Communications
Security Establishment

Centre de la sécurité
des télécommunications

CANADIAN CENTRE FOR
CYBER SECURITY

GUIDANCE ON CLOUD SECURITY ASSESSMENT AND AUTHORIZATION

ITSP.50.105

May 2020

PRACTITIONER

Canada

FOREWORD

ITSP.50.105 Guidance on Cloud Security Assessment and Authorization is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE). For more information or suggestions for amendments contact Canadian Centre for Cyber Security (Cyber Centre) Client Services team:

Cyber Centre Contact Centre
contact@cyber.gc.ca
613-949-7048 or 1-833-CYBER-88

EFFECTIVE DATE

This publication takes effect on (20/05/2020).

OVERVIEW

Cloud computing has the potential to provide your organization with flexible, on-demand, scalable and self-service IT services. To benefit from cloud computing, your organization must ensure that security risks are properly managed, cloud-specific security considerations are addressed, and security controls of cloud-based services are properly assessed before authorized.

You organization can use the guidance in this document to assist with its security assessment and authorization of cloud-based services. *ITSP.50.105* and its appendices:

- review third-party assurance frameworks;
- recommend ways to assess cloud service provider (CSP) controls;
- recommend ways to assess your organization’s controls;
- recommend ways to authorize, continuously monitor, and maintain the authorization of cloud-based services; and
- provide assessment considerations for security controls.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ANNEXES

1 INTRODUCTION

Cloud environments are more complex than traditional computing environments. CSPs rely on a number of complex technologies to secure the cloud infrastructure and provide key security features to your organization for the protection of its cloud workload. Both CSPs and your organization are responsible for securing different components under their respective responsibility. This shared responsibility model adds further complexity to the cloud ecosystem. Strong security assessment and monitoring practices must be applied to provide assurance that appropriate controls are applied by the different cloud actors, and that they are operating and functioning effectively.

While the shared responsibility model of cloud computing allows for the delegation of some responsibilities to the CSP, your organization is responsible for determining and managing the residual risks under which the cloud-based service will be operating. As a result, your organization must understand the overall effectiveness of its security controls and those implemented by the CSP.

This publication recommends an approach that ensures:

- security risks are properly managed;
- cloud specific security considerations are addressed; and
- security controls of cloud-based services are correctly assessed before authorization.

ITSP.50.105 is part of a suite of documents developed by the Cyber Centre to help secure cloud-based services and supports the approach defined in *ITSM.50.062 Cloud Security Risk Management*.[1][1]

1.1 POLICY DRIVERS

The need to assess security is normally identified in your organization's security policies, directives, regulations, standards, and guidelines. The publications identified below can be used as reference material when your organization is creating its own security assessment program for cloud services security:

- Cyber Centre, *ITSG-33 IT Security Risk Management: A Lifecycle Approach* [2]
- Cloud Security Alliance (CSA), *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0* [3]
- National Institute of Standards and Technology (NIST), *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (Discussion Draft*) [4].
- Treasury Board of Canada Secretariat, *Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice (SPIN)* [5]

[1] Numbers in square brackets indicate a reference cited in the Supporting Content section of this document.

1.2 APPLICABLE ENVIRONMENTS

The security guidance provided in this document applies to private and public sector organizations. The guidance can be applied to cloud-based services independently of the cloud service and the deployment models.

1.3 RELATIONSHIP TO CLOUD RISK MANAGEMENT

ITSG-33 [2] suggests a set of activities at two levels within your organization: the departmental-level and the information system-level.

Departmental-level activities[2] integrate into your organization's security program to plan, manage, assess, and improve the management of IT security-related risks faced by your organization.

Information system-level activities[3] are integrated into an information system development lifecycle (SDLC). These activities include the implementation of information system security engineering, threat and risk assessment, security assessment, and authorization. The Cyber Centre risk management approach for cloud security is aligned with the information system-level activities. As depicted in Figure 1, the assessment, authorization, and continuous monitoring activities supports steps four, six, seven, eight, and nine of the cloud security risk management approach.

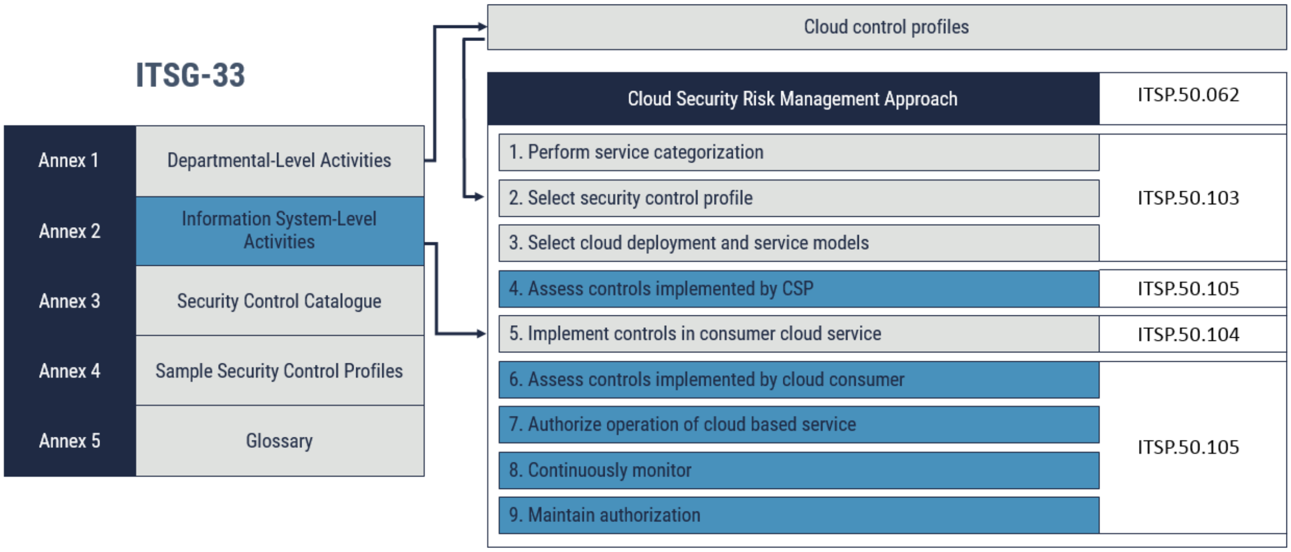

ITSG-33
Annex 1
Departmental-Level Activities
Annex 2
Information System-Level Activities
Annex 3
Security Control Catalogue
Annex 4
Sample Security Control Profiles
Annex 5
Glossary
Cloud control profiles
Cloud Security Risk Management Approach
ITSP.50.062
1. Perform service categorization
2. Select security control profile
3. Select cloud deployment and service models
ITSP.50.103
4. Assess controls implemented by CSP
ITSP.50.105
5. Implement controls in consumer cloud service
ITSP.50.104
6. Assess controls implemented by cloud consumer
7. Authorize operation of cloud based service
8. Continuously monitor
9. Maintain authorization
ITSP.50.105

Figure 1: **Security assessment, authorization and monitoring relationship to Information system-level activities and Cloud security risk management approach**

[2] Annex 1 of ITSG-33 [2] describes departmental-level activities in detail.
[3] Annex 2 of ITSG-33 [2] describes information system-level activities in detail.

1.4 WHAT IS CLOUD SECURITY ASSESSMENT AND MONITORING?

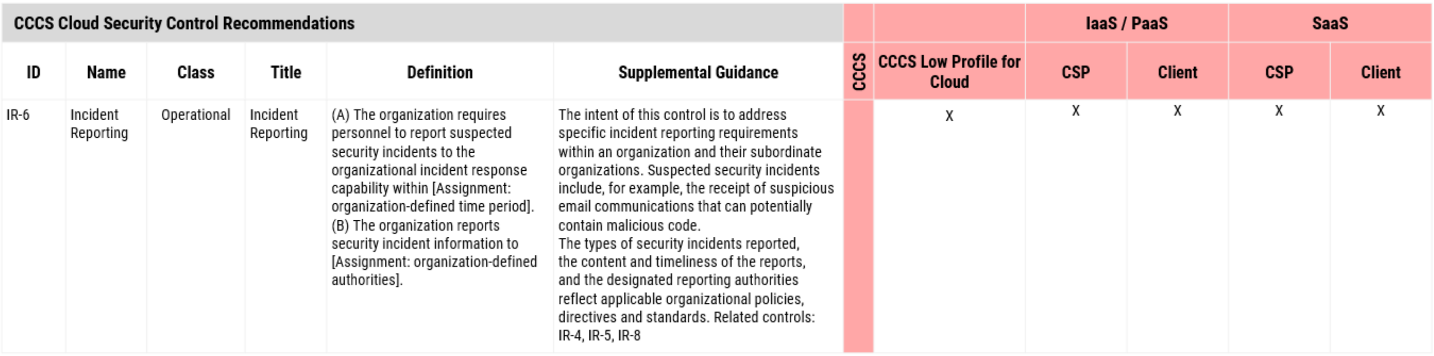
Your organization and your CSP need to implement and operate policies, standards, procedures, guidelines, and controls to assure the security of cloud computing. Cloud security assessment and monitoring:

- assures the necessary security controls are integrated into the design and implementation of a cloud-based service;
- identifies gaps between security control requirements and their actual implementation;
- validates that cloud security controls operate and function effectively; and
- serves as the basis for risk acceptance, avoidance, or mitigation decisions.

2 CONTEXT

2.1 CLOUD CONTROL PROFILES

Security control profiles have been developed for cloud-based services based upon the baseline profiles in Annex 4 of ITSG-33 [2]. The cloud security control profiles identify the recommended security controls that your CSP and your organization should implement for the assessed security category of each respective business domain[4]. The selected cloud control profile also serves as the basis for assessment of the security controls. As depicted in Figure 2, the cloud security control profiles indicate the recommended controls for each cloud service deployment model. The control profiles also indicate who is responsible for the controls (either your CSP or your organization).



CCCS Cloud Security Control Recommendations								IaaS / PaaS		SaaS	
ID	Name	Class	Title	Definition	Supplemental Guidance	CCCS	CCCS Low Profile for Cloud	CSP	Client	CSP	Client
IR-6	Incident Reporting	Operational	Incident Reporting	(A) The organization requires personnel to report suspected security incidents to the organizational incident response capability within [Assignment: organization-defined time period]. (B) The organization reports security incident information to [Assignment: organization-defined authorities].	The intent of this control is to address specific incident reporting requirements within an organization and their subordinate organizations. Suspected security incidents include, for example, the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable organizational policies, directives and standards. Related controls: IR-4, IR-5, IR-8		X	X	X	X	X

Figure 2: **Cloud control profile, CSP vs client control**

Your organization does not have direct control or the necessary visibility to directly assess controls under the responsibility of the CSP. For that reason, your organization should review formal certifications or attestations from independent third-parties to verify that the CSP has implemented their controls and that they are functioning effectively. Your organization should directly assess any controls within the scope of its responsibilities.

