security assessment and authorization (SA&A). For more information on these topics, see *Applying ITSG-33 guidance to IT projects* (ITSG-33 Primer for IT Projects), which is available on the ESA Tools and Templates GCpedia page (accessible only on the Government of Canada network).

For the underlying cloud services, project teams can obtain security assurance by asking for SA&A evidence, either directly from internal service providers (for example, in the department or at Shared Services Canada), or through request for proposal (RFP) requirements or contractual clauses for commercial cloud service providers. See the *Government of Canada Cloud Security Risk Management Approach and Procedures* for more information on the SA&A process for commercial cloud services.

It is assumed that any underlying and external service used by a solution has been established through an approved security assurance process.

2.7 Security design considerations

While these security controls provide a strong foundation for the protection of most GC information system solutions that have a maximum security category of PBMM, project teams need to consider other factors when designing and building their solutions. These factors are:

- business needs for security and other business-related requirements for which specific security controls are prescribed
- design constraints, such as network security zoning, multi-tiered application structures, security design patterns and other architectural requirements
- the requirement for additional security controls to conform to departmental security standards or address specific threats
- the need to select stronger security mechanisms to address increasing levels of threat capabilities or impacts

3. Activities

This section describes a set of security activities and tasks that are recommended for most information system solutions. Projects teams can integrate these security activities and tasks when they are looking to:

- implement a web server
- configure a software as a service (SaaS) application
- implement a tiered web application

Note: Depending on the scenario, some of the activities may not apply.

Activity	Description
3.1 Security categorization	**Objective** Determine the security category of the solution being implemented.
	Tasks to complete ☐ Identify the business processes and information assets relating to the solution. ☐ Conduct an injury assessment. ☐ Determine the security category of the solution.
	References 1. SPIN 2017-01, subsection 6.1.1 2. Security Categorization Tool (accessible only on the Government of Canada network) 3. Related security control: RA-2
3.2 System concept	**Objective** Understand stakeholder needs and requirements as they relate to the solution.
	Tasks to complete ☐ Describe the concept for the solution. **Note:** Projects can use the concept case for digital projects [3] template to describe: • the problem or opportunity • the conceptual future state and desired business outcome(s) for their solution In addition, enterprise security architecture (ESA) templates and guides are also available on GCpedia (accessible only on the Government of Canada network). ☐ Identify all user and service management roles. Users should include administrators and auditors, as applicable. ☐ Describe all operational scenarios using cases or storyboards, including those related to service management and maintenance.
	References 1. Related security control: PL-7
3.3 Identity and access management	**Objective** Implement identity and access management mechanisms for the solution.

[3] According to Appendix C to the *Policy on the Planning and Management of Investments*.

Activity	Description
	Tasks to complete ☐ Implement a mechanism for uniquely identifying and authenticating organizational users, non-organizational users (if applicable), and processes (for example, username and password). ☐ Implement a multi-factor authentication mechanism for privileged accounts (for example, username, password and one-time password). ☐ Implement a process for managing accounts, access privileges, and access credentials for organizational users, non-organizational users (if required), and processes based on the principles of separation of duties and least privilege (for example, operational procedures and active directory). ☐ Determine access restrictions and configuration requirements for GC-issued endpoint devices, including those of non-privileged and privileged users, and configure access restrictions for endpoint devices accordingly. **Note:** Some service providers may offer configuration options to restrict endpoint device access. Alternatively, organizational policy and procedural instruments can be implemented to restrict access. ☐ Determine access restrictions and configuration requirements for non-organizational endpoint devices, including those of non-privileged and privileged users, and configure access restrictions for endpoint devices accordingly. ☐ Implement a mechanism for enforcing access authorizations. ☐ Change default passwords.
	References 1. SPIN 2017-01, subsection 6.2.3 2. *Guideline on Defining Authentication Requirements* 3. *Guideline on Identity Assurance* 4. *User Authentication Guidance for Information Technology Systems (ITSP.20.031 v3)* 5. Related security controls: AC-2, AC-2(1), AC-3, AC-5, AC-6, AC-6(5), AC-6(10), AC-7, AC-9, AC-19, AC-20(3), IA-2, IA-2(1), IA-2(2), IA-2(11), IA-4, IA-5, IA-5(1), IA-5(6), IA-5(7), IA-5(13), IA-6, IA-8
3.4 Auditing	**Objective** Implement an auditing mechanism for the solution.

