Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

Guidance on the Security Categorization of Cloud-Based Services

ITSP.50.103

MAY 2020

PRACTITIONER

Canada

FOREWORD

ITSP.50.103 Guidance on Security Categorization of Cloud-Based Services is an UNCLASSIFIED publication that is issued under the authority of the Head of the Canadian Centre for Cyber Security (Cyber Centre). For more information, email or phone our Contact Centre:

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

EFFECTIVE DATE

This publication takes effect on May 20, 2020.

REVISION HISTORY

Revision	Amendments	Date
1	First release.	May 20, 2020

OVERVIEW

The purpose of this document is to help your organization categorize the security of cloud-based services. You can use this document to help you select a security control profile that adequately protects information and business activities. You can also use this document as a guide when selecting a cloud deployment model and a cloud service model.

Security categorization is a fundamental step in protecting against the risks associated with the use of cloud computing. Your organization can use security categorization to help determine the potential injury if business processes or information assets are compromised. This document helps your organization with the following activities:

- Categorizing the security of cloud-based services;
- Selecting an appropriate security control profile for protecting business information; and,
- Selecting a cloud deployment and service model.

To help your organization with these activities, this document includes the following content:

- Reviews security categorization terms and definitions established by *ITSG-33 IT Security Risk Management: A Lifecycle Approach* [1][1];
- Recommends a security categorization process to guide organizations in the identification of expected level of injury from threat compromise;
- Recommends an approach to inventory business process and information assets;
- Describes how to identify expected injuries and injury levels from threat compromise;
- Describes special factors impacting the level of expected injury levels;
- Describes an approach to identify business domains;
- Describes how to select a cloud security control profile based on the security category of business activity;
- Describes how to select a cloud deployment model and a cloud service model based on the security category of business activity; and
- Provides recommended security control profiles for the low and medium security categories.

This document is part of a suite of documents that the Cyber Centre has developed to help secure cloud-based services. Security categorization, the selection of a security control profile, and the selection of a cloud deployment model and a cloud service model are the first three steps of the Cloud Security Risk Management approach. This approach is defined in *ITSM.50.062 Cloud Security Risk Management* [2].

[1] Numbers in square brackets refer to references that are cited in the Supporting Content section of this document.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ANNEXES

1 INTRODUCTION

This document can assist organizations in the security categorization of information systems, the selection of an appropriate security control profile, and the selection of a cloud deployment model and a cloud service model.

Security categorization activities play a critical role in ensuring the right level of protection for cloud solutions. These cloud solutions provide public and private organizations with agile, flexible and cost-effective information technology options. However, cloud solutions can be subject to serious threats that can have adverse effects on business activities. Compromises of cloud-based services can be expensive to fix, and threaten the availability, confidentiality, and integrity of business information.

Security controls are critical elements in the design of cloud-based services. While too much protection can lead to increased costs and wasted resources, not enough protection can put information and business processes at risk. Security categorization is fundamental; it provides the basis for selecting the appropriate cloud capabilities, security control profile, cloud deployment model, and cloud service model[2].

For more information on determining appropriate security controls for secure architectures, refer to ITSG-33 [1].

1.1 POLICY DRIVERS

The need for security categorization is normally identified in the security policies, directives, regulations, or standards that are applicable to each organization[3]. The publications below identify the correct level of protection needed to counter cyber threats and vulnerabilities affecting cloud-based services:

- *Government of Canada Cloud Adoption Strategy* [4];
- *Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice (SPIN)* [5]; and
- *Policy on Service and Digital* [6].

In addition to ITSG-33 [1], you can use these publications as reference materials when your organization is creating policies and building the foundation for security categorization within your cloud security risk management practices and programs.

[2] See the TBS *Government of Canada Cloud Security Risk Management Approach and Procedures* [3] for more information.

[3] Security policies, directives, standards, guidelines and regulations may not always use the term security categorization. It is common for such document to use the terms level of injury, harm, or sensitivity. For example, one of the principles of PIPEDA states: “Personal information shall be protected by security safeguards appropriate to the sensitivity of the information” [7].

