Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

Cloud Security Risk Management

ITSM.50.062

March 2019

MANAGEMENT SERIES

FOREWORD

This description of the Cloud Security Risk Management is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE). For further information or suggestions for amendments, contact the Canadian Centre for Cyber Security (CCCS) Contact Centre:

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

EFFECTIVE DATE

This publication takes effect on March 8, 2019.

TABLE OF CONTENTS

LIST OF FIGURES

1 INTRODUCTION

Cloud computing has the potential to deliver agile, flexible, and cost-effective information system services. Under the cloud-computing paradigm, organizations give up direct control over many aspects of security and privacy, and in doing so, grant a level of trust to the cloud service provider (CSP). At the same time, organizations using cloud services are still accountable for the confidentiality, integrity, and availability of the information system and related information hosted by the CSP.

As a result, organizations must extend their information system security risk management practice to include cloud environments. The shared nature of operating and using a cloud environment changes who is responsible for the implementation, operation, and maintenance of security controls. Organizations therefore need to understand cloud security to address risks effectively.

To enable the adoption of cloud computing, the Government of Canada (GC) developed an integrated risk management approach to establish cloud-based services. ITSM.50.062 outlines this approach which can be applied to all cloud based services independently of the cloud service and deployment models.

2 CONTEXT

2.1 CLOUD SERVICE MODELS

The NIST Cloud Computing Reference Architecture (Special Publication 500-292) [9] outlines the definitions of the various types of service models. Broadly, service models describe what type of service the CSP provides to consumers: an application, a programming platform, or raw computing resources. In cloud computing scenarios, the cloud consumer has three different service models from which to choose:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

In an IaaS service model, the capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer can deploy and run arbitrary software, which may include operating systems and applications.

In a PaaS service model, the capability provided to the consumer is to deploy onto the cloud infrastructure consumer created or acquired applications created using programming, libraries, services, and tools supported by the provider.

In a SaaS model, the service provided to the consumer is to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface such as a web browser (e.g. web-based email), or a program interface (e.g. local application).

2.2 CLOUD DEPLOYMENT MODELS

Deployment models describe the relationship between the cloud service provider and cloud service consumer. NIST identifies four cloud deployment models:

- Public
- Private
- Community
- Hybrid

In a public cloud, the cloud infrastructure is provisioned for open use by the general public.

In a private cloud, the cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g. business units).

In a community cloud, the cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g. mission, security requirements, policy, and compliance considerations).

In a hybrid cloud, the cloud infrastructure is a composite of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities bound together by standardized or proprietary technology enabling data and application portability.

2.3 ACTORS

To be successful, the cloud security risk management approach relies on the activities of several actors, some working independently of the organization. These actors are as follows:

- CSP: Any commercial provider of cloud services that wishes to offer its services to consumers. A CSP may or may not hold an attestation[1] for its cloud services when first engaging in the risk management process.
- Cloud service broker: An organization that acts as an intermediary between CSPs and consumers by offering various types of brokerage services including cloud marketplace[2].
- Consumer organization: Any organization that wishes to get a CSP to implement a cloud based service.
- Third party security assessor: Any organization working independently of CSPs and the consumer organization that conducts security assessments under one or more security attestation programs.
- Cloud security assessor: An organization (or individual acting on its behalf) that conducts security assessments of cloud services.
- Authorizer: The organization (or individual acting on its behalf) accountable for the security of a cloud based service, that must authorize its operations based on the results of security assessments.

[1] This document uses the term attestation generically to mean any IT security related certification, or assessment to which CSPs may subject their services. These include, for example, Service Organization Control 2 (SOC2) and International Electrotechnical Commission / International Organization for Standardization (IEC/ISO) 27001 standard.