[3] According to Appendix C to the *Policy on the Planning and Management of Investments*.

Activity	Description
	Tasks to complete ☐ Identify the events within the solution that must be audited. **Note:** At a minimum, it is recommended that the following events are included: • successful and unsuccessful account log-on events • account management events • object access • policy change • privilege functions • process tracking • system events For web applications, it is recommended that the following events are included: • all administrator activity • authentication checks • authorization checks • deletions of data • data access times • changes to data • permission changes ☐ Implement an audit process for the auditable events identified. At a minimum, the business owner or an auditor should audit actions against user accounts according to SPIN 2017-01. Additional auditing requirements may be provided by the business owner to satisfy specific business needs. **Note:** You may need to configure your solution to send the audit log records to a centralized logging facility, if one is available, where existing auditing mechanisms will be applied. ☐ Configure or use an authoritative time source for the time-stamp of the audit records generated by your solution components. ☐ Protect audit information by controlling access to the audit log tools.
	References 1. SPIN 2017-01, subsection 6.3.1 2. Related security controls: AU-2, AU-3, AU-6, AU-8, AU-9, AU-9(4), AU-12
3.5 Data protection	**Objective** Implement mechanisms for the protection of data in transit and at rest.
	Tasks to complete ☐ Implement an encryption mechanism to protect the confidentiality and integrity of data when data are in transit to and from your solution. ☐ Implement an encryption mechanism to protect the confidentiality and integrity of data when data are at rest in your solution's storage. ☐ Implement key data management procedures.

[3] According to Appendix C to the *Policy on the Planning and Management of Investments*.

Activity	Description
	References 1. SPIN 2017-01, subsection 6.2 2. Refer to the cryptography guidance in ITSP.40.111 and ITSP.40.062. 3. Refer to the *Considerations for Cryptography in Commercial Cloud Services* (accessible only on the Government of Canada network) 4. Related security controls: SC-8, SC-8(1), SC-12, SC-13, SC-17, SC-28, SC-28(1)
3.6 Networking	**Objective** Implement mechanisms to establish external and internal network perimeters and monitor network traffic. **Note:** This activity may not apply to all projects.
	Tasks to complete ☐ Implement network boundary protection mechanisms for all external facing interfaces that enforce a deny-all or allow-by-exception policy. ☐ Implement network security zones for your solution, in alignment with ITSG-22 and ITSG-38. Consider implementing increased levels of protection for management interfaces. ☐ Where feasible, implement a host-based firewall that enforces a deny-all or allow-by-exception policy.
	References 1. SPIN 2017-01, subsection 6.2.4 2. Related security controls: AC-4, SC-7, SC-7(5)
3.7 Secure development	**Objective** Limit vulnerabilities in the solution and ensure the integrity of data.

[3] According to Appendix C to the *Policy on the Planning and Management of Investments*.