[4] Cyber Centre *ITSP.50.103 Guidance on Security Categorization of Cloud-Based Services* [6] recommends an approach to inventory and categorize business processes and information assets.

2.2 SHARED RESPONSIBILITIES AND SECURITY ASSESSMENT

Cloud security assessment and monitoring is a shared responsibility. Responsibility for assessment of security controls will vary based on the chosen cloud deployment and service model. In the Infrastructure as a Service (IaaS) model, your organization is responsible for direct assessment of more components and controls, while in the PaaS and SaaS models, your organization must leverage formal certifications or attestations from independent third- parties to assure that the security controls are implemented and functioning effectively.

2.2.1 CLOUD CONSUMER RESPONSIBILITIES

During security assessment and monitoring, your organization is responsible for the following:

- understanding security controls that are under their responsibility and which ones are under CSP responsibility;
- conducting all required threat and risk assessments (TRA) and privacy impact assessments (PIA);
- obligating its CSP (with clauses in the CSP contract) to demonstrate security requirement compliance with independent third-party attestations [5];
- requiring that any formal certification or attestation is from an independent third-party [6];
- ensuring that CSP security controls and features are clearly defined, implemented, and maintained throughout the life of the contract;
- reviewing security controls under their own responsibility;
- reviewing formal certifications or attestations (from an independent third-party) that show its CSP is complying to industry regulations and requirements [7];
- understanding the overall effectiveness of CSP and cloud consumer security controls to determine and manage the residual risks under which the service will be operating;
- performing security assessments and authorizations of information systems or services before they are approved for operation; and
- managing security risks continuously to its own information and IT assets throughout the life of the programs and services.

[5] Your organization should require its CSP to demonstrate compliance periodically (by providing formal certification or attestation from an independent third party) throughout the duration of the contract to support continuous monitoring activities.

[6] Formal certification and attestation should be issued from an independent third party certified under the AICPA and/or ISO certification regime and conform to ISO/IEC 17020 quality management system standard. A third party needs to be objective and apply professional standards to the evidence reviewed and produced.

[7] Industry regulations and requirements such as Payment Card Industry Data Security Standard (PCI DSS), Service Organization Control (SOC) 1&2, Health Insurance Portability and Accountability Act (HIPAA), Cloud Security Alliance (CSA) Security Trust and Assurance Registry (STAR) and the International Organization for Standardization (ISO 27001, 27017, and 27018).

2.2.2 CLOUD SERVICE PROVIDER RESPONSIBILITIES

CSPs have the following security assessment and monitoring responsibilities:

- documenting the security controls and features used by their cloud services to help your organization understand the security controls under its responsibility[8];
- ensuring that contractual and service level agreements are met;
- demonstrating compliance to security requirements by providing formal certification or attestation from an independent third-party[9];
- demonstrating compliance to security requirements periodically through the duration of the contract to support continuous monitoring activities;
- providing cloud consumers with information describing their cloud services and implemented security controls;
- providing cloud consumers with information on how to securely deploy applications and services on their cloud platforms; and
- continuously monitoring their cloud services to detect changes in the security posture of the cloud service environment and reporting back on incidents and any changes to the security posture.

2.3 THIRD-PARTY AUDITS, REPORTING FRAMEWORKS, AND CERTIFICATIONS

Conducting a comprehensive and independent security assessments of a CSP requires time, financial, and personnel resources. Fortunately, most CSPs undergo third-party audits, and compliance verification. These audits (which follow various regulations and industry requirements[10]) provide your organization with attestations or certifications that security controls are in place and operating effectively.

2.3.1 SYSTEM AND ORGANIZATION CONTROLS (SOC)

A SOC report is produced by an independent Certified Public Accountant (CPA) to provide assurance to a service organization (an organization which provide services to other entities) that the service and controls in the services they offer are comprehensive. Each type of SOC report is designed to help service organizations meet specific user needs.[11]

Originally developed by the American Institute of Certified Public Accountants (AICPA), three SOC report formats have been established to meet different needs. A SOC 1 report accounts for controls within a service organization which are relevant to

[8] CSPs can document their security controls using System Security Plans, and standard industry documents and tools such as the Cloud Security Alliance (CSA) Consensus Assessment Initiative Questionnaire (CAIQ).

[9] Formal certification or attestation for various regulations and industry requirements include PCI DSS, SOC 1, SOC2, HIPAA, CSA STAR, ISO 27001, ISO 27017, and ISO 27018.

[10] These attestation and certification programs include the United States Federal Risk and Authorization Management Program (FedRAMP), the American Institute of Certified Public Accountants (AICPA) System and Organization Controls (SOC) for service organizations, the International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) standards, and the Cloud Security Alliance (CSA) Security Trust and Assurance Registry (STAR) program.

[11] Additional information on SOC for Service Organizations can be found at AICPA.org (English only)

a user's internal control over financial reporting. For example, your organization's financial auditor may require a SOC 1 report to have confidence over a service organization's controls that relate to your organization's financial reporting. SOC 2 and SOC 3 reports describe controls at a service organization which relate to the trust service principles of security, availability, processing integrity confidentiality, or privacy.[12] It should be noted that SOC 1 and SOC 2 reports are not a certification but rather an auditor's opinion on a service organization's internal controls and security practices. It should also be noted that SOC 3 engagements are general use reports, can result in a certification being issued,[13] and allow for a seal to be placed on the CSP website for marketing purposes. SOC examinations do not provide a complete assessment of security governance. Instead, they focus on specific trust principles and criteria.

There are five sections to a SOC 2 report:

- Section I: An independent service auditor's opinion;
- Section II: A management assertion (whether the description of the service organization's systems is fairly presented, and whether the controls included in the description are suitably designed to meet the applicable Trust Service criteria);
- Section III: A system description overview (provided by the service organization);
- Section IV: A topical area system description (provided by the service organization) and testing and results (provided by the service auditor); and
- Section V: Other information provided by the service organization.

A SOC 3 report differs from a SOC 2 report in that it provides limited auditor opinions, a CSP management assertion, and an abbreviated description of the CSP system. SOC 3 reports are shorter and do not provide a description of controls and testing procedures. SOC 3 reports are meant for general use, are often used by CSPs for marketing purposes, and do not provide details of the controls. The distribution of SOC 1 and SOC 2 reports is generally restricted, and requires a non-disclosure agreement, while SOC 3 reports can be distributed freely.

There are two types of SOC reports. A Type 1 report is an attestation of controls at a specific point in time, while a Type 2 report provides an attestation of controls over a minimum period of six months. In both Type 1 and Type 2 reports, the auditor provides an opinion on whether the management's description of the service organization's systems is fairly presented. Both types of reports provide opinions on whether the controls included in the description are suitably designed to meet the applicable Trust Service criteria. Type 2 reports includes an additional opinion on whether the controls are operating effectively.

2.3.1.1 ADDITIONAL COMPLIANCE REQUIREMENTS

SOC 2 and SOC 3 reports are intended for a broad range of users and provide assurance with regards to the trust service principles of security, availability, processing integrity, confidentiality, and privacy. While this might be sufficient for most organizations, some may require assurance for controls related to additional areas. For example, organizations in the financial, government, and health sectors have to comply to different (and often multiple) control frameworks. This may be required to meet specific regulations or industry sector requirements. The SOC 2 trust services and associated criteria might

[12] Information on Trust Services and Information Integrity can be found at AICPA.org (English only)

[13] Note that a SOC 2 examination is a pre-requisite to the completion of a SOC 3 report.

not map directly to controls in other control frameworks.[14] This means a larger effort for your organization and your CSP to address additional requests for information, prepare additional assurance reports, and review against multiple compliance requirements. This larger effort can lead to increased costs and risks of non-compliance due to the complexity of reviewing information from a variety of reports.

To help address these challenges, service organizations can request third-party auditors to perform a SOC 2 examination that addresses additional subject matters and criteria.[15] This is commonly referred to as a SOC 2+ examination. For example, a service provider may include NIST 800-53 or the CSA CCM as additional criteria. The control overlap between each framework has the potential to save time and money.

We recommend that your organization contact its CSP to ask about the availability of SOC 2+ reports for addressing any additional requirements. When available, a SOC 2+ report can help facilitate CSP assessment activities. When not available, your organization may have to request multiple assurance reports to certify all its compliance and assurance requirements are addressed by the service provider.

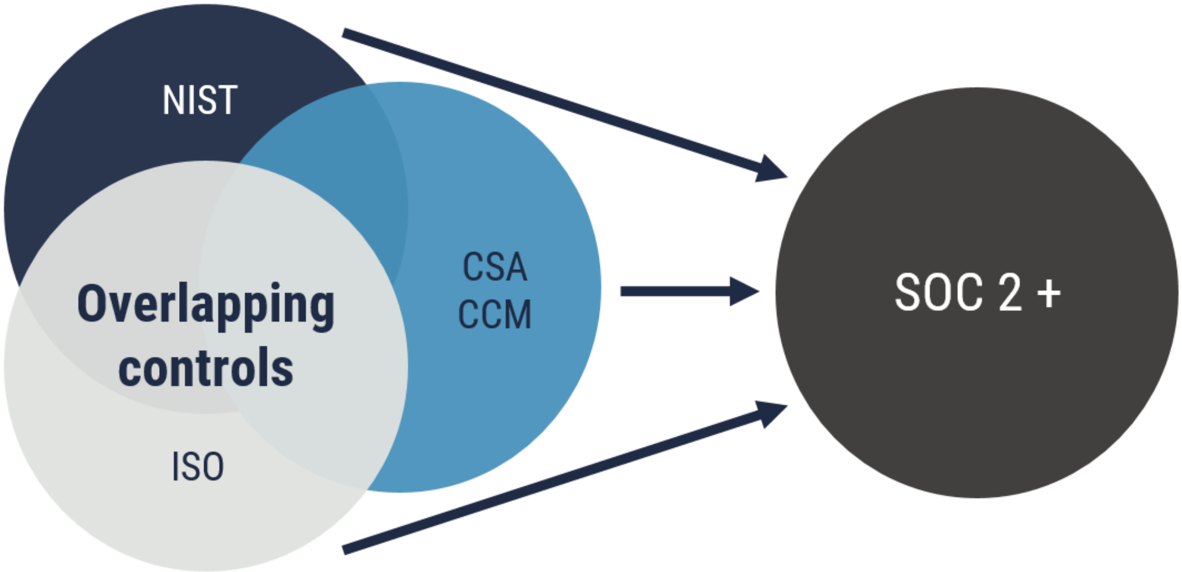


Figure 3: **SOC 2 vs SOC2 + examination of controls from multiple control framework**

[14] Trust Services Criteria (TSC) mappings to various frameworks can be found at AICPA.org. (English only)
[15] Additional subject matter on SOC 2+ can be found at AICPA.org. (English only)

2.3.1.2 REVIEW OF SOC REPORTS

We recommend that your organization determine which SOC reports it requires (either SOC 1, 2, 3). In cloud computing, a SOC 2 type 2 report is generally recommended due to the increased level of assurance that it provides. SOC 3 reports are not recommended as they do not provide enough details and do not contain sufficient information to perform an adequate assessment of the CSP.