[2] A cloud marketplace is an online storefront operated by a CSP

3 CLOUD SECURITY RISK MANAGEMENT APPROACH

3.1 POLICY DRIVERS

Organizations need to understand the security policies, standards, and guidelines that address cloud security requirements. As cloud computing also poses additional privacy challenges to organizations using cloud services, organizations must understand their obligations under Canada's privacy legislation [5]:

- Privacy Act [6][3]
- Personal Information Protection and Electronic Documents Act (PIPEDA) [7][4]
- Provincial privacy laws
- Sector-specific privacy laws

3.2 RELATIONSHIP TO THE IT RISK MANAGEMENT PROCESS

The approach presented in this document is an adaptation of existing risk management and cloud security standards from the following institutions:

- The US National Institute of Standards and Technology (NIST)
- The Canadian Centre for Cyber Security (CCCS)
- The Treasury Board of Canada Secretariat (TBS)

As part of its risk management framework, an organization must determine the security goals needed to protect their information and services.

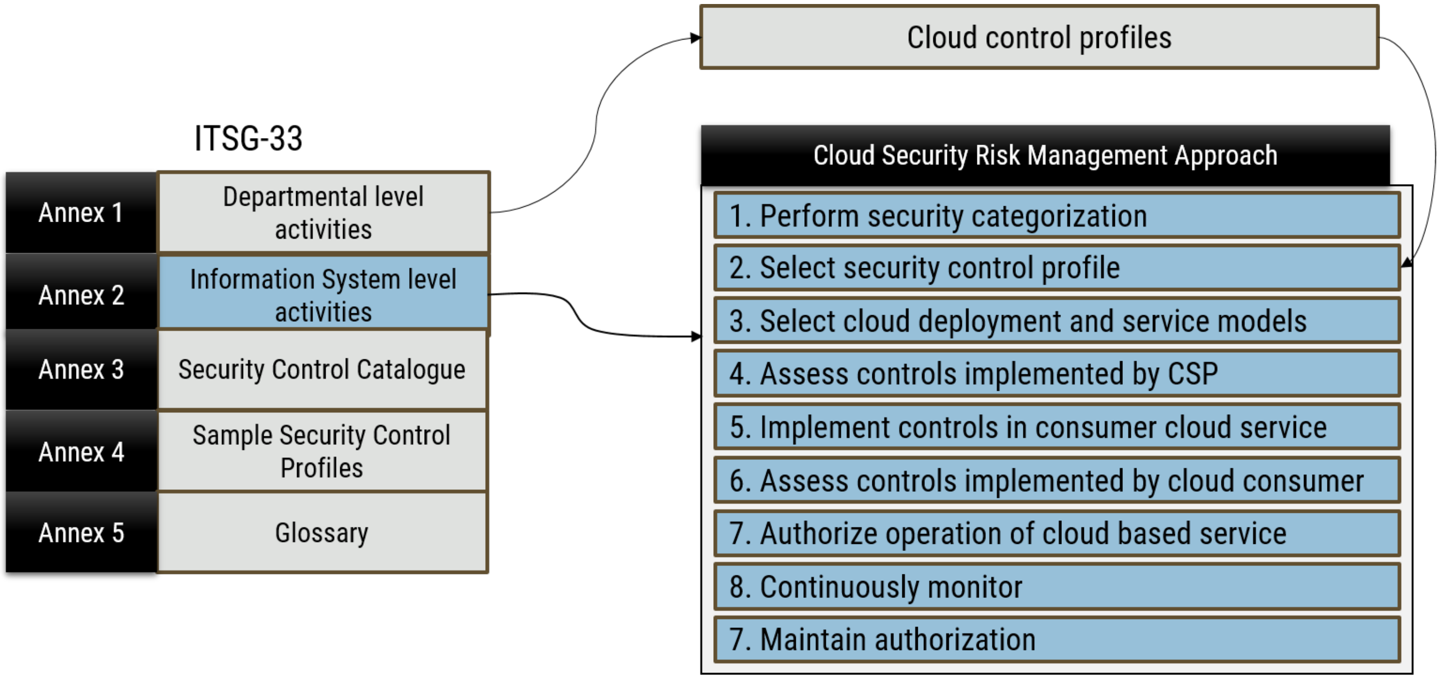
CCCS's IT Security Risk Management: A Lifecycle Approach (ITSG-33) [8] guidelines suggest a set of activities at two levels within an organization: the departmental level and the information system level.