Activity	Description
	Tasks to complete ☐ Implement session management mechanisms in accordance with best practices (for example, Open Web Application Security Project (OWASP) recommendations for web sessions). ☐ Implement application partitioning to separate user functionality and data from system management functionality and data. ☐ Implement input validation mechanisms to protect your solution from injection attacks and user input errors. ☐ Ensure that error messages generated by the software code do not reveal information that could be exploited by adversaries. ☐ Add a system-use notification as part of the log-on process before granting user access to your solution. ☐ Review information before it is released publicly to ensure that it does not contain sensitive information. ☐ Implement mechanisms to appropriately handle and retain information in storage and in outputs. ☐ Follow secure development practices to develop software code. ☐ Before allowing production operations, perform a vulnerability scan of the solution environment and apply any required updates and patches. Where possible, integrate vulnerability remediation into the continuous development process. ☐ Before allowing production operations, perform penetration testing and/or a run-time vulnerability assessment against publicly accessible interfaces, and apply any necessary corrective measures, such as patches. **Note:** More extensive penetration testing activities may be required depending on the nature of the solution being implemented. ☐ Provide any necessary training to users, administrators, and operators to ensure the correct use and operation of the implemented security mechanisms.
	References 1. SPIN 2017-01, subsections 6.2.1 and 6.2.6 2. Related security controls: AC-8, AC-12, AC-22, CA-5, CA-8, RA-3, RA-5, SA-8, SA-11, SA-11(1), SA-11(4), SA-15, SA-15(4), SA-16, SC-2, SC-23, SI-10, SI-11, SI-12
3.8 Service continuity	**Objective** Implement the required security mechanisms to support service continuity.
	Tasks to complete ☐ Obtain service continuity requirements from the business owner. **Note:** Service continuity requirements typically consist of a recovery-time objective and a recovery-point objective. They may also include maximum permissible downtime or maximum allowable downtime. ☐ Implement a backup-and-restore process for the GC data maintained in your solution. ☐ Implement a process to restore the solution's service or services within required objectives. ☐ Implement a transaction recovery mechanism, where applicable. ☐ Implement a contingency plan for your solution to support IT continuity requirements.

[3] According to Appendix C to the *Policy on the Planning and Management of Investments*.

Activity	Description
	References 1. SPIN 2017-01, subsection 6.2.9. 2. Related security controls: CP-2, CP-4, CP-9, CP-10, CP-10(2)
3.9 Configuration management	**Objective** Implement the security aspects of configuration management.
	Tasks to complete ☐ For each component of your solution, define and document a baseline configuration, including the configuration settings of commercial products, that represents the most restrictive mode of operation. ☐ Implement a process to keep the solution’s baseline configuration up to date as changes are implemented. **Note:** Configuration management should be automated to the maximum extent feasible. ☐ Implement a process to track and replace unsupported information system components.
	References 1. SPIN 2017-01, subsection 6.2.5 2. Related security controls: CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-8, CM-9, SA-22
3.10 Security operations	**Objective** Implement security operations mechanisms for your solution.
	Tasks to complete ☐ Implement a periodic vulnerability scanning process for your solution. **Note:** The vulnerability and patch management process should be automated and integrated in the release management process. ☐ Implement a process for periodic penetration testing or a run-time vulnerability assessment for your solution. ☐ Implement a vulnerability and patch management process for your solution. ☐ Implement an information system monitoring process for your solution. ☐ Implement an incident response plan for your solution. Consider the requirements in the *Government of Canada Cyber Security Event Management Plan (GC CSEMP) 2018*.
	References 1. SPIN 2017-01, subsection 6.3 2. Related security controls: IR-4, IR-5, IR-6, IR-8, SI-2, SI-4

[3] According to Appendix C to the *Policy on the Planning and Management of Investments*.

4. References

▼ In this section

4.1 Related policy instruments

- *Directive on Security Management*
- Direction on the Secure Use of Commercial Cloud Services: Security Implementation Notice (SPIN) 2017-01

4.2 Additional references

- *Government of Canada Security Control Profile for Cloud-based GC Services*
- *Government of Canada Cloud Security Risk Management Approach and Procedures*
- Security categorization guide and tool (accessible only on the Government of Canada network)
- *Government of Canada Cyber Security Event Management Plan (GC CSEMP) 2018*
- Concept case for digital projects
- Enterprise security architecture (ESA) template guides (accessible only on the Government of Canada network)
- *Guideline on Defining Authentication Requirements*
- *Guideline on Identity Assurance*
- *Considerations for Cryptography in Commercial Cloud Services*(accessible only on the Government of Canada network)
- *IT Security Risk Management: A Lifecycle Approach (ITSG-33)*
- *Guidance on Securely Configuring Network Protocols (ITSP.40.062)*
- *Baseline Security Requirements for Network Security Zones in the Government of Canada (ITSG-22)*
- *Network Security Zoning: Design Considerations for Placement of Services within Zones (ITSG-38)*

Appendix: baseline security controls

▼ In this section

- Abbreviations

The following table outlines a preliminary set of baseline security controls that are recommended for the application layer of information system solutions. Project teams should:

- use the table as a starting point
- implement additional security controls based on the nature and scope of what is being implemented and the analysis of threats and risks

See section 2 of the playbook for more information.