1.2 APPLICABLE ENVIRONMENTS

The information provided in this document applies to both private and public-sector organizations. We describe a security categorization process that your organization can apply for all business processes and associated information assets.

Government of Canada (GC) partners and other levels of government may have sensitive business processes and information assets of national interest. These sensitive assets must be considered in the security categorization process. Some national interest considerations are also presented in this document.

1.3 RELATIONSHIP TO CLOUD RISK MANAGEMENT

ITSG-33 [1] suggests two levels of IT security risk management activities: organizational-level activities (referred to as departmental-level activities in ITSG-33 [1]) and information system-level activities.

You should integrate organizational-level activities into your organization's security program. Organizational-level activities can help you plan, manage, assess, and improve the management of your organization's IT security-related risks. For more information on these activities, see ITSG-33, Annex 1 [1]. Figure 1 shows that security categorization supports organizational risk management by defining the business context of security control profiles.

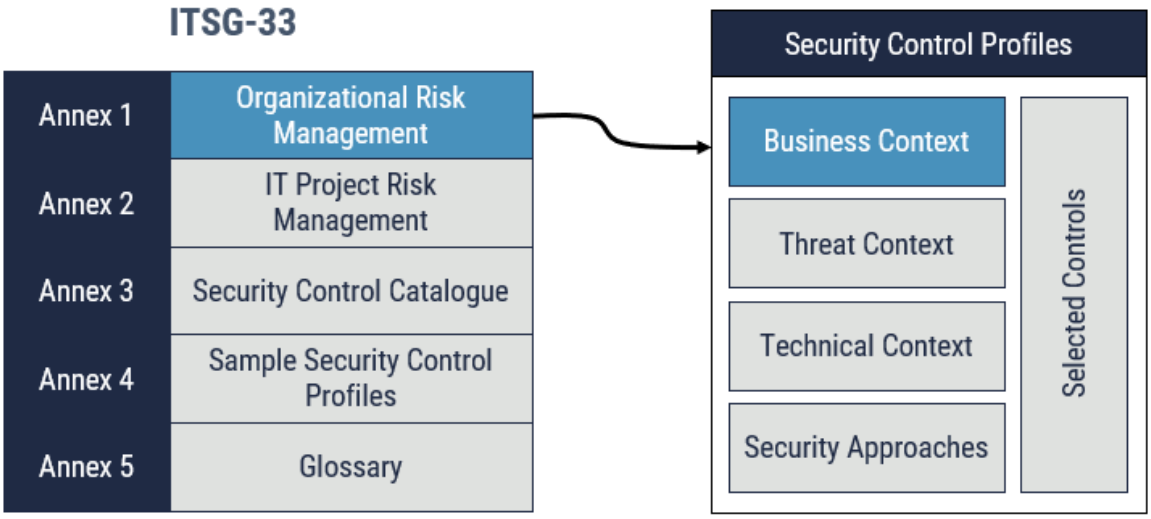


Figure 1: Security Categorization Relationship to Departmental Risk Management

You should integrate information system-level activities into your organization's information system development lifecycle (SDLC). These activities include the execution of information system security engineering, threat and risk assessment, security assessment, and authorization. For more information on these activities, see Annex 2 of ITSG-33 [1].

Our cloud security risk management approach aligns with the information system-level activities discussed in ITSG-33 [1]. Figure 2 shows that security categorization, cloud security control profile selection, and cloud deployment and service model selection support the first three steps of the cloud security risk management approach. Categorizing cloud-based services provides the information needed to determine the security requirements and the security controls that the cloud service provider (CSP) and cloud consumer should meet.