It is possible that CSPs rely on a subservice organization for delivery of its own service. For example, a CSP providing Software as a Service (SaaS) may rely on a different CSP providing Infrastructure as a Service (IaaS). Your organization should review the SOC report to determine if your CSP relies on a subservice organization and verify that all relevant controls of the subservice organization are included in the SOC report. If not, your organization should request additional information or request a copy of the subservice organization SOC report.

We recommend that your organization review the scope of the report to ensure it covers applicable and relevant cloud hosting locations, dates, timeframes, CSP cloud services, and trust services principles. Your organization should request SOC 2 type 2 reports that include the trust service principles of security, availability, processing integrity, and confidentiality for assessment of CSPs. Organizations may require the privacy trust service principle if they have privacy requirements.

Once confirmed that the appropriate report has been provided, your organization should review key areas of the report including the auditor opinion, the complementary end user controls (CEUC) section, and any identified testing exceptions.

We suggest that your organization review the SOC report for unmodified, qualified, disclaimer, and negative opinions. Unmodified opinion means that the auditor fully supports the management assertion. A qualified opinion is a statement by the auditor to identify a scope limitation or the existence of significant control exceptions. Your organization should look for qualified opinions to determine how relevant an identified control weakness is to your organization. If the control weakness is relevant, your organization should determine the impact it could have and whether the risks are mitigated. Note that not all exceptions result in a qualified opinion. As such, your organization should review any testing exceptions identified by the auditor to determine if they are of concern. Disclaimers are included in SOC reports when an auditor cannot express an opinion, (e.g. there was not enough information provided or available). A negative auditor opinion reflects more serious issues. We advise your organization to discuss negative auditor opinions with its CSP before using any cloud service from that particular CSP.

CUEC are controls that the CSP has identified as necessary for your organization to have in place for the trust service principles to be met. Your organization must determine if any CUECs are applicable, and if so, verify that its controls address the CSP’s recommendations.

2.3.2 ISO 27001, 27017, AND 27018

The ISO 27001 [7] standard provides a best practice framework for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). ISO 27001 [7] lets your organization have confidence in a CSP's security governance and management of risk. A CSP holding an ISO 27001 [7] certification must:

- Examine your organization's information security risks (taking account of the threats, vulnerabilities, and impacts).
- Address risks that are deemed unacceptable by designing and implementing information security controls (or other forms of risk treatment such as risk avoidance or risk transfer).
- Adopt a management process to ensure that the information security controls continue to meet your organization's information security needs on a present and ongoing basis.

ISO 27001 [7] relies on detailed guidelines in ISO 27002 [8] for control implementation and includes a list of mandatory and optional controls. All mandatory controls must be met before your organization is awarded the certification. Optional controls can be found in Annex A, of the ISO standard and are selected based on a risk assessment. The selected controls are documented in a statement of applicability.

While the ISO 27001 [7] standard provides a best practice framework for an ISMS, two codes of practice were developed to provide guidance on security and privacy in cloud computing. These codes include:

- ISO 270017 [9] code of practice for information security controls based on ISO/IEC 27002 for cloud services.
- ISO 27018 [10] code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

ISO 27017 provides cloud specific guidance to CSPs on implementing controls in ISO 27002 [8], and introduces new controls specific to cloud computing. ISO 27018 [10] provides CSPs with necessary guidance to protect PII entrusted to them.

2.3.2.1 REVIEW OF ISO CERTIFICATION AND REPORT

Upon successful completion of an ISO 27001 [7] audit, the CSP will receive a certificate. The certificate is generally made available to your organization, and includes the following:

- name of the service organization;
- date of issue;
- date of expiration;
- ISMS scope;
- in-scope locations; and
- certification standard.

Your organization should review the scope of the ISO 27001 [7] certificate to ensure that it covers applicable and relevant cloud hosting locations, timeframes, and CSP cloud services.

While a report is delivered at the end of an ISO 27001 [7] audit, this report is meant for internal use and may not be made available for your organization to review. If the ISO 27001 [7] report is made available by the CSP, it normally includes the same information found in the certificate, in addition to the list of audit participants and evidence details. When available for review, your organization should confirm that the scope of the ISO 27001 [7] report covers applicable and relevant cloud hosting locations, timeframes, and CSP cloud services.

When an ISO report is made available for review, your organization should confirm that the report concludes with a recommended status. A status of recommended means that no non-conformities were identified.

Non-conformities (both minor and major) can arise when the CSP does not meet a requirement of the ISO standard, has undocumented practices, or does not abide by its own documented policies and procedures. Minor non-conformities generally result in a **recommended upon action plan development** status. In such a case, the service organization must prepare an action plan to resolve the audit findings. Upon receipt of the action plan, the auditor may proceed to recommend the certification of the ISMS.

Major non-conformities (or too many minor nonconformities), such as a failure to meet mandatory control objectives, leads to a **not recommended** status. The service organization must resolve the findings before proceeding further with the certification activities.

2.3.3 SECURITY TRUST AND ASSURANCE PROGRAM

The CSA Security Trust and Assurance Registry (STAR) is a cloud security assurance program encompassing key principles of transparency, rigorous auditing, and harmonization of standards. The registry is publicly accessible and helps your organization in assessing CSPs.

The CSA STAR program consist in three levels of assurance:

- Level 1 – Self-assessment;
- Level 2 - Third-party certification or attestation; and
- Level 3 - Continuous auditing (currently in development).

The STAR assessments are based on the CSA Cloud Controls Matrix (CCM) and the CSA Consensus Assessments Initiative Questionnaire (CAIQ). The CCM consists of a controls framework that assists in assessing the risk associated with a CSP. The controls framework covers fundamental security principles across the following 16 domains:

- Application and interface security;
- Audit assurance and compliance;
- Business continuity management and operational resilience;
- Change control and configuration management;
- Data centre processes and operations;
- Data security and information lifecycle management;
- Encryption and key management;
- Governance and risk management;
- Human resources;
- Identity and access management;
- Infrastructure and virtualization security;

- Interoperability and portability;
- Mobile security;
- Security incident management, e-discovery, and cloud forensics;
- Supply chain management, transparency, and accountability; and
- Threat and vulnerability management.

The CAIQ is a set of nearly 300 questions based on the CCM. The questionnaire can be used by your organization in its assessment of its CSP. It can be used as a first level filter during procurement of cloud services. As depicted in Figure 4, CSA STAR provides an increasing level of assurance and transparency with each assessment level.

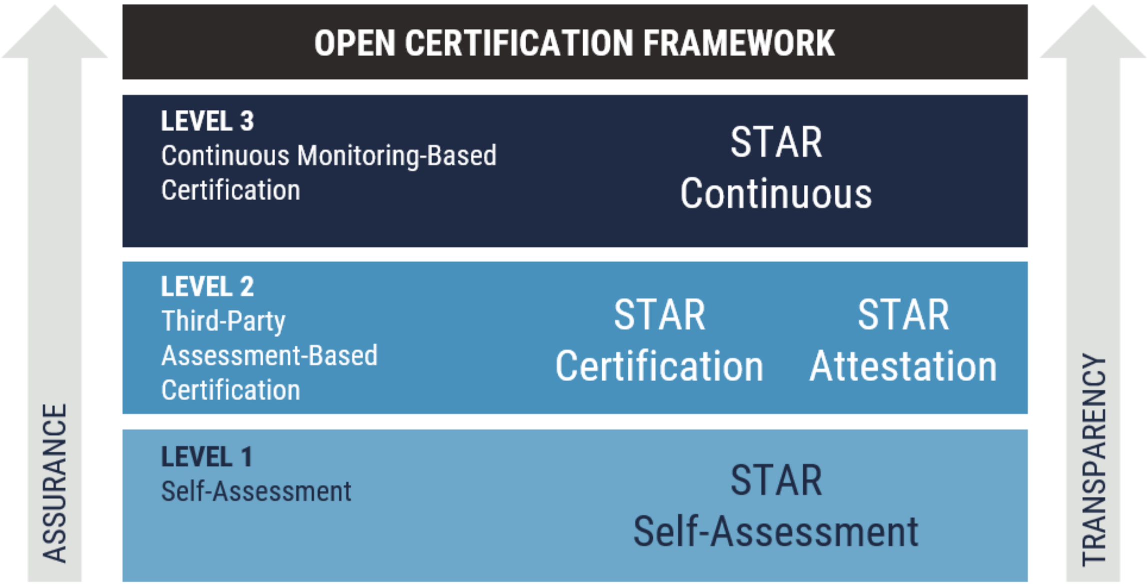


Figure 4: **CSA Open Certification Framework**

CSA STAR Level 1 is a self-assessment which CSPs can use to document the security controls provided by their cloud service offerings. In a Level 1 self-assessment, the CSP completes a CAIQ. The CAIQ must be updated yearly or when the CSP introduces significant changes to its cloud services and controls. While your organization can use a Level 1 self-assessment for a high-level screening of CSPs, we recommend using a more in-depth verification by an independent third-party.

If your organization is looking for an independent third-party assessment of their CSP, it should require CSA Level 2 assessments. There are three types of CSA STAR Level 2 claims:

- **CSA STAR *Level 2* attestations** are based on SOC 2 attestations and are supplemented by the criteria found in the CCM.[16]

[16] More information on STAR attestations can be found on the Cloud Security Alliance website. (English only)

- **CSA STAR *Level 2* certifications** leverage requirements from both the ISO/IEC 27001:2013 standard for security management and the CCM.[17]
- **CSA C-STAR *Level 2* assessments** are independent third-party security assessments of a cloud service provider for the Greater China market. CSA C-STAR Level 2 assessments are not covered in this guidance.