The applicability of security controls to security categories up to Protected B, medium integrity and medium availability is included to help project teams determine which security controls should be implemented based on the security category of their information system solution.

Abbreviations

DSM: *Directive on Security Management*
SPIN: Security Policy Implementation Notice
OWASP: Open Web Application Security Project

								Implementation of security control				
								Confidentiality		Integrity		Availa
Identifier	Security control	DSM (July 2019)	SPIN 2017-01	OWASP top 10	Primary objective	Function	Related activities	Low [4]	Medium [5]	Low	Medium	Low

								Implementation of security control				
								Confidentiality		Integrity		Availa
Identifier	Security control	DSM (July 2019)	SPIN 2017-01	OWASP top 10	Primary objective	Function	Related activities	Low [4]	Medium [5]	Low	Medium	Low
AC-2	Account management	B.2.3.2.1 B.2.3.2.6	6.2.3(a)	n/a (not available)	Enabler	Prevent	3.3	Control selected	Control selected	Control selected	Control selected	n/a (not available)
AC-2(1)	Account management: automated system account management	B.2.3.2.1 B.2.3.2.6	6.2.3(a)	n/a (not available)	Enabler	Prevent	3.3	Control selected	Control selected	Control selected	Control selected	n/a (not available)
AC-3	Access enforcement	n/a (not available)	6.2.3(a)	A5	Threat	Prevent	3.3	Control selected	Control selected	Control selected	Control selected	n/a (not available)
AC-4	Information flow control	n/a (not available)	6.2.4(b)	A6	Enabler	Prevent	3.6	Control selected	Control selected	Control selected	Control selected	n/a (not available)
AC-5	Separation of duties	B.2.3.2.2 B.2.3.2.4 B.2.3.2.5	6.2.3(a)	A5	Threat	Prevent	3.3	Control selected	Control selected	Control selected	Control selected	n/a (not available)
AC-6	Least privilege	B.2.3.2.2 B.2.3.2.4 B.2.3.2.5	6.2.3(a)	A5	Threat	Prevent	3.3	Control selected	Control selected	Control selected	Control selected	n/a (not available)
AC-6(5)	Least privilege: privileged accounts	B.2.3.2.4	6.3.2(a)	A5	Threat	Prevent	3.3	Control selected	Control selected	Control selected	Control selected	n/a (not available)
AC-6(10)	Least privilege: prohibit non-privileged users from executing	B.2.3.2.4	6.2.3(a)	A5	Threat	Prevent	3.3	Control selected	Control selected	Control selected	Control selected	n/a (not available)
AC-7	Unsuccessful log-on	n/a (not available)	6.2.3(a)	A2	Threat	Prevent	3.3	Control selected	Control selected	Control selected	Control selected	Control selected
AC-8	System use notification	B.2.3.2.3	6.2.1	n/a (not available)	Threat	Prevent	3.7	Control selected	Control selected	Control selected	Control selected	n/a (not available)
AC-9	Previous log-on (access)	n/a (not available)	6.2.3(a)	n/a (not available)	Threat	Detect	3.3	Control not selected	Control selected	Control not selected	Control selected	n/a (not available)
AC-12	Session termination	n/a (not available)	6.2.1	A2	Threat	Prevent	3.7	Control selected	Control selected	Control selected	Control selected	n/a (not available)
AC-19	Access control for mobile devices	n/a (not available)	6.2.3(a)	n/a (not available)	Threat	Prevent	3.3	Control not selected	Control selected	Control not selected	Control selected	n/a (not available)
AC-20(3)	Use of external information systems: systems, components or devices not owned by the organization	n/a (not available)	6.2.3(a)	n/a (not available)	Assurance	n/a (not available)	3.3	Control not selected	Control selected	Control not selected	Control selected	n/a (not available)
AC-22	Publicly accessible content	n/a (not available)	6.2.1	n/a (not available)	Threat	Prevent	3.7	Control selected	Control selected	n/a (not available)	n/a (not available)	n/a (not available)

[4] Low for confidentiality means Protected A.