Departmental level activities[5] are integrated into the organization's security program to plan, manage, assess, and improve the management of IT security-related risks the organization faces.

Information System level activities[6] are integrated into an information system development lifecycle (SDLC). These activities include the execution of information system security engineering, threat and risk assessment, security assessment, and authorization. As shown in Figure 1, the cloud security risk management approach supports the Information System level activities.

Information security managers are responsible for including cloud environments in their information system security risk management practices. Responsibility for security assessment and authorization resides with the business owner within the consumer organization seeking the cloud service capability.

[3] The Privacy Act covers how the federal government handles personal information.
[4] PIPEDA covers how business handle personal information.
[5] Annex 1 of ITSG-33 [8] describes Departmental level activities in detail.
[6] Annex 2 of ITSG-33 [8] describes Information System level activities in detail



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
1. Perform security categorization
2. Select security control profile
3. Select cloud deployment and service models
4. Assess controls implemented by CSP
5. Implement controls in consumer cloud service
6. Assess controls implemented by cloud consumer
7. Authorize operation of cloud based service
8. Continuously monitor
7. Maintain authorization

Figure 1: Cloud security risk management approach relationship to IT risk management process

3.3 FOUNDATION FRAMEWORKS

This cloud security risk management approach is derived from the following cloud computing and information system security risk management standards, recommendations, and guidance:

- CCCS information system security risk management guidance, ITSG-33 [8]
- NIST's standards on information system security risk management, which are specified in the Special Publications 800 series [9]
- The NIST cloud computing reference architecture, which is documented in Special Publication 500 292 [10]
- The NIST cloud computing security reference architecture, which is documented in Special Publication 500 299 [11]
- The Federal Risk and Authorization Management Program (FedRAMP) [12]
- TBS's Security Risk management approach and procedure [13]

3.4 RISK MANAGEMENT PROCESS OVERVIEW

Organizations are ultimately responsible and accountable for the security risks incurred by using information system services offered by external suppliers, including the cloud services provided by CSPs and cloud brokers. As a result, organizations needs to adopt a structured approach for managing risks that accounts for the incorporation of cloud services to support their program goals and outcomes.

As shown in Figure 2, the cloud security risk management process consists of a series of procedures implemented by a CSP and consumer organization, as described below.