Level 2 attestations must be performed by a CPA firm, while Level 2 certifications must be performed by a CSA-accredited certification body.

CSA STAR Level 2 attestations enhance SOC 2 attestations by reporting on the suitability of the design and operating effectiveness of a CSP's controls in meeting criteria from the 16 CSA CCM security domains. The CSA STAR Level 2 attestation report follows the same structure and format as a SOC 2 report.[18]

CSA STAR Level 2 certifications enhance ISO 27001 certifications by assigning a management capability score to each of the CCM security domains. Each domain is scored on a specific maturity level and is measured against five management principles, including:

- communication and stakeholder engagement;
- policies, plans and procedures, and a systematic approach;
- skills and expertise;
- ownership, leadership, and management; and
- monitoring and measuring.

The average maturity level for each CCM security domain provides an overall maturity score[19]. The resulting maturity level is used to designate the certification award as bronze, silver or gold in the certification report to the CSP. Similar to ISO 27001, the resulting deliverable is a certificate.

2.3.3.1 REVIEW OF CSA STAR CERTIFICATE AND REPORT

When reviewing a CSA STAR Level 2 attestation report, your organization should follow the guidance provided in section 2.2.1.1 for SOC 2 attestations. The only added element is that the STAR attestation should also report on the suitability of the design and operating effectiveness of a CSP's controls, in meeting the criteria from the 16 security domains of the CSA CCM.

After successfully completing a CSA STAR Level 2 certification, a certificate will be delivered to the CSP. Similar to a 27001 certification, a report is not provided for review by cloud consumer organizations. Note that, although the maturity level achieved is included in the STAR certification report to the CSP, it is not included on the certificate.[20]

[17] More information on STAR certifications can be found on the Cloud Security Alliance website. (English only)
[18] The CSA STAR level 2 attestation is a good example of a SOC2+ examination report described in section 2.3.1.1.
[19] A detailed description of maturity score determination is provided in this pdf from the Cloud Security Alliance. (English only)
[20] Information on third-party assessors can be found on the FedRamp website [11]. (English only)

2.3.4 FEDERAL RISK AND AUTHORIZATION MANAGEMENT PROGRAM

The Federal Risk and Authorization Management Program (FedRAMP) is a US government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. Once authorized under this program, CSPs can provide services for US government agencies. Under FedRAMP, accredited Third-Party Assessment Organizations (3PAOs) perform the initial and periodic assessments of cloud systems to ensure they meet FedRAMP security requirements as part of a CSP's FedRAMP authorization.

Although FedRAMP assessments will never cover CSP service implementation and operation outside of the United States, the FedRAMP System Security Plan (SSP) aligns well with the Cyber Centre cloud control profiles, and can provide valuable insight on CSP implementation and operation of controls. When available, your organization can review the FedRAMP SSP to better understand the CSP implementation of controls and guide discussions with CSPs during the assessment.

For CSP services in Canada, FedRAMP can be used to supplement the information available via SOC, ISO and CSA STAR to better understand CSP implementation and operation of controls. It should not be the only third-party assessment used to evaluate CSPs.

3 ASSESS CONTROLS IMPLEMENTED BY THE CSP

As identified in ITSM.50.062 [1], your organization does not always have control or visibility into the design, installation, and assessment of the CSP's security controls. An alternative security assessment approach needs to be applied by considering other trusted security assessments.

In the context of the cloud security risk management, these trusted security assessments mainly consist of third-party attestations that have more value than self-assessments. Common third-party attestations cover various regulations and industry requirements.[21]

These attestations require an independent third-party that is objective and applies professional standards to the evidence it reviews and produces. However, third-party attestations rarely cover all security requirements identified in the selected security control profile. Additional security requirements and contract clauses may need to be included to ensure that your CSP provides the required evidence to support the security assessment activities.

Formal third-party attestations often require your organization to have non-disclosure agreements (NDA). These NDAs represent specific, point-in-time, assessments of the security controls and represent specific cloud provider services. It is important for your organization to monitor for any changes in coverage, status, and findings over time.

3.1 CSP ASSESSMENT COMMITTEE

The CSP assessment committee is a multifaceted team composed of a security assessor, a cloud security architect, an IT practitioner, and a compliance officer. This committee is responsible for overseeing the CSP assessment process.

3.2 PROCESS

Before a security assessment of cloud services can be completed, your organization must complete the following actions:

- Confirm or establish an NDA between your organization and the CSP being assessed;
- Determine the target security categorization;
- Select the cloud service model and cloud security control profile[22] ; and
- Procure current and relevant independent third-party reports from the CSP (for the services being assessed).

[21] Industry regulations and requirements such as Payment Card Industry Data Security Standard (PCI DSS), Service Organization Control (SOC) 1&2, Health Insurance Portability and Accountability Act (HIPAA), Cloud Security Alliance (CSA) Security Trust and Assurance Registry (STAR) and the International Organization for Standardization (ISO 27001, 27017, and 27018).

[22] *ITSP.50.103* [6] recommends an approach to the security categorization of business process and information assets, the selection of the cloud service model, and the selection of the security control profile.

As shown in Figure 5, the CSP cloud services security assessment will be conducted in the following five phases:

- Determination of current and applicable third-party reports, attestations, certifications, and other information;
- Confirmation of attestation scope and period;
- Evaluation and review of detailed evidence;
- Preparation of CSP assessment report; and
- Performance of continuous monitoring.

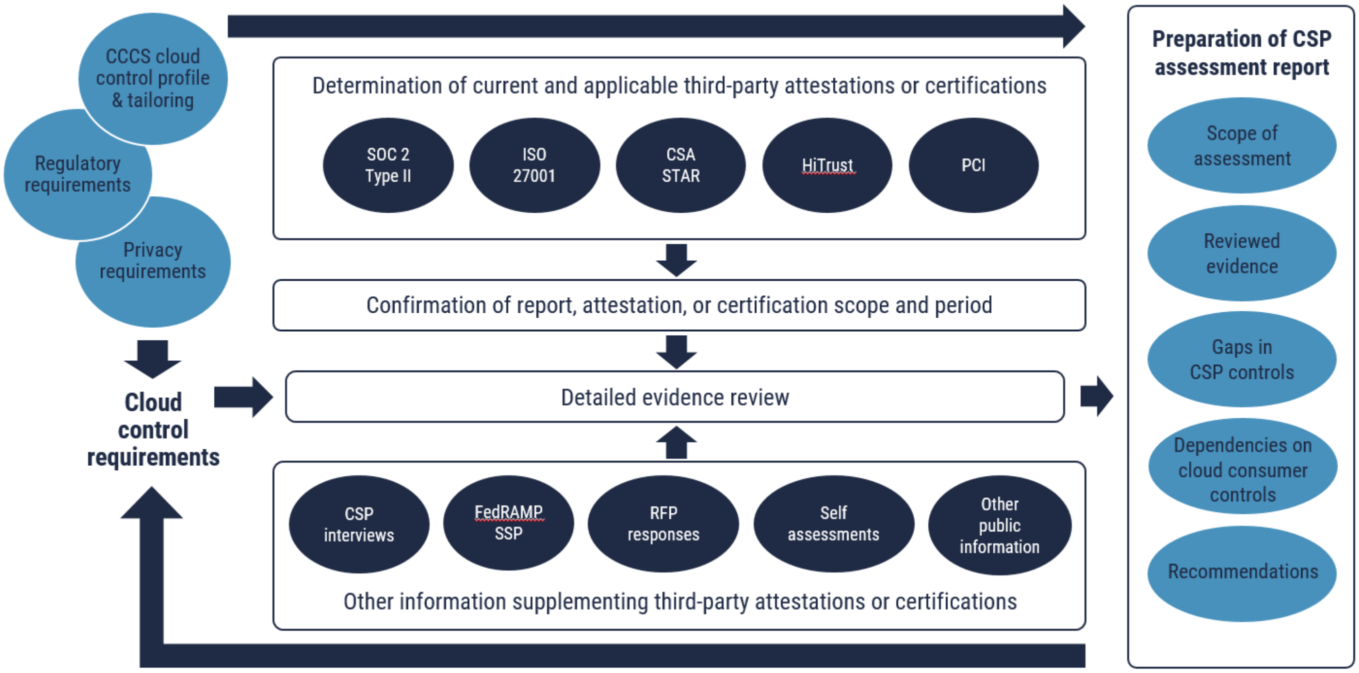

CCCS cloud control profile & tailoring
Regulatory requirements
Privacy requirements
Cloud control requirements
Determination of current and applicable third-party attestations or certifications
SOC 2 Type II
ISO 27001
CSA STAR
HiTrust
PCI
Confirmation of report, attestation, or certification scope and period
Detailed evidence review
CSP interviews
FedRAMP SSP
RFP responses
Self assessments
Other public information
Other information supplementing third-party attestations or certifications
Preparation of CSP assessment report
Scope of assessment
Reviewed evidence
Gaps in CSP controls
Dependencies on cloud consumer controls
Recommendations

Figure 5: **CSP cloud services security assessment**

3.2.1 DETERMINE REQUIRED INDEPENDENT THIRD-PARTY REPORTS AND OTHER INFORMATION

The Cyber Centre cloud security control profiles represent the baseline controls for protecting your organization's business activities. In many cases, it is necessary to tailor the cloud security control profile to address unique threats, technical limitations, business requirements, legislation, policies, or regulations. We recommend that your organization ensures it identifies all compliance obligations and cloud control requirements to determine which independent third-party reports, attestations, or certifications are required to perform a security assessment of the CSP cloud services. Each compliance or control requirement should be addressed by one or more third-party reports. As shown in Figure 6, the Cyber Centre recommends that your organization consider supplementing third-party assessments with other information if the third-party reports do not cover all control requirements. This supplementary information can include responses to CSP interviews, self-assessments, system security plans, request for proposals(RFP) responses, and other public information. Many CSPs have additional information (relevant to the assessment activities) and consolidated reports available on portals, which can be directly accessed by your organization.