[5] Medium for confidentiality means Protected B.

								Implementation of security control				
								Confidentiality		Integrity		Availa
Identifier	**Security control**	**DSM (July 2019)**	**SPIN 2017-01**	**OWASP top 10**	**Primary objective**	**Function**	**Related activities**	**Low [4]**	**Medium [5]**	**Low**	**Medium**	**Low**
AU-2	Auditable events	B.2.3.8.1	6.3	A2, A5, A8, A10	Enabler	Detect	3.4	Control selected	Control selected	Control selected	Control selected	n/a (not available)
AU-3	Content of audit records	n/a (not available)	6.3	A10	Enabler	Detect	3.4	Control selected	Control selected	Control selected	Control selected	n/a (not available)
AU-6	Audit review, analysis, and reporting	B.2.7.2	6.3	n/a (not available)	Enabler	Detect	3.4	Control selected	Control selected	Control selected	Control selected	n/a (not available)
AU-8	Time-stamps	B.2.3.8.1	6.3	n/a (not available)	Enabler	Detect	3.4	n/a (not available)	n/a (not available)	Control selected	Control selected	n/a (not available)
AU-9	Protection of audit information	B.2.3.8.1	n/a (not available)	n/a (not available)	Threat	Prevent	3.4	Control selected	Control selected	Control selected	Control selected	n/a (not available)
AU-9(4)	Protection of audit information: access by subset of privileged users	B.2.3.2.5	n/a (not available)	n/a (not available)	Threat	Prevent	3.4	Control selected	Control selected	Control selected	Control selected	n/a (not available)
AU-12	Audit generation	B.2.3.8.1	6.3	A2, A5, A8	Enabler	Detect	3.4	Control selected	Control selected	Control selected	Control selected	n/a (not available)
CA-5	Plan of action and milestones	B.2.6.2	6.2.1	n/a (not available)	Business	Prevent	3.7	Control selected	Control selected	Control selected	Control selected	Control selected
CA-8	Penetration testing	n/a (not available)	6.2.1	n/a (not available)	Assurance	n/a (not available)	3.7	Control not selected	Control selected	Control not selected	Control selected	Control not selected
CM-2	Baseline configuration	B.2.3.3.3 B.2.3.3.4	6.2.5	A6	Threat	Prevent	3.9	n/a (not available)	n/a (not available)	Control selected	Control selected	n/a (not available)
CM-3	Configuration change control	B.2.3.3.3 B.2.3.3.4	6.2.5	n/a (not available)	Enabler	Prevent	3.9	n/a (not available)	n/a (not available)	Control selected	Control selected	n/a (not available)
CM-4	Security impact analysis	B.2.3.3.1	6.2.5	n/a (not available)	Enabler	Prevent	3.9	n/a (not available)	n/a (not available)	Control selected	Control selected	n/a (not available)
CM-5	Access restrictions for change	B.2.3.3.3 B.2.3.3.4	6.2.5	n/a (not available)	Threat	Prevent	3.9	n/a (not available)	n/a (not available)	Control selected	Control selected	n/a (not available)
CM-6	Configuration settings	B.2.3.3.2	6.2.5	A5, A6	Threat	Prevent	3.9	n/a (not available)	n/a (not available)	Control selected	Control selected	n/a (not available)
CM-7	Least functionality	B.2.3.3.2 B.2.3.3.3 B.2.3.3.4	6.2.5	A5, A6	Security approach	n/a (not available)	3.9	Control selected	Control selected	Control selected	Control selected	n/a (not available)
CM-8	Information system component inventory	B.2.3.3.3 B.2.3.3.4	6.2.5	A9	Enabler	Prevent	3.9	n/a (not available)	n/a (not available)	Control selected	Control selected	n/a (not available)
CM-9	Configuration management plan	n/a (not available)	6.2.5	n/a (not available)	Assurance	n/a (not available)	3.9	n/a (not available)	n/a (not available)	Control selected	Control selected	n/a (not available)

[4] Low for confidentiality means Protected A.