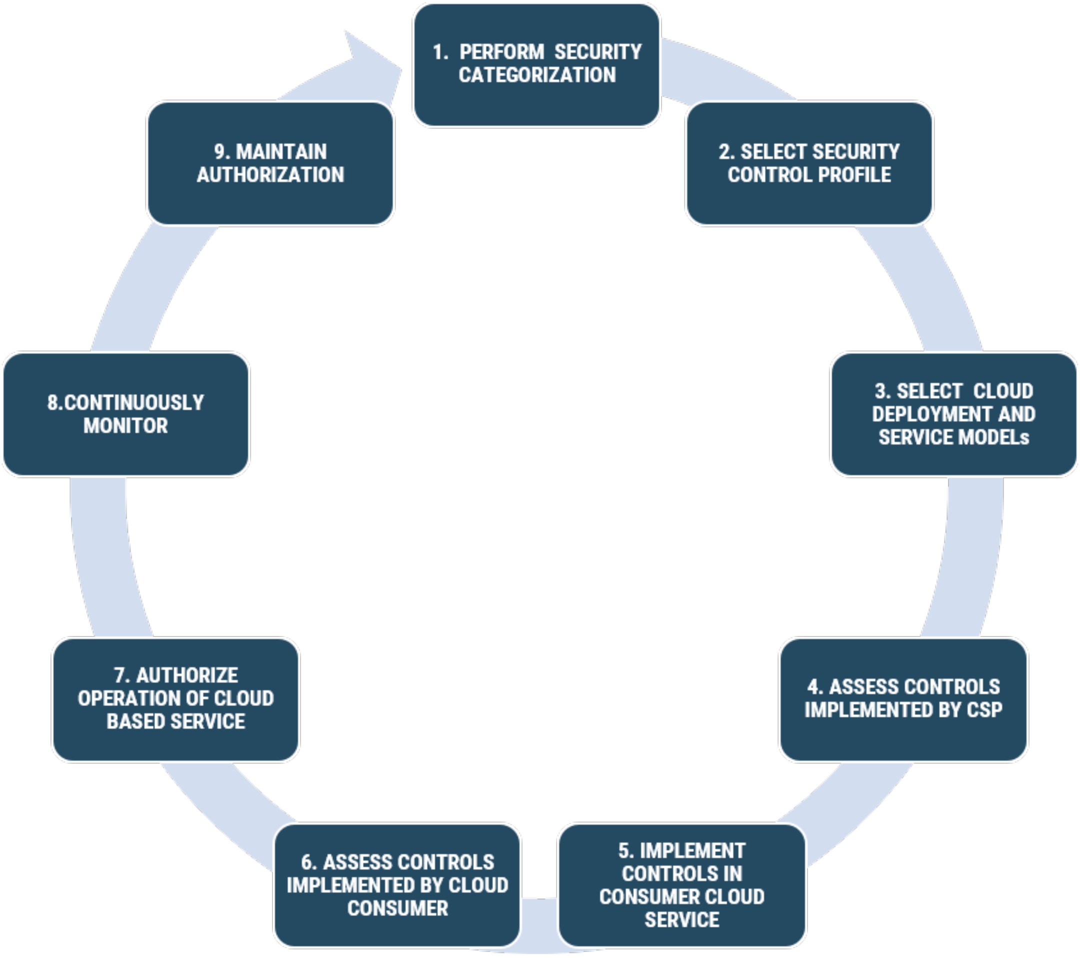

1. PERFORM SECURITY CATEGORIZATION
2. SELECT SECURITY CONTROL PROFILE
3. SELECT CLOUD DEPLOYMENT AND SERVICE MODELs
4. ASSESS CONTROLS IMPLEMENTED BY CSP
5. IMPLEMENT CONTROLS IN CONSUMER CLOUD SERVICE
6. ASSESS CONTROLS IMPLEMENTED BY CLOUD CONSUMER
7. AUTHORIZE OPERATION OF CLOUD BASED SERVICE
8.CONTINUOUSLY MONITOR
9. MAINTAIN AUTHORIZATION

Figure 2: Cloud security risk management process

Step 1 – Perform Security Categorization

Security categorization is a fundamental activity of the cloud security risk management approach as it provides the basis for determining the level of expected injuries from information system related threat compromise. Through this process, the business activities that will be supported by a cloud based service are identified and categorized, and the service inherits the resulting security category. Consumer organizations then select a suitable security control profile based on the security category and their risk tolerance.

Step 2 – Select Security Control Profile

Security control profiles have been developed for cloud based services. These profiles were derived from the baseline profiles in Annex 4 of ITSG-33 [2]. The cloud control profiles identify the recommended security controls that the CSPs and consumer organizations should implement for the assessed security category. The selected cloud control profile also serves as the basis for assessing the security controls.

Step 3 – Select Cloud Service and Deployment Models

When deploying to a cloud service, consumer organizations need to determine the appropriate cloud service and deployment models for their IT service. This choice will be motivated by the nature of the service, how much control the consumer organization wants to keep, and the level of expertise and maturity the consumer organization has in operating and maintaining cloud-based information system environments.

Step 4 – Assess Security Controls Implemented by CSP

A consumer organization does not always have control over or visibility into the design, installation, and assessment of the CSP's security controls. An alternative security assessment approach needs to be applied, and can be done by considering other trusted security assessments. Results from these security assessments, if considered applicable and reliable, can be incorporated into the organization security assessments.

In the context of the cloud security risk management approach, these trusted security assessments consist of third-party attestations that have much more value than self-assessments. These attestations should have been carried out by an independent third party that is bound to be objective and apply professional standards to the evidence it reviews and produces. However, third party attestations rarely cover all security requirements in the selected security control profile. Additional security requirements and contract clauses may be needed to ensure that CSPs provide required evidence to support the security assessment activities.