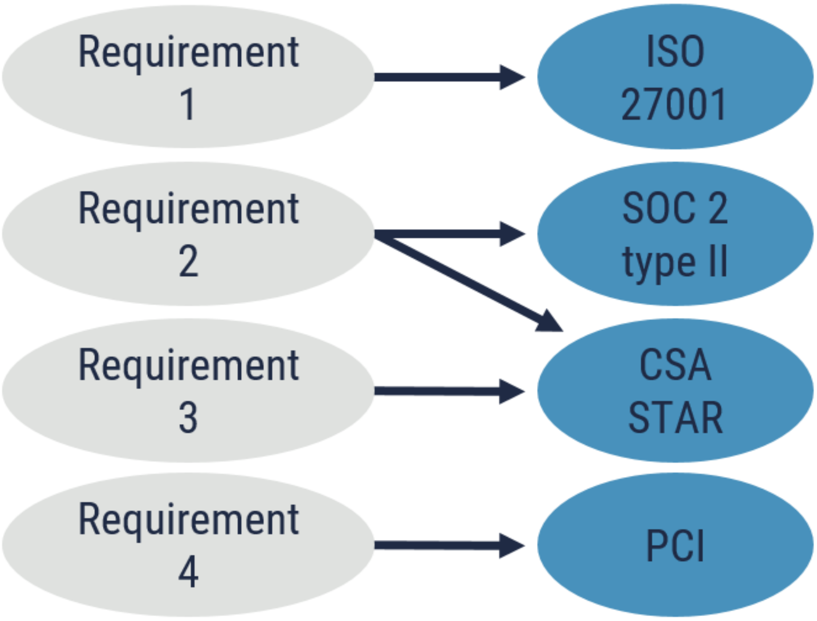


Figure 6: **Determination of required third-party reports, attestations, or certifications**

3.2.1.1 CONFIRM ATTESTATION SCOPE AND TIME PERIOD

Information contained in a third-party attestation or certification reports differs depending on the CSP location. For example, CSPs located in the United States may have significantly different configurations compared to those in other parts of the world (including Canada). Before proceeding to a detailed review of the evidence provided by the CSP, we recommend that your organization review the scope of the assessment to ensure it covers applicable and relevant cloud hosting locations, dates, time periods, CSP cloud features, services, and security controls. This information is available on the third-party report, attestation or certification. Your organization should work with its cloud provider to determine the appropriateness of other sources of information.

Cloud services evolve quickly and it is possible that new regions, cloud services, and features may not be covered by current reports. Generally, those new services will be included in the CSP's next audit cycle. While your organization can assess these new services (through self-assessments, CSP interviews and other information), it must realize that this approach does not provide the same level of assurance as a third-party assessment. This approach should be avoided when such cloud services or features are required to support and secure critical business services and information.

3.3 DETAILED EVIDENCE REVIEW

When your organization is sure it has current and applicable information to perform a detailed evidence review, it must examine the information to identify evidence for each control requirement. For this task, your organization should select security assessors with experience in cloud computing and the use of pass-through third-party assessments.
A detailed evidence review will determine if the following conditions are met:

- The security control and enhancement requirements (as defined by the selected Cyber Centre cloud control profile) have been met.
- The documentation provides enough assurance of appropriate security design, operation, and maintenance of the CSP cloud services.

The assessor should pay particular attention to the control assignments when determining if the security controls and enhancements are met.[23] For example, some control assignments may be important to meet policies, laws, regulations, and organizational risk tolerance.[24]

We recommend that your organization analyze the gathered evidence, and identify any control gaps and concerns that relate to:

- the security of the underlying cloud fabric;
- the isolation of the cloud fabric from the CSP network and systems;
- the isolation of the cloud tenants from each other;
- the security of the management plane; and
- the security of interfaces and application program interfaces (API).

Your organization needs to understand how the CSP and consumer incident response practices and points of contact will interface and where there may be problems. Your organization may want to discuss any identified gaps or concerns with its CSP before including them in an assessment report. When the CSP provided details are not sufficient, your organization should create and collect its own details to support the assessment activities. This could include information from RFP responses, interviews with other CSPs, public information, and CSP system security plans.

[23] For some security controls in the control profile, your organization is provided with the flexibility to tailor the controls using assignments and selection statements. The Cyber Centre control profiles defined in ITSP.50.103 [6] identifies assignments and selection statements by enclosing them by brackets.

[24] Initial draft NIST *Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations* [12].

CSPs often identify policies, practices, services, or configurations that are necessary for your organization to have in place for the security of the cloud service. By reviewing the provided evidence, your organization should determine if these controls are applicable, and if so, verify it has controls in place to satisfy the recommended cloud consumer controls.

The detailed evidence review may also help your organization identify any additional contractual terms that should be included in the procurement documentation.

3.3.1 PREPARE CSP ASSESSMENT REPORT

A CSP security assessment report is produced at the end of the CSP security assessment. The report contains the following:

- Description of the CSP that was assessed.
- Description of the assessment committee’s participants and roles.
- Description of the security category, cloud service, and deployment model.
- Description of the control requirements.
- Description of the assessment’s scope, including locations and cloud services.
- Description of the documents reviewed, and period they covered.
- Description of the gaps identified in CSP security controls.
- Description of the necessary policies, practices, services, or configurations needed by your organization to ensure the security of the cloud services.
- Description of any recommended terms that should be included in the procurement contract.
- Summary of the resulting residual risks and recommendations.

The security assessor should provide recommendations to your organization if gaps in the CSP security control implementation have been identified. Possible recommendations include:

- filling gaps with their own controls;
- accepting the residual risks; and
- selecting a different CSP.

Note that it is easier for your organization to fill gaps in its own controls in an IaaS situation than with SaaS.

3.3.2 CONTINUOUS MONITORING

Third-party reports, attestations, or certifications generally cover the assessment of security controls for a specific period of time. To assure that your CSP is committed to continually protecting your information systems (in line with the security control profiles under which they were assessed), your organization should:

- require continuous coverage of third-party assessments in cloud contracts (typically yearly);
- require your CSP provide periodic evidence of continuous coverage (including certification, assessment reports, and attestations); and
- analyze the gathered evidence to identify any gaps or concerns in the controls.

CSPs generally make periodic assessments available to their clients. The scope of these assessments often include any cloud services that have been released by the CSP since the last assessment period.

The CSA is currently developing the CSA STAR Level 3 program. This new program will provide continuous auditing and assessment of relevant security properties. Once available, your organization may want to determine the benefits and feasibility of using this new assurance level to support its continuous monitoring program.

3.3.3 STACK ASSESSMENTS

Many cloud systems rely on other cloud providers to offer a comprehensive set of services for the end customer. For example, a software provider may use an infrastructure provider to deliver a SaaS offering. In this case, the software provider will inherit security controls from the infrastructure provider.

As illustrated in Figure 7, the cloud security risk management approach allows for the stacking of assessments like building blocks. In this model, the assessment for each cloud system must only cover the implementation of that specific system. For example, a SaaS service provider would not specify in its own documentation, implementation details, or evidence related to the infrastructure service that it leverages. This reduces the number of attestations or security assessments, eliminates redundancy across authorization packages, and keeps assessments delineated by information system boundaries.

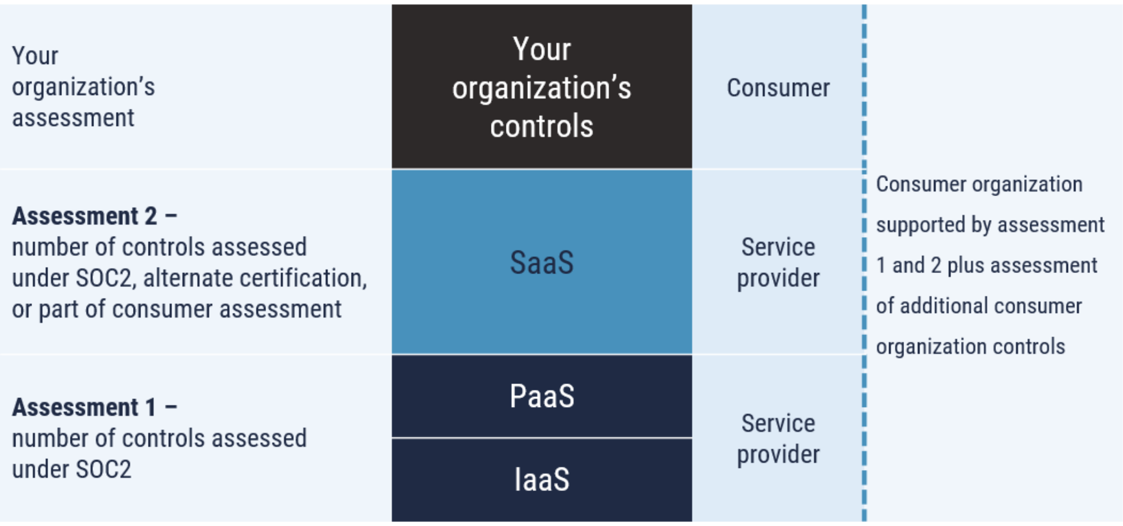

Your organization's assessment
Your organization's controls
Consumer
Assessment 2 – number of controls assessed under SOC2, alternate certification, or part of consumer assessment
SaaS
Service provider
Consumer organization supported by assessment 1 and 2 plus assessment of additional consumer organization controls
Assessment 1 – number of controls assessed under SOC2
PaaS
IaaS
Service provider

Figure 7: **Assessment stacking**

4 ASSESS CONTROLS IMPLEMENTED BY YOUR ORGANIZATION

4.1 CLOUD-SPECIFIC CONSIDERATIONS

Your organization needs to understand the differences between cloud and traditional infrastructure and adapt its security architecture and security controls accordingly. Understanding the differences will greatly assist your organization in its assessment activities. The Cyber Centre's *ITSP.50.104 Guidance on Defence in Depth for Cloud-Based Services* [13] should be reviewed by security assessors to better understand key security differences and considerations for cloud-based computing. Annex A of this document maps key cloud security considerations identified in ITSP.50.104 [13], to the controls found in the Cyber Centre profile. This mapping provides the assessor with guidance on important aspects to consider when assessing each control area.

The controls used in the cloud by your organization will vary based on the cloud service model. The Cyber Centre control profiles described in section 2.1 identify which controls are applicable to each service deployment model. While your organization is responsible for direct assessment of more components and controls in the IaaS model, many controls must be assessed directly by your organization in the PaaS or SaaS models. For example, most PaaS and SaaS offerings will provide key security features, capabilities, and options that must be enabled by configuration settings. This includes features such as encryption, logging, authentication, network access control, and location. Implementing IaaS security controls is similar from one CSP to another. However, PaaS and SaaS security configurations vary greatly from one CSP to another. Awareness of these differences helps the security assessor in their assessment activities.