[5] Medium for confidentiality means Protected B.

								Implementation of security control				
								Confidentiality		Integrity		Availa
Identifier	Security control	DSM (July 2019)	SPIN 2017-01	OWASP top 10	Primary objective	Function	Related activities	Low [4]	Medium [5]	Low	Medium	Low
CP-2	Contingency plan	B.2.3.10.1	6.2.9	A10	Assurance	n/a (not available)	3.8	n/a (not available)	n/a (not available)	n/a (not available)	n/a (not available)	Control selected
CP-4	Contingency plan testing	B.2.3.10.3	6.2.9	A10	Assurance	n/a (not available)	3.8	n/a (not available)	n/a (not available)	n/a (not available)	n/a (not available)	Control selected
CP-9	Information system backups	n/a (not available)	6.2.9	A10	Enabler	Recover	3.8	n/a (not available)	n/a (not available)	n/a (not available)	n/a (not available)	Control selected
CP-10	Information system recovery and reconstitution	B.2.3.10.2	6.2.9	A10	Enabler	Recover	3.8	n/a (not available)	n/a (not available)	n/a (not available)	n/a (not available)	Control selected
CP-10(2)	Information system recovery and reconstitution: transaction recovery	B.2.3.10.2	6.2.9	A10	Enabler	Recover	3.8	n/a (not available)	n/a (not available)	Control selected	Control selected	Control selected
IA-2	Identification and authentication (organizational users)	B.2.3.1	6.2.3(a)	A2	Enabler	Prevent	3.3	Control selected	Control selected	Control selected	Control selected	n/a (not available)
IA-2(1)	Identification and authentication (organizational users): network access for privileged accounts	B.2.3.1	6.2.3(a)	A2	Enabler	Prevent	3.3	Control selected	Control selected	Control selected	Control selected	n/a (not available)
IA-2(2)	Identification and authentication (organizational users): network access for non-privileged accounts	B.2.3.1	6.2.3(a)	A2	Enabler	Prevent	3.3	Control selected	Control selected	Control selected	Control selected	n/a (not available)
IA-2(11)	Identification and authentication (organizational users): remote access for separate device	B.2.3.1	6.2.3(a)	A2	Threat	Prevent	3.3	Control selected	Control selected	Control selected	Control selected	n/a (not available)
IA-4	Identifier management	n/a (not available)	6.2.3(a)	n/a (not available)	Enabler	Prevent	3.3	Control selected	Control selected	Control selected	Control selected	n/a (not available)
IA-5	Authenticator management	n/a (not available)	6.2.3(a)	A2	Enabler	Prevent	3.3	Control selected	Control selected	Control selected	Control selected	n/a (not available)

[4] Low for confidentiality means Protected A.

[5] Medium for confidentiality means Protected B.