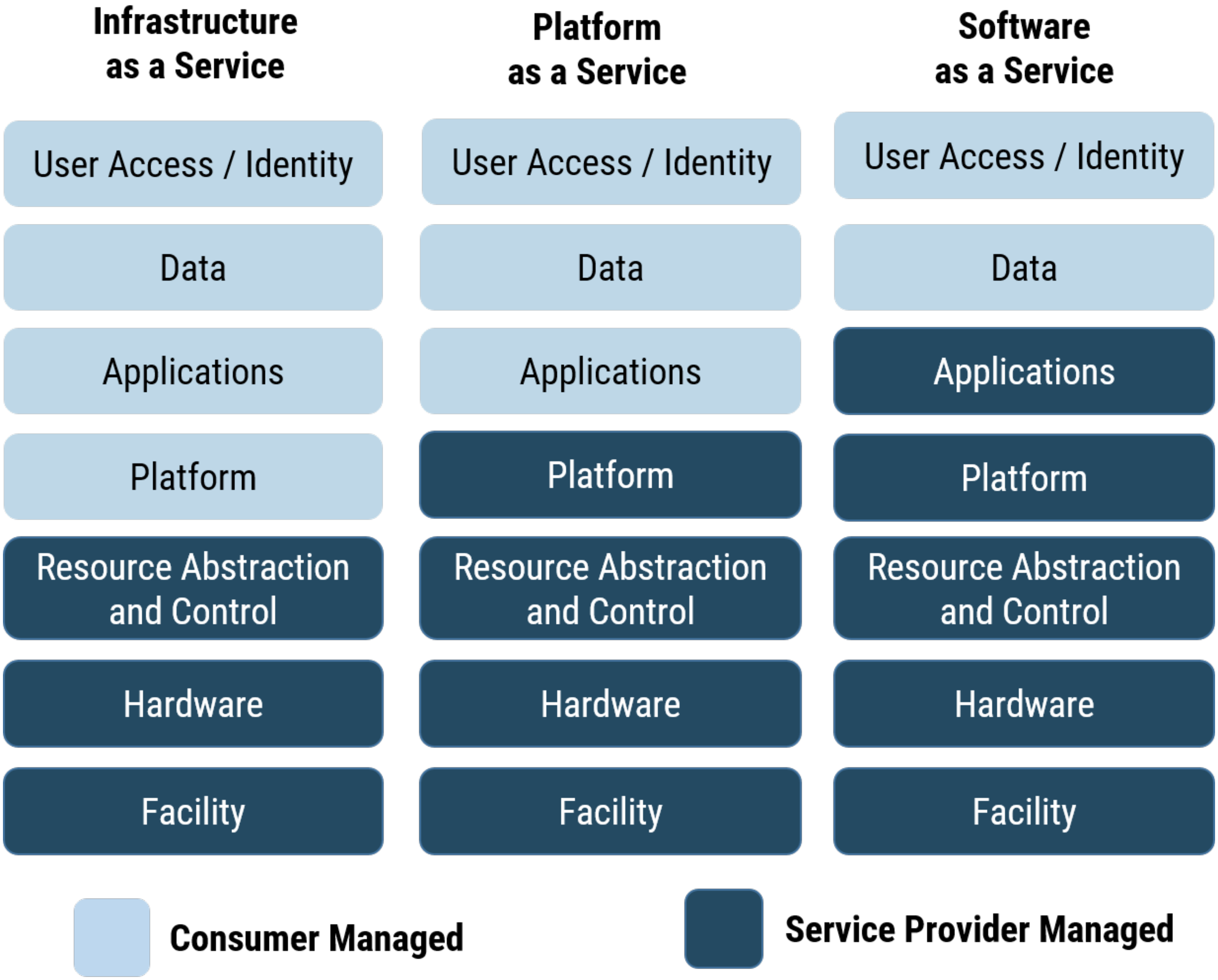
Step 5 – Implement Security Controls in the Consumer Organization Cloud Service

When implementing a cloud profile, the consumer organization and the CSP are each responsible to implement many of the recommended security controls. In addition, there are some security controls that must be implemented by both the CSP and the consumer organization.