4.2 OTHER ASSESSMENT CONSIDERATIONS

4.2.1 AUTOMATION

Traditional security assessments generally rely upon manual review of evidence and artefacts to validate that the required controls have been addressed in the design, have been correctly implemented, and are operated effectively. This manual process requires a lot of effort, is time consuming, and does not align well with the agility of the cloud environment.

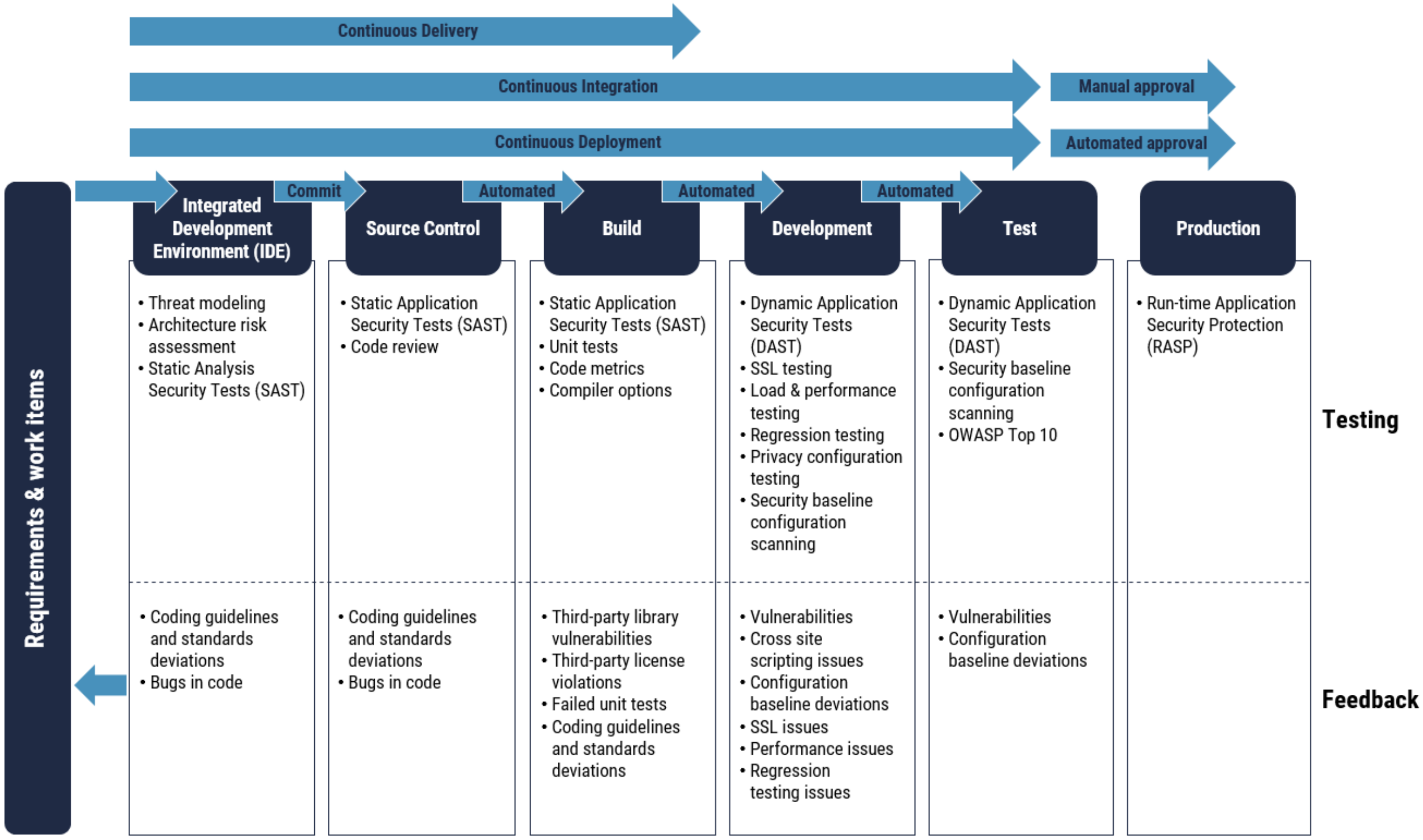
Modern cloud platforms offer many automation tools, templates, and scripting languages that can be used for enforcement and reporting on security baseline configurations. This means less effort is spent on conducting compliance enforcement, ensuring consistent configurations and achieving fewer configuration errors. This approach provides a repeatable security assessment which allows security practitioners to concentrate on less automatable aspects of their job.

4.2.2 DEVSECOPS

To stay competitive, CSPs must be able to deliver new products and features continuously, and in shorter cycles. DevOps combines software development (Dev) and IT operations (Ops) with the goal of improving the collaboration, rapid delivery, and security aspects of a software development workflow. DevSecOps extends the DevOps workflow by incorporating automated security tasks and processes using various security tools. According to devsecops.org, the purpose and intent of DevSecOps is to build on the mindset that "**everyone is responsible for security**", with the goal of safely distributing security decisions at speed and scale to those who hold the highest level of context without sacrificing the safety required.

The DevSecOps practice relies on incorporating automated security services in the continuous integration (CI) and continuous delivery (CD) models. With CI, developers merge changes into a central repository (on a daily basis). Frequently checking code (after completion of small changes) helps to catch bugs and security flaws early in the development process. Changes committed to the central repository trigger automated build and unit testing processes. CD builds on constant integration by deploying multiple testing or staging environments and testing additional aspects of the builds. By automating security testing as part of the CI/CD pipeline, your organization can identify security flaws and deviations from security best practices, standards, and security controls. Figure 8 describes typical security assessment activities that can be automated as part of this build and testing process.

Automated security testing (as part of the CI/CD pipeline) helps avoid errors from manual assessment activities, ensures security assessment tasks are performed on a continuous basis, and decreases the amount of time needed to identify issues and get authorization to operate (ATO).



	Integrated Development Environment (IDE)	Source Control	Build	Development	Test	Production
Testing	• Threat modeling • Architecture risk assessment • Static Analysis Security Tests (SAST)	• Static Application Security Tests (SAST) • Code review	• Static Application Security Tests (SAST) • Unit tests • Code metrics • Compiler options	• Dynamic Application Security Tests (DAST) • SSL testing • Load & performance testing • Regression testing • Privacy configuration testing • Security baseline configuration scanning	• Dynamic Application Security Tests (DAST) • Security baseline configuration scanning • OWASP Top 10	• Run-time Application Security Protection (RASP)
Feedback	• Coding guidelines and standards deviations • Bugs in code	• Coding guidelines and standards deviations • Bugs in code	• Third-party library vulnerabilities • Third-party license violations • Failed unit tests • Coding guidelines and standards deviations	• Vulnerabilities • Cross site scripting issues • Configuration baseline deviations • SSL issues • Performance issues • Regression testing issues	• Vulnerabilities • Configuration baseline deviations	

Figure 8: **Typical automated security assessment activities**

4.2.3 VULNERABILITY ASSESSMENTS

Your organization is frequently required to perform technical vulnerability assessments of its controls using a variety of scanning tools. We recommend that your organization ensure that such scanning activities are performed as per the terms of service with its CSP. Your organization may require notification and authorization from its CSPs before beginning such activities. Notification and authorization allows your organization's CSP to distinguish between a legitimate assessment and an attack.

4.2.4 BETA OR PREVIEW CLOUD SERVICES

The services and capabilities provided by cloud platforms evolve rapidly. Many service providers allow cloud consumers to sign-up for use of beta or preview versions of new cloud services that they are developing. Access to beta or preview services allow your organization to evaluate how new CSP offerings meet its future cloud-based service needs. Access also allows your organization to offer feedback to its CSPs on areas that need improvement. We recommend that your organization monitor its cloud service to ensure that beta or preview cloud services are never used for production workloads. Restrictions should be included in your organization's cloud security policy to address this if not already in place.

Beta or preview versions of cloud services are:

- Covered by different terms of service and service level agreements (SLA);
- Provided with no security compliance and no privacy commitments; and
- Can be terminated at any time.

Security assessors should verify that no beta or preview cloud services are used for production workloads when assessing the security of your organization's implemented cloud workloads.

4.3 PROCESS DESCRIPTION

4.3.1 ASSESS CONTROLS IMPLEMENTED BY YOUR ORGANIZATION

Your organization is responsible for assessing the security controls allocated to it in its selected cloud profiles. As described in section 2.1, the scope of cloud profiles includes all CSP and organizational components used to provide and consume the cloud-based service.

We recommend that your organization conduct security assessment activities when implementing cloud-based services. These security assessment activities should be conducted as part of the system development life cycle (SDLC) process and should be automated as part of a DevSecOps model described in section 4.2.2.

Automated testing is an integral part of the security assessment plan. Using automated tools and scripts can help your organization identify the following issues:

- Deviations in coding guidelines and standards;
- Bugs in code;
- Vulnerabilities in third-party libraries;
- Violations of configuration baselines and licenses;

- Issues in encryption protocol; and
- Compliance problems.

This approach reduces the effort, the costs, and the time spent on fixing and assessing security flaws.

Your organization can further simplify its security assessment of cloud-based services by pre-approving and reusing the following items:

- Security design patterns;
- Compliance templates;
- Disk images;
- Scripts; and
- Documentation that describes the implementation of controls.

By reusing pre-approved design patterns, architectures, and solutions, your organization will inherit controls that have already been assessed and will be able to focus its assessment effort on controls that are specific to each cloud-based service.

4.3.2 AUTHORIZE OPERATION OF CLOUD-BASED SERVICES

Authorization is the ongoing process of obtaining and maintaining official management decisions by a senior organizational official for the operation of an information system. Through authorization, the authorizer clearly accepts the risk of relying on the information system to support a set of business activities based on the implementation of an agreed-upon set of security controls and the results of continuous security assessments.

When granting an authorization, a consumer organization must authorize the use of the entire cloud-based service, which consists of both the CSP cloud services and the consumer organization service hosted on these cloud services. To that end, the results of the security assessments on the CSP cloud service and the consumer cloud service are key parts of the documentation package that authorizing officials need to determine whether they should authorize operations of the cloud-based service and accept residual risks.

4.3.2.1 DEFINE AND DOCUMENT REQUIRED MITIGATION ACTIVITIES

Findings in a security assessment help to identify gaps and develop fixes. It is important to consider the business and risk context of any gaps found (all services are likely to have deficiencies) to determine which ones could clearly cause harm to your organization. From the resulting analysis, a plan of action and milestones (PoAM) is created that addresses how your CSP and your organization will correct or mitigate any of the deficiencies within an agreed upon timeline. This information must be incorporated in the authorization package. In the DevSecOps model, the status of security controls is updated each time automated tests are run as part of the CI/CD pipeline. Feedback and output from automated test tools can be used as input to generate the PoAM.