								Implementation of security control				
								Confidentiality		Integrity		Availa
Identifier	Security control	DSM (July 2019)	SPIN 2017-01	OWASP top 10	Primary objective	Function	Related activities	Low [4]	Medium [5]	Low	Medium	Low
IA-5(1)	Authenticator management: password-based authentication	n/a (not available)	6.2.3(a)	A2	Threat	Prevent	3.3	Control selected	Control selected	Control selected	Control selected	n/a (not available)
IA-5(6)	Authenticator management: protection of authenticators	n/a (not available)	n/a (not available)	A2	Threat	Prevent	3.3	Control selected	Control selected	Control selected	Control selected	n/a (not available)
IA-5(7)	Authenticator management: no embedded unencrypted static authenticators	n/a (not available)	6.2.3(a)	A2	Threat	Prevent	3.3	Control selected	Control selected	n/a (not available)	n/a (not available)	n/a (not available)
IA-5(13)	Authenticator management: expiration of cached authenticators	n/a (not available)	n/a (not available)	A2, A3	Threat	Prevent	3.3	Control selected	Control selected	Control selected	Control selected	n/a (not available)
IA-6	Authenticator feedback	n/a (not available)	6.2.3(a)	n/a (not available)	Threat	Prevent	3.3	Control selected	Control selected	n/a (not available)	n/a (not available)	n/a (not available)
IA-8	Identification and authentication (non-organizational users)	B.2.3.1	6.2.3(a)	A2	Enabler	Prevent	3.3	Control selected	Control selected	Control selected	Control selected	n/a (not available)
IR-4	Incident handling	n/a (not available)	6.3.2	A10	Threat	Detect or respond	3.10	Control selected	Control selected	Control selected	Control selected	Control selected
IR-5	Incident monitoring	n/a (not available)	6.3.2	A10	Assurance	n/a (not available)	3.10	Control selected	Control selected	Control selected	Control selected	Control selected
IR-6	Incident reporting	B.2.3.7.4	6.3.2	A10	Assurance	n/a (not available)	3.10	Control selected	Control selected	Control selected	Control selected	Control selected
IR-8	Incident response plan	n/a (not available)	6.3.2	A10	Assurance	n/a (not available)	3.10	Control selected	Control selected	Control selected	Control selected	Control selected
PL-7	Security concept of operations	n/a (not available)	6.2.1	n/a (not available)	Assurance	n/a (not available)	3.2	Control selected	Control selected	Control selected	Control selected	Control selected
RA-2	Security categorization	n/a (not available)	6.1.1	A3	Business	n/a (not available)	3.1	Control selected	Control selected	Control selected	Control selected	Control selected
RA-3	Risk assessment	B.2.2.1.2 B.2.5.3 B.2.7.1	6.2.1	n/a (not available)	Business	n/a (not available)	3.7	Control selected	Control selected	Control selected	Control selected	Control selected
RA-5	Vulnerability scanning	B.2.3.7.2 B.2.3.7.3 B.2.3.7.4 B.2.7.1	6.2.6	A4, A9	Enabler	Prevent	3.7	Control selected	Control selected	Control selected	Control selected	Control selected

[4] Low for confidentiality means Protected A.

[5] Medium for confidentiality means Protected B.

								Implementation of security control				
								Confidentiality		Integrity		Availa
Identifier	**Security control**	**DSM (July 2019)**	**SPIN 2017-01**	**OWASP top 10**	**Primary objective**	**Function**	**Related activities**	**Low [4]**	**Medium [5]**	**Low**	**Medium**	**Low**
SA-8	Security engineering principles	B.2.5.1	6.2.1	n/a (not available)	Security approach	n/a (not available)	3.7	Control selected	Control selected	Control selected	Control selected	Control selected
SA-11	Developer security testing and evaluation	n/a (not available)	6.2.1	n/a (not available)	Assurance	n/a (not available)	3.7	Control selected	Control selected	Control selected	Control selected	Control selected
SA-11(1)	Developer security testing and evaluation: static code analysis	n/a (not available)	6.2.1	A4	Assurance	n/a (not available)	3.7	Control selected	Control selected	Control selected	Control selected	Control selected
SA-11(4)	Developer security testing and evaluation: manual code reviews	n/a (not available)	6.2.1	A4	Assurance	n/a (not available)	3.7	Control selected	Control selected	Control selected	Control selected	Control selected
SA-15	Development process, standards and tools	n/a (not available)	6.2.1	n/a (not available)	Security approach	n/a (not available)	3.7	Control selected	Control selected	Control selected	Control selected	Control selected
SA-15(4)	Development process, standards, and tools: threat modelling and vulnerability analysis	n/a (not available)	6.2.1	n/a (not available)	Security approach	n/a (not available)	3.7	Control selected	Control selected	Control selected	Control selected	Control selected
SA-16	Developer-provided training	n/a (not available)	6.2.1	n/a (not available)	Assurance	n/a (not available)	3.7	Control selected	Control selected	Control selected	Control selected	Control selected
SA-22	Unsupported system components	n/a (not available)	6.2.5	n/a (not available)	Business	n/a (not available)	3.9	Control selected	Control selected	Control selected	Control selected	Control selected
SC-2	Application partitioning	n/a (not available)	6.2.1	A6	Security approach	n/a (not available)	3.7	Control selected	Control selected	Control selected	Control selected	Control selected
SC-7	Boundary protection	B.2.3.6.1	6.2.4(b)	A6	Threat	Prevent or detect	3.6	Control selected	Control selected	Control selected	Control selected	n/a (not available)
SC-7(5)	Boundary protection: deny-by-default or allow-by-exception	B.2.3.6.1	6.2.4(b)	A6	Security approach	n/a (not available)	3.6	Control selected	Control selected	Control selected	Control selected	n/a (not available)
SC-8	Transmission confidentiality and integrity	B.2.3.6.3	6.2(b) 6.2.4(a)	A3	Threat	Prevent	3.5	Control selected	Control selected	Control selected	Control selected	n/a (not available)