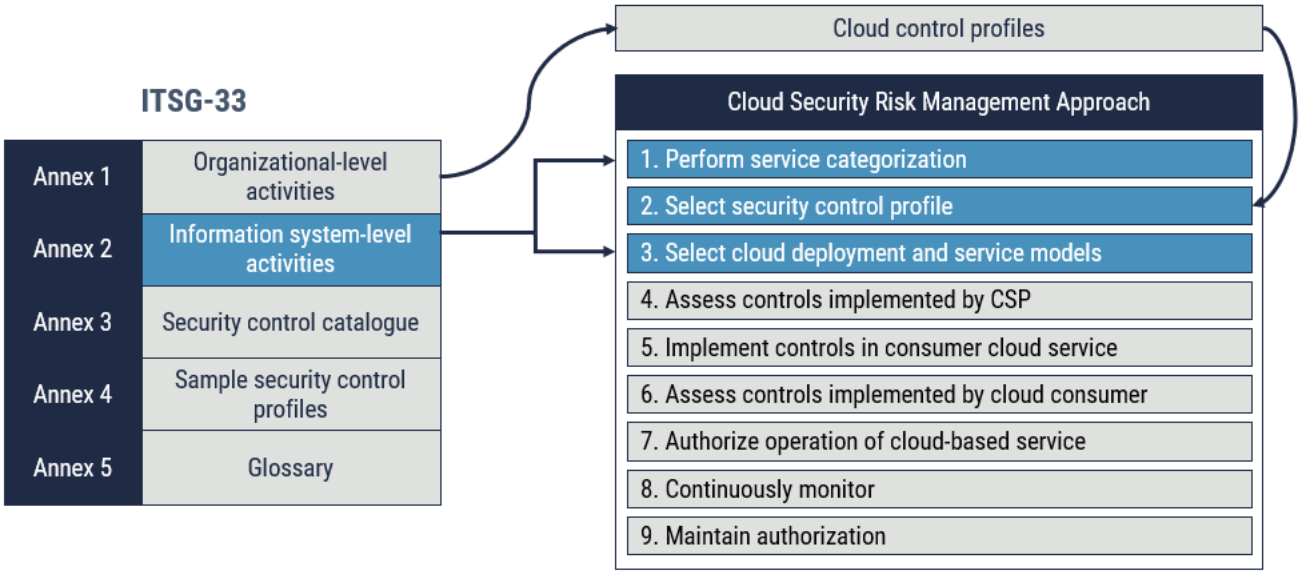


Figure 2: Security Categorization Relationship to Information System-Level Activities

2 SECURITY CATEGORIZATION

This document describes the following security categorization activities for the adoption of cloud-based services:

1. Develop an injury assessment table;
2. Create an inventory of business activities, processes, and information assets;
3. Assess injuries resulting from business process and information asset failures; and
4. Analyze domains.

Security categorization is the process of identifying the potential injuries that could result from compromises to business processes, business activities, and related information. To categorize business processes and activities, you must first determine the expected injuries that could result from a compromise and the level of these expected injuries.

Through this process, the business processes and activities that will be supported by a cloud-based service are identified and categorized, and the service inherits the resulting security category. Cloud consumers then select a suitable security control profile based on a combination of the security category and their risk tolerance. The security category is also one of the factors considered in the selection of the cloud service deployment model and service model.

A security category expresses the highest levels of expected injuries from threat compromise with respect to the security objectives of confidentiality, integrity, and availability.

Table 1: Security Objectives

Security objectives	Definition
Confidentiality	The state of being disclosed only to authorized principals.
Integrity	The state of being accurate, complete, authentic and intact.
Availability	The state of being accessible and usable in a timely and reliable manner.

Organizations should assign a business analyst to lead and facilitate the security categorization activities. The business analyst, supported by a security advisor, should conduct the security categorization process as an organization-wide activity that involves information system owners, information owners, chief information officers, senior information security officers, and business owners[4]. Senior leadership and other key officials can provide the essential oversight in the security categorization process to ensure that cloud risk management activities are carried out effectively and consistently throughout the organization[5]. If security categorization activities are not performed as an organization-wide activity, the business analyst will need to repeat these activities for each project.

[4] ITSG-33 Annex 4A Control profile, RA-2 supplemental guidance [1]

[5] National Institute for Standards and Technology (NIST) *800-60, Vol 1 Guide for Mapping Types of Information and Information Systems to Security Categories* [8]

3 STEP 1: DEVELOP AN INJURY ASSESSMENT TABLE

The first step of the categorization process is to develop an injury assessment table.