4.3.2.2 ASSEMBLE AND SUBMIT AUTHORIZATION PACKAGE

After preparing the PoAM, the project team assembles a final package and submits it for authorization review. This final package will include all documents created and referenced during the security assessment activities. These documents include additional authorization evidence reviewed for services, and components that were inherited by the new information system service. The authorizing official will review the authorization package and make a risk-based decision on whether or not to authorize the cloud-based service. The package will include an authorization letter for signature by the authorizing official.

In cloud environments, this process can be improved through the use of DevSecOps techniques. Security reports that were traditionally generated manually can be generated automatically each time security controls are tested. DevSecOps techniques decrease the amount of effort needed and the number of errors found to generate the required documentation for authorization. These techniques also support the continuous authorization of the information system.

4.3.2.3 GRANT AUTHORIZATION FOR OPERATING CLOUD-BASED SERVICES

Authorization documents are meant to detail and communicate the following specifics:

- Authorization decision;
- Conditions (if any) for operating cloud-based services in support of organizational business requirements;
- Required mitigation efforts (if any) and plans to achieve these (along with target dates); and
- Record of management's intent for the operating the service.

In the DevSecOps model, the security team works with the authorizers and the development and operation teams to define criteria that must be met as part of the CI/CD pipeline. This is done before the cloud-based services can be authorized for use in production. This allows for automation of the authorization function for some types of changes. Examples of authorization criteria that may be automated as part of the CI/CD pipeline include the following:

- All high and critical severity scan issues have been resolved;
- All high and critical severity bug fixes have been applied;
- All third-party library vulnerabilities and license issues have been resolved;
- All deviations from coding guidelines and standards have been addressed;
- All deviations from security baseline configuration have been addressed;
- All automated control verifications were successful; and
- No substantive changes were made to the cloud-based service[25].

[25] Substantive changes can include new external services, new encryption methods, changes to type of information stored (e.g. Personally identifiable information (PII)), changes to administrative functionality, and changes to the authentication or authorization approach.

4.3.3 CONTINUOUS MONITORING

The cloud security risk management approach extends beyond implementation by including activities for continuous monitoring during the operational phase of cloud-based services. The continuous monitoring approach defines how the security controls of cloud-based services are monitored over time, and how monitoring data is used to determine if these services are still operating within their authorization parameters. Continuous monitoring generally includes the periodic assessment of security controls (preferably automated)[26], the periodic review of security events and incident reports, and the periodic review of operation personnel security activities.

Through continuous monitoring, your organization will have the necessary capabilities to identify security deviations from the authorization state in both CSP and consumer organization components of cloud-based services.

Your organization needs to monitor the service operating on the cloud service as well as the infrastructure components that it uses to access and consume the service. Your organization then uses this monitoring data, in conjunction with the monitoring data provided by the CSP, for ongoing authorization decisions as part of its enterprise-wide risk management program.

By integrating security testing into the DevSecOps model, your organization can put in place the basis of a continuous monitoring program to support continuous risk management, security compliance and authorization of cloud-based services.

4.3.4 AUTHORIZATION MAINTENANCE

Through authorization maintenance, your organization has the necessary capabilities to react to deviations from the authorization state in a timely and effective manner. In line with ITSG-33 [2] guidance, when it is determined that cloud-based services are not operating within their authorization parameters, your organization should consider the following measures:

- Implementing temporary measures to protect the supported business activities;
- Updating implemented security controls to correct security deficiencies; and
- Accepting the new level of residual risk.

If the level of residual risk remains unacceptable after initial remedial actions, authorizers may choose to revoke the authority to operate pending further remedial action. The revocation of authorization would lead to additional security analysis activities to identify specific deficiencies within the operational context. This is followed by the application of corrective measures or improvements to the implemented security controls so that the cloud-based service can return to its authorized state.

In the context of supporting cloud services, the authorization maintenance process consists of activities where your organization must do the following:

- Review the security category of supported business activities periodically;
- Re-assess the threat environment and the security performance of technical environments;
- Review the results of security control performance assessments; and

[26] Continuous monitoring of CSP security control is covered in section 3.2.5 of this document.

- Review the activities of CSPs to ensure that they have adequately maintained the security posture of their information systems (according to the security provisions of their operations plans).

The outputs of authorization maintenance activities include updated residual risk assessments, updated plans of action and milestones, and updated security provisions of operations plans.

Automated DevSecOps practices improve the authorization maintenance process by identifying security issues and providing feedback from static and dynamic application security testing (DAST), infrastructure scanning, and other automated tests.

5 SUMMARY

The security assessment and authorization of cloud-based services requires your organization to apply strong security assessment and monitoring practices. This assures that the appropriate controls used by the different cloud actors are operating and functioning effectively. Security assessment and authorization requires your organization to evolve its risk management framework and adapt its security assessment and authorization to the realities of the cloud. We recommend that your organization leverage independent third-party audits, reporting frameworks, and certifications to assess CSP security controls, in addition to adopting automation and DevSecOps practices to truly benefit from cloud capabilities. Your organization can use this document to understand the security assessment and authorization considerations that are needed to support an effective cloud risk management process.

5.1 CONTACTS AND ASSISTANCE

For more information on security assessment and authorization for cloud-based services, please contact:

Cyber Centre Contact Centre
contact@cyber.gc.ca
613-949-7048

6 SUPPORTING CONTENT

6.1 LIST OF ABBREVIATIONS

Term	Definition
AICPA	American Institute of Certified Public Accountants
API	Application Program Interface
ATO	Authority to Operate
CCM	Cloud Control Matrix
Cyber Centre	Canadian Center for Cyber Security
CI/CD	Continuous Integration/Continuous Delivery
CPA	Certified Public Accountant
CSA	Cloud Security Alliance
CSE	Communications Security Establishment
CSP	Cloud Service Provider
DAST	Dynamic Application Security Testing
HIPAA	Health Insurance Portability and Accountability Act
IaaS	Infrastructure as a Service
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IT	Information Technology
NDA	Non-Disclosure Agreement
PCI DSS	Payment Card Industry Data Security Standard
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
RFP	Request for proposal
SaaS	Software as a service
SAST	Static application security testing
SOC	AICPA Service Organization Controls
SSAE	Statement on Standards for Attestation Engagements
SSP	System Security Plan
SPIN	Security Policy Implementation Notice
STAR	CSA Security Trust and Assurance Registry
TRA	Threat and Risk Assessment

6.2 GLOSSARY

Term	Definition
Cloud consumer organization	Any organization that wishes to acquire a CSP cloud service to implement a cloud-based service.
API	Put simply, an API is a go-between that takes in requests and tells a system what to do and then returns a response. Created using defined routines, protocols, and software building tools, an API makes interactions between data, applications, and devices possible.
CCM	Control framework developed to assist organizations assess the risk associated with a CSP. The controls framework covers fundamental security principles across 16 domains, including application and interface security, identity and access management, infrastructure and virtualization security, interoperability and portability, encryption and key management and data center operations.
CI/CD	Combined practices of continuous integration and continuous delivery.
DAST	Technologies designed to detect conditions indicative of a security vulnerability in an application in its running state. Most DAST solutions test only the exposed HTTP and HTML interfaces of web-enabled applications; however, some solutions are designed specifically for non-web protocol and data malformation (e.g. remote procedure call, session initiation protocol). [14]
DevOps	Software development methodology that combines software development (Dev) with information technology operations (Ops) to provide improved collaboration, rapid delivery and security.
DevSecOps	DevSecOps automates security assessment tasks by integrating security testing into the DevOps workflow.
FedRAMP	US government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. Once authorized under this program, a CSP can provide services for US government agencies.
SOC	Suite of service offerings CPAs may provide in connection with system-level controls of a service organization or entity-level controls of other organizations.
SAST	A set of technologies designed to analyze application source code, byte code and binaries for coding and design conditions that are indicative of security vulnerabilities. SAST solutions analyze an application from the “inside out” in a nonrunning state. [15]
STAR	Cloud Security Alliance security assurance program.

6.3 REFERENCES

Number	Reference
[1]	Canadian Centre for Cyber Security. *ITSM.50.062 Cloud Security Risk Management*. March 2019.
[2]	Canadian Centre for Cyber Security. *ITSG-33 IT Security Risk Management: A Lifecycle Approach*. December 2014.
[3]	Cloud Security Alliance. *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0. 2017.*
[4]	National Institute of Standards and Technology. *Special Publication 800-37, Revision 2*, *Risk Management Framework for Information Systems and Organizations--A System Life Cycle Approach for Security and Privacy.* December 2018.
[5]	Treasury Board of Canada Secretariat. *Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice (SPIN)*. November 2017.
[6]	Canadian Centre for Cyber Security. *ITSP.50.103 Guidance on Security Categorization of Cloud-Based Services*. 2020.
[7]	ISO/IEC 27001:2013 Information Technology - Security Techniques - Information Security Management Systems - Requirements
[8]	ISO/IEC 27002:2013 Information Technology - Security Techniques - Code of Practice for Information Security Controls
[9]	ISO/IEC 27017:2015 Information Technology - Security Techniques - Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Cloud Services
[10]	ISO/IEC 27018:2014 Information Technology - Security Techniques - Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors
[11]	United States FedRAMP website.nd.
[12]	National Institute of Standards and Technology. Initial public draft *Special Publication 800-53, Revision 5*, *Security and Privacy Controls for Information Systems and Organizations.* August 2017.
[13]	Canadian Centre for Cyber Security. *ITSP.50.104 Guidance on Defence-In-Depth for Cloud-Based Services.* 2020.
[14]	Gartner IT Glossary. https://www.gartner.com/it-glossary/dynamic-application-security-testing-dast
[15]	Gartner IT Glossary. https://www.gartner.com/it-glossary/static-application-security-testing-sast

Annex A

A.1 Implementing Security Controls in cloud Computing[27]

Type	Security consideration	Implementation example	Control mapping
Isolation			
4.1 – Isolation	Your organization should seek to increase the isolation between itself and its CSPs, and between itself and other organizational environments.	• storage encryption • dedicated VM instances instead of shared instances • hardware security modules (HSMs) for protection of keys and secrets	AC-4(21), SC-12, SC-12(2), SC-7, SC-12(3), SC-28(1)
Governance			
4.2.1 – Allocation of security resources	Your organization should appoint cloud leaders to direct cloud core teams that address the different aspects of the cloud transformation.	• cloud security and risk management process • procurement • licensing • roles and responsibilities	CM-4, PL-8, RA-3, SA-4, SA-1, SA-2, SA-9, SA-9(5), SA-12, CM-4
4.2.1 – Allocation of security resources	Senior management needs to communicate its support for cloud computing and encourage employees to develop their cloud computing and security skills.	• updates to information technology plans • updates to security policies • inclusion of cloud security in employees' development plans • cloud security training • on the job experimentation	PL-8, AT-1, AT-2, RA-3

[27] Summarized from *ITSP.50.104 Guidance on Defence-In-Depth for Cloud-Based Services*.