[4] Low for confidentiality means Protected A.

[5] Medium for confidentiality means Protected B.

								Implementation of security control				
								Confidentiality		Integrity		Availa
Identifier	Security control	DSM (July 2019)	SPIN 2017-01	OWASP top 10	Primary objective	Function	Related activities	Low [4]	Medium [5]	Low	Medium	Low
SC-8(1)	Transmission confidentiality and integrity: cryptographic or alternative physical protection	B.2.3.6.3	6.2(b) 6.2.4(a)	A3	Threat	Prevent	3.5	Control selected	Control selected	Control selected	Control selected	n/a (not available)
SC-12	Cryptographic key establishment and management	n/a (not available)	6.2(b) 6.2.4(a)	A3	Enabler	Prevent or detect	3.5	Control selected	Control selected	Control selected	Control selected	n/a (not available)
SC-13	Cryptographic protection	n/a (not available)	6.2(b) 6.2.4(a)	A3	Threat	Prevent	3.5	Control selected	Control selected	Control selected	Control selected	n/a (not available)
SC-17	Public key infrastructure certificates	n/a (not available)	6.2(b) 6.2.4(a)	A2	Threat	Prevent	3.5	Control selected	Control selected	Control selected	Control selected	n/a (not available)
SC-23	Session authenticity	n/a (not available)	6.2.1	A2	Threat	Prevent	3.7	n/a (not available)	n/a (not available)	Control selected	Control selected	n/a (not available)
SC-28	Protection of information at rest	n/a (not available)	6.2(b)	A3	Threat	Prevent	3.5	Control not selected	Control selected	Control not selected	Control selected	n/a (not available)
SC-28(1)	Protection of information at rest: cryptographic protection	n/a (not available)	6.2(b)	A3	Threat	Prevent	3.5	Control not selected	Control selected	Control not selected	Control selected	n/a (not available)
SI-2	Flaw remediation	B.2.3.7.3	6.2.6	A4, A9	Enabler	Prevent	3.10	n/a (not available)	n/a (not available)	Control selected	Control selected	n/a (not available)
SI-4	Information system monitoring	B.2.3.7.1 B.2.3.8.2	6.3 6.3.1	A10	Threat	Detect	3.10	Control selected	Control selected	Control selected	Control selected	Control selected
SI-10	Information input validation	n/a (not available)	6.2.1	A1, A4, A7, A8	Threat	Detect	3.7	n/a (not available)	n/a (not available)	Control selected	Control selected	n/a (not available)
SI-11	Error handling	n/a (not available)	6.2.1	n/a (not available)	Threat	Prevent	3.7	n/a (not available)	n/a (not available)	Control selected	Control selected	n/a (not available)
SI-12	Information handling and retention	n/a (not available)	n/a (not available)	n/a (not available)	Business	Prevent	3.7	Control selected	Control selected	Control selected	Control selected	n/a (not available)

[4] Low for confidentiality means Protected A.

[5] Medium for confidentiality means Protected B.

Footnotes

[1] Equivalent to the program and service delivery manager and business owner.

[2] Security assurance is defined in ITSG-33 as “confidence-building tasks that aim to ensure that a security control is designed and implemented correctly, and is operating as intended. In addition, security assurance includes tasks that aim to ensure the ability of all security controls in an information system’s security design, implementation and operations to satisfy the business needs for security.”

Date modified:
2020-01-23