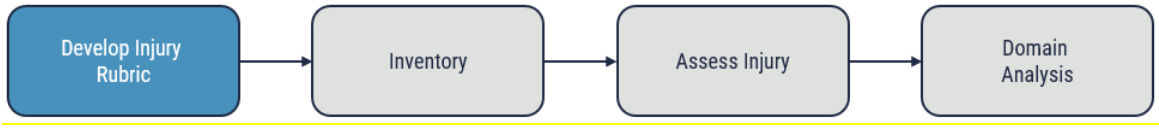


Figure 3: Security Categorization Process: Step 1 – Develop an Injury Rubric

Table 2 is a sample injury table that you can use to ensure consistency when identifying injury types (listed along the vertical axis) and levels (listed along the horizontal axis). A qualifier is shown for comparison purposes where the injury type intersects with the injury level. The nine types of injury proposed in ITSG-33 [1] describe common critical injuries that may impact an organization's mission. However, given that each organization has a different risk tolerance profile, a single injury assessment table is not universally applicable across all organizations. Your organization should confirm that the sample injury table accurately represents the injury types that are the most likely to impact business activities and the confidentiality, integrity, or availability of information. If the sample injury table does not reflect expected injury types and risk tolerance criteria, organizations should develop their own injury assessment table.

Table 2: ITSG-33 Sample Injury Table

Injury Type	Qualifier and Level				
	Very low	Low	Medium	High	Very High
Civil disorder or unrest	No reasonable or negligible expectation of injury	Civil disobedience, public obstructions	Riot	Sabotage affecting critical assets (e.g., critical infrastructure)	Large scale riot or sabotage requiring martial law
Physical harm to people	No reasonable or negligible expectation of injury	Physical discomfort	Physical pain, injury, trauma, hardship, illness	Physical disability, loss of life	Widespread loss of life
Psychological harm to people	No reasonable or negligible expectation of injury	Stress	Distress, psychological trauma	Causing a mental disorder or illness	Widespread psychological trauma
Financial loss to individuals	No reasonable or negligible expectation of injury	Causing stress or discomfort	Affecting quality of life	Financial security compromised	N/A
Financial loss to Canadian companies	No reasonable or negligible expectation of injury	Affecting performance	Reducing competitiveness	Viability compromised	N/A
Financial loss to the Canadian government	No reasonable or negligible expectation of injury	Affecting program performance	Affecting program outcomes	Program viability compromised	Key programs viability compromised
Harm to Canadian economy	N/A	N/A	Affecting performance	Reducing international competitiveness	Compromising key economic sectors
Harm to Canada's reputation	No reasonable or negligible expectation of injury	Loss of Canadian public confidence	Embarrassment (home or abroad)	Damage to federal-provincial relations	Damage to diplomatic or international relations
Loss of Canadian sovereignty	N/A	N/A	Impediment to the development of major government policies	Impediments to effective law enforcement Loss of continuity of government	Loss of territorial sovereignty

3.1 INJURY TYPES

To develop an injury table, you must first identify the injury types that are the most likely to impact your organization's critical functions or reputation. Injury types can be determined by reviewing existing impact assessments, privacy impact assessments, business risk assessments, and threat and risk assessments. Regulatory instruments such as laws, policies, and regulations may also be helpful as non-compliance to regulatory requirements could lead to penalties, sanctions, and increased injury[6].

If such documents are not available, organizations can develop the injury types from business goals, objectives, and performance statements found in business plans and performance reports.

Some examples of injury types include the following:

- Loss of reputation;
- Loss of privacy (data under your organization's responsibility);
- Regulatory fines (government regulations);
- Contractual penalties (non-compliance with existing contracts);
- Harm to customer satisfaction;
- Loss of intellectual property;
- Loss of revenue;
- Loss of business;
- Increased operating cost;
- Increase in personnel requirements;
- Loss of critical capability;
- Loss of competitive edge;
- Loss of stockholder confidence;
- Increase in legal cost;
- Loss of life; and
- Harm to health.