The nature of the security controls that a consumer organization needs to implement in the cloud-based service is dictated by the service model upon which the service is being chosen. Figure 3 gives a view of the division of responsibility for implementing security controls between the CSP and the consumer organization. Under the IaaS service model, consumer organizations implement more security controls than in the SaaS service model.

Step 6 – Assess Security Controls Implemented by Consumer Organization

Consumer organizations are responsible for the assessment of the security controls assigned to them in the cloud control profiles. As shown in Figure 3, the scope of cloud control profiles includes all CSP and consumer organization components used to provide and consume the cloud-based service. As a result, consumer organizations must understand the overall effectiveness of security controls implemented by the CSP and their own organizations. Understanding the overall effectiveness of security controls is essential in determining and managing the residual risks under which the cloud-based service will be operating.



Infrastructure as a Service	Platform as a Service	Software as a Service
□ User Access / Identity	□ User Access / Identity	□ User Access / Identity
□ Data	□ Data	□ Data
□ Applications	□ Applications	■ Applications
□ Platform	■ Platform	■ Platform
■ Resource Abstraction and Control	■ Resource Abstraction and Control	■ Resource Abstraction and Control
■ Hardware	■ Hardware	■ Hardware
■ Facility	■ Facility	■ Facility

□ Consumer Managed ■ Service Provider Managed

Figure 3: Shared responsibility

Step 7 – Authorize Operation of Cloud Service

Authorization is the ongoing process of getting and maintaining official management decisions by a senior organizational official to authorize operation of an information system to support a set of business activities. The risk-based decision whether to authorize operations is made based on the content of the authorization package.

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 authorizing officials need to consider when deciding whether they should authorize operations of the cloud based service and accept residual risks.

Step 8 – Continuously Monitor

Cloud security risk management goes beyond implementation by incorporating activities for continuous monitoring during the operational phase of cloud based services. Continuous monitoring defines how the security controls of cloud based services are monitored over time, and how monitoring data is used to find out if these services are still operating within their authorization parameters.

Through continuous monitoring, consumer organizations equip themselves with capabilities for finding security deviations from the authorization state in both CSP and consumer organization portions of cloud based services.

Step 9 – Maintain Authorization

Through maintaining their authorization, consumer organizations equip themselves with capabilities to react to deviations from the authorization state in a timely and effective manner. In line with ITSG-33[8] guidance, when it is found that cloud-based services are not operating within their authorization parameters, consumer organizations should consider taking the following steps:

- Implement temporary measures to protect the supported business activities.
- Update implemented security controls to correct security deficiencies.
- Accept the new level of residual risk.

4 STACKING ASSESSMENTS

In the cloud space, many cloud systems rely on other cloud providers to give a comprehensive set of services for the end customer. An example is a software provider using an infrastructure provider to deliver a SaaS offering. In this case, the software provider will inherit security controls from the infrastructure provider.

Cloud security risk management makes allowances for stacking 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 provider would not need to give evidence for the security assessment of the IaaS and PaaS systems that it leverages. Instead, separate security assessments would need to be completed and could then be reused for the leveraged IaaS and PaaS systems. This would reduce the number of attestations or security assessments, remove duplication across authorization packages, and keep assessments delineated by information system boundaries.