Type	Security consideration	Implementation example	Control mapping
4.2.2 – Establishment of policies and guidelines	Your organization should adapt its security policies to the reality of the cloud.	• acceptable use of cloud computing • acceptable cloud deployment and service models • roles and responsibilities • data residency • requirements for third-party assessments • contractual requirements • integration to identity management process • connectivity with external service providers • encryption and key management • data backup • service decommissioning	AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PS-1, RA-1, SA-1, SC-1, SI-1, AC-2, CA-2(3), RA-3, SA-9(5), MP-6
4.2.3 – Formal third-party assessments	Your organization should incorporate trusted third-party security assessments into its security assessment process.	• PCI DSS, SOC 1, SOC2, HIPAA, CSA STAR, ISO 27001, ISO 27017, and ISO 27018 • inclusion of additional security requirements and contract clauses	CA-1, CA-2, CA-2(3), PL-2, RA-3
4.2.4 – Cloud contracts	Your organization should leverage contracts to document and extend its governance to the cloud.	• CSP and cloud consumer responsibilities • service level agreements (SLA) • data ownership • data residency • requirement for third-party assessments • notification of security incident in an agreed to mechanism and time period • any other requirement or evidence required to address third-party assessment gaps	CA-1, CA-2, CA-2(3), CA-3, IR-4, IR-7(2), SA-9, SA-9(5)
Network Security			

Type	Security consideration	Implementation example	Control mapping
4.3.3 – Network segmentation and zoning	Your organization should understand the network segmentation methods available from its CSPs. Your organization should consider an **assume breach** security model and employ techniques such as micro-segmentation and software defined perimeter.	• configuration of subnets as public or private • provision cloud workloads and associated data in their own virtual network • provision dedicated instances of cloud services directly in cloud consumer virtual network • use cloud native security features to regulate traffic between segments (e.g. security groups) • use NVA such as firewalls and load balancers to regulate traffic between segments • regulate traffic based on tags or other attributes instead of IP addressing	AC-4, SC-7
4.3.4 – Routing	Your organizations should be aware of cloud routing considerations when designing and implementing its IaaS solutions.	• are routes required to be explicitly specified before traffic is permitted between source and destination subnets? • is routing between all subnets allowed by default within a virtual network? • is there a default route to the internet by default? • can virtual networks be provisioned without routes to internet? • how is connectivity to each subnet impacted when two virtual networks are peered together? • is a route required to force traffic to network virtual appliances?	AC-4, SC-7, SC-7(8)

Type	Security consideration	Implementation example	Control mapping
4.3.5 – Hybrid cloud networking	Your organization should ensure that adequate separation is in place to monitor and control traffic between on-premise networks to off-premise cloud environments.	• bastion or transit virtual networks • routing & access controls • firewalls, or network virtual appliances	AC-4, AC-17(3), CA-3(3), SC-7, SC-7(8)
Compute security			
4.4.2 – Compute workload security considerations	Your organization should adapt its security controls to each type of cloud workload and take advantage of cloud platform capabilities.	• leverage cloud platforms high availability features in their workload design • use multiple VMs for high availability • take advantage of cloud automation capabilities to enforce VM security baselines • leverage auto-scaling for improved availability • use agents that support auto-scaling • avoid agents not built for the cloud (possible performance issues) • notify CSPs prior to performing a vulnerability assessment ▪ capture logs externally (workloads can be dynamic and short-lived) • deploy VMs in approved CSP regions	AU-4(1), CM-2(2), ,PL-8, RA-5, SA-9(5)
4.4.3 – Image management	Your organization should seek to leverage auto-scaling and containers by using new approaches to image management	• frequent and automated image updates to apply security patch and malware signature to workload images • automated image security baseline enforcement during image creation • automated security testing during image creation • disabled logins and restricted services before image deployment	CM-2(2), CM-3(2), CM-3(3), CM-4, CM-5, CM-6(1), RA-5, SA-15, SA-15(7), SI-2, SI-3

Type	Security consideration	Implementation example	Control mapping
Data security			
4.5.3 – Data migration	Your organization should identify which data should be allowed to be migrated to the cloud, and ensure confidentiality and integrity of data is maintained throughout the migration.	• review of organization security policies, compliance requirements and categorization of business process and information assets • identification of compliance, legal, contractual and business constraints, data residency and location requirements, retention obligations, and security category of information assets • data back-up • encryption in transit • data protection in temporary and final storage destination	CP-9, RA-2, SA-9(5), SC-8, SC-8(1), SC-13, SC-28, SC-28(1)
4.5.4.1 – Management plane security	Your organization should use role based access to control who can create, configure and delete storage resources, including storage access keys.		AC-2(7), AC-3(7)
4.5.4.2 – Data in transit	Your organization should ensure that data in transit is encrypted to ensure secure communications to and from cloud environments.	• configure cloud services to specify that only the HTTPS protocol can be used for access to cloud storage services and APIs • disable weak encryption ciphers • allow use of other encrypted network protocols for application specific use cases, such as SMB for access to file storage	SC-8, SC-8(1), SC-13
4.5.4.3 – Data at rest	Your organization should consider encryption of data at rest to protect confidentiality and integrity of data, VM images, applications and backups.	• security policies should be updated to address encryption of data at rest requirement and identify class of data requiring to be encrypted on cloud storage • enforce data at rest encryption through baseline security	CP-10(6), SC-12, SC-12(2), SC-12(3), SC-28, SC-28(1)

Type	Security consideration	Implementation example	Control mapping
		configuration and continuous monitoring • ensure key management processes are well designed, documented and tested • consider the use of a dedicated HSM option from CSP	
4.5.4.4 – Data replication	Your organization should understand the data replication choices available to it and select the options required to meet its availability, durability and business continuity requirements.	• configure Geo redundant storage option to ensures data is replicated to multiple geographic locations	CP-6, CP-6(1), CP-6(2)
4.5.4.5 – Data remanence	Your organization should routinely encrypt storage media throughout its life cycle, to protect the ongoing confidentiality of data after media decommissioning and disposal.	• leverage crypto erase as a sanitization process to erase the encryption key that is used on encrypted media, to make the data unreadable media decommissioning and disposal • leverage HSM or Key management Services offered by the CSPs to protect storage key encryption keys (KEK)	MP-6, SC-12, SC-12(2), SC-12(3)
Identity and access management			
4.6.2.2 – Need for strong authentication	Your organization should consider the use of Multi-Factor authentication (MFA) to reduce the risk of account compromise. This is especially important for privileged user accounts and business critical systems.	• consider credentials and authentication mechanisms for privileged accounts to provide a higher level of assurance • restrict management of cloud workloads through a separate access point or jump host	IA-2(3), IA-2(6), IA-12(13)
4.6.2.4 – Access management	Your organization should prefer ABAC to RBAC solutions for the greater flexibility and finer granularity they provide in implementing access policies and decisions in rapidly changing cloud ecosystem.		AC-2(7), AC-3(7)
Application security			

Type	Security consideration	Implementation example	Control mapping
4.7.2- Application security considerations	Your organization should develop cloud application security architecture and pre-approve cloud application security design patterns.	• move to a continuous deployment process and automate security, including security testing, into the deployment pipeline • automate security in deployment and operations • Scrutinize API calls to cloud service and management plane, and ensure that only least privilege entitlements are enabled • account for CSP cloud platform features, services and security capabilities in security plans • ensure no static embedded credentials in application code, and leverage KMS and HSM for secret and key management • leverage micro services security and architecture to facilitate workload lock down and minimize the services running on them • leverage serverless computing security and architecture to reduce the attack surface	PL-2, PL-8
	Your organization should ensure application development, operation, and security personnel are trained on cloud security fundamentals and cloud provider technical security services and capabilities.		AT-1, AT-2, AT-3
Monitoring and incident response			
4.8.2 – Monitoring and incident	Your organization should adapt its security monitoring and incident response policies and processes to the reality of the cloud.	• understand SLA and coordination with CSP • test the incident response process with the CSP if possible	AU-2, AU-6, IR-3, IR-3(2), R-4(8), IR-10, CM-8(3), SC-5(3), SI-4, SI-4(1), SI-4(2), SI-4(4), Si-

Type	Security consideration	Implementation example	Control mapping
response considerations[28]		• validate that escalations and roles responsibilities are clear • ensure the CSP has contacts to notify client organization of incidents they detect, and that such notifications are integrated into your organization processes • ensure to maintain and test contacts, including out-of-band methods, for communication with CSP • for each service, understand and document what data and logs will be available in an incident • architect the cloud environment for faster detection, investigation, and response • ensure monitoring scope covers the cloud's management plane activities • leverage in-cloud monitoring and alerts to speed up the response process • integrate cloud platform logs into organization security operations/monitoring • understand what is logged and the gaps that could affect incident analysis • instrument additional logging into cloud workloads to address gaps in visibility to cloud platform logs	4(5), SI-4(7), SI-4(11), SI-4(13), SI-4(16), SI-4(23)

[28] The information summarized in the monitoring and incident response section of this table is based on information from domain 9of the Cloud Security Alliance (CSA), *Security guidance for critical areas of focus in cloud computing v4.0*[3]. https://cloudsecurityalliance.org/artifacts/security-guidance-v4/

Type	Security consideration	Implementation example	Control mapping
		• understand potential chain of custody issues in forensics and investigative support • automate forensic /investigation processes in cloud environments to address dynamic and higher-velocity cloud workloads (e.g. VM snapshots) • leverage the capabilities of the cloud platform to determine the extent of the potential compromise (e.g., network flow, configuration data, and access logs) • ensure the cloud management plane is free of an attacker • leverage cloud platform capabilities to speed up quarantine, eradication, and recovery process • confirm that the templates, configurations for new infrastructure applications have not been compromised • work with the organization internal response team and CSP to figure what worked and what did not • if agreed-upon response time, data, or other support wasn't sufficient, consider renegotiating SLAs	