After reviewing existing business impact assessments, privacy impact assessments, and other business risks reports, organizations can identify the injury types that are applicable to them. Tables 3 and 4 depict the injury types that apply to a private sector or non-profit organization respectively. The applicable injury types are captured in an injury table that will be more representative of the potential injuries that could result from compromises for each of these organizational types.

[6] ITSG-33 [1], Annex 1, p. 37.

Table 3: Example Injury Table for Private Sector Organizations

Injury Type	Injury Level		
	Low	Medium	High
Financial harm			
Regulatory violation			
Harm to reputation			
Loss of privacy			
Harm to intellectual property			

Table 4: Example Injury Table for a Non-Profit Organization

Injury Type	Injury Level		
	Low	Medium	High
Loss of privacy			
Financial harm			
Harm to reputation			
Harm to beneficiaries			
Regulatory violation			

3.2 INJURY LEVELS AND QUALIFIERS

To develop an injury table, you also need to identify the qualifiers for each injury level. Qualifiers describe injury level selection criteria for each injury level across all injury types. To define the qualifiers, it is important to understand the definition for each injury level. Table 5 provides definitions and examples for each injury level.

Table 5: Definitions and Example Qualifiers for Injury Levels

Injury Level			
	Low	**Medium**	**High**
Definition	The potential injury is **LOW** if unauthorized disclosure, modification or loss of access to the information or services used by the business activity could reasonably be expected to cause no or limited injury to individuals or the organization.	The potential injury is **MEDIUM** if unauthorized disclosure, modification or loss of access to the information or services used by the business activity could reasonably be expected to cause serious injury to an individual, organization or limited injury to a group of individuals.	The potential injury is **HIGH** if unauthorized disclosure, modification or loss of access to the information or services used by the business activity could reasonably be expected to cause extremely grave injury to an individual, organization or serious injury to a group of individuals.
Example qualifiers	• Minor effect on annual profit • Minor loss of sale • Minor compliance violation • Privacy violation 1 person • Affects program performance • Stress • Physical discomfort • Civil disobedience • Loss of confidence	• Significant effect annual profit • Loss of major accounts • Loss of goodwill • Clear compliance violation • Privacy violation – hundreds of people • Affects program outcome • Distress, psychological trauma • Affects quality of life • Riots • Embarrassment (home and abroad) • Affects business competitiveness	• Bankruptcy • Brand damage • High profile compliance violation • Privacy violation – thousands or millions of people • Affects program performance • Causing mental disorder or illness • Sabotage • Damage to reputation • Affects business viability

Based on the examples provided in tables 3 and 4, a private sector and a non-profit organization identified qualifiers for each injury level. Each type of organization can use the completed injury tables 6 and 7 to support their respective security categorization activities. This will ensure consistency in the selection of injury level.

Table 6: Example of a Completed Injury Table (Private Sector Organization)

Injury Type	Injury Level		
	Low	Medium	High
Financial harm	• Minor effect on annual profit • Minor loss of sale	• Significant effect on annual profit	• Bankruptcy
Regulatory violation	• Minor penalty	• Significant penalty	• Brand damage • Devaluation of trade name • Loss of major accounts
Harm to reputation	• Loss of confidence	• Loss of major accounts	• Brand damage • Devaluation of trade name
Loss of privacy	• Stress • Privacy violation (1 person)	• Privacy violation (hundreds of people)	• Privacy violation (thousands of people)
Harm to intellectual property	• Potential loss of competitive edge	• Affects business competitiveness	• Affects business viability

Table 7: Example of a Completed Injury Table (Non-Profit Organization)

Injury Type	Injury Level		
	Low	Medium	High
Loss of privacy	• Stress • Privacy violation (1 person)	• Privacy violation (hundreds of people)	• Privacy violation (thousands of people)
Financial harm	• Minor effect on funding	• Significant effect on funding	• Bankruptcy
Harm to reputation	• Loss of confidence	• Loss of major donors	• Brand damage
Harm to beneficiaries	• Affect program performance	• Affect program outcome	• Program viability compromised
Regulatory violation	• Minor penalty	• Significant penalty	• Brand damage • Loss of major donors

4 STEP 2: INVENTORY

The second step of the security categorization process is for the cloud consumer to