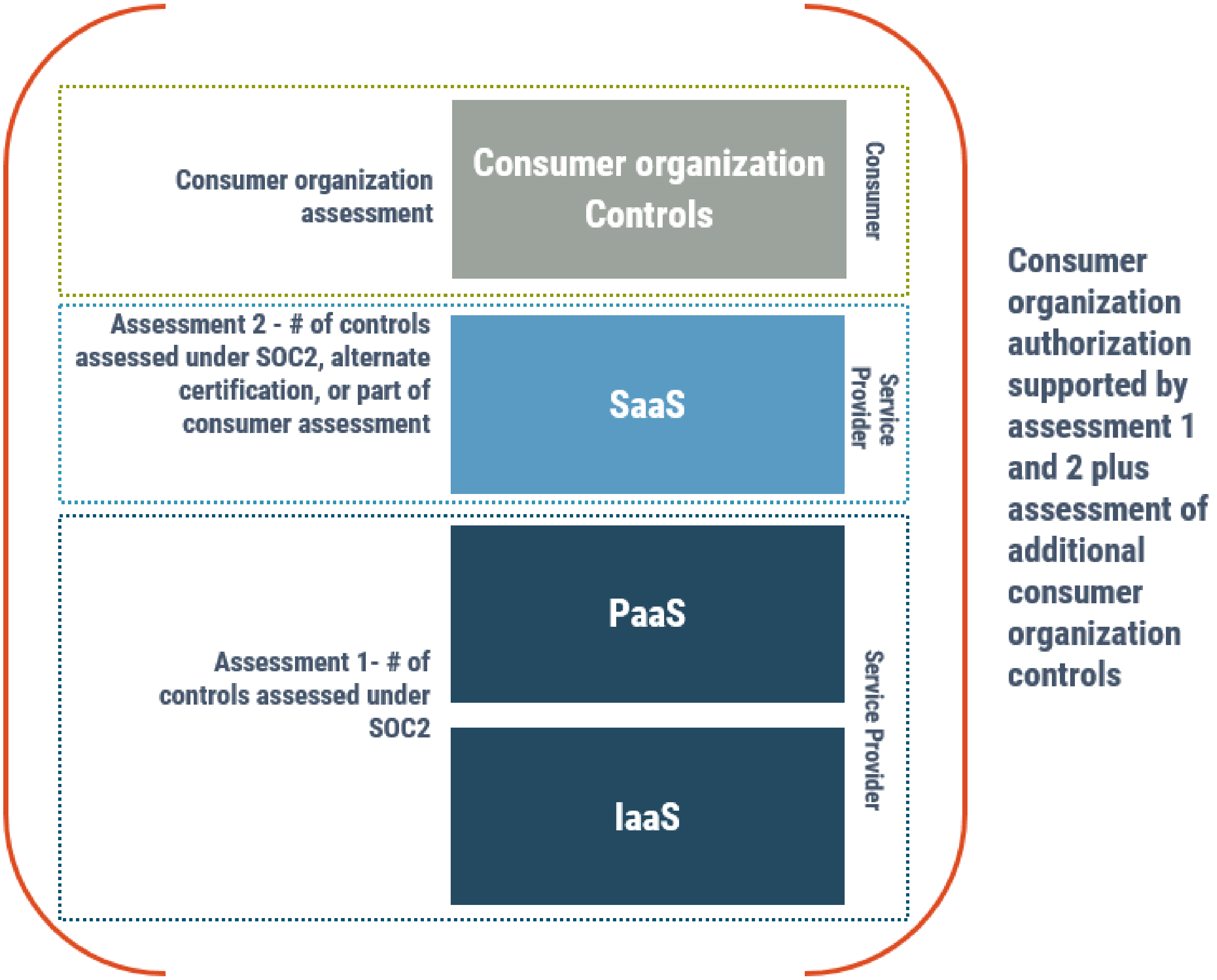

Consumer organization assessment
Consumer organization Controls
Consumer
Assessment 2 - # of controls assessed under SOC2, alternate certification, or part of consumer assessment
SaaS
Service Provider
Assessment 1- # of controls assessed under SOC2
PaaS
IaaS
Service Provider
Consumer organization authorization supported by assessment 1 and 2 plus assessment of additional consumer organization controls

Figure 4: Assessment stacking

5 REUSING ASSESSMENTS

There are many scenarios where assessments of CSP cloud services and consumer cloud based services can be reused. For example, consumer organizations might leverage IaaS and PaaS from the same CSP for implementation of their cloud-based services. It may be appropriate for the consumer organization to reuse an existing CSP assessment. However, prior to reuse, consumer organizations must confirm the scope of the CSP assessment covers each applicable cloud service model and deployment region.

6 SUMMARY

Adopting cloud-based services will require cloud consumer organizations to include cloud environments in their information system security risk management practice. ITSM.50.062 will help cloud consumer organizations understand the risk management activities to perform when adopting cloud services.

7 CONTACTS AND ASSISTANCE

If your department has identified a requirement for ITSM.50.062 Cloud Security Risk Management based on business needs and would like more information, please contact us through the:

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

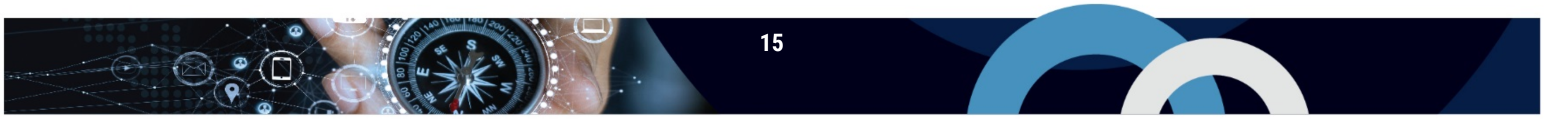
8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
CCCS	Canadian Centre for Cyber Security
CSE	Communications Security Establishment
CSP	Cloud Service Provider
IaaS	Infrastructure as a Service
FedRAMP	Federal Risk and Authorization Management Program
GC	Government of Canada
IEC/ISO	International Electrotechnical Commission / International Organization for Standardization
IT	Information Technology
ITS	Information Technology Security
ITSG	Information Technology Security Guidance
NIST	National Institute of Standard and Technology
PaaS	Platform as a Service
SaaS	Software as a Service
SDLC	System Development Lifecycle
SSAE	Statements on Standards for Attestation Engagements
SOC	Service Organization Control
TBS	Treasury Board of Canada Secretariat

8.2 GLOSSARY

Term	Definition
Residual risk	The part of risk left after security measures are applied.
Security category	A security category characterizes a business activity by the severity of expected injuries (injury level) from compromise with respect to the security goals of confidentiality, integrity, and availability.
Security control profile	A security control profile specifies a set of controls and enhancements. When applied appropriately with your specific technical and threat context in mind, these controls and enhancements protect the confidentiality, integrity, and availability of information systems that are used to support business activities.



8.3 REFERENCES

Number	Reference
1	Treasury Board of Canada Secretariat. *Government of Canada Cloud Adoption Strategy,* n. d.
2	Treasury Board of Canada Secretariat. *Policy on the Management of Information Technology*, 1 July 2007
3	Treasury Board of Canada Secretariat. *Policy on Government Security,* 1 July 2009.
4	Treasury Board of Canada Secretariat. *Operational Security Standard: Management of Information Technology*, n.d.
5	Office of the Privacy Commissioner of Canada. *Summary of privacy laws in Canada*, January 2018
6	Department of Justice Canada. *Privacy Act*, 1985
7	Department of Justice Canada. *The Personal Information Protection and Electronic Documents Act*, 2015
8	Canadian Centre for Cyber Security. *IT Security Risk Management: A Lifecycle Approach (ITSG-33),* December 2014.
9	National Institute of Standards and Technology. *NIST Special Publications, SP800s - Computer Security.*
10	National Institute of Standards and Technology. *NIST Cloud Computing Reference Architecture (Special Publication 500-292),* September 2011.
11	National Institute of Standards and Technology. *NIST Cloud Computing Security Reference Architecture (Special Publication 500-299)*, DRAFT.
12	US Government, Federal Risk and Authorization Program (FedRAMP).
13	Treasury Board of Canada Secretariat. *Cloud Security Risk Management Approach and Procedures*, n. d.
14	National Institute of Standards and Technology. *Managing Risk in a Cloud Ecosystem*, n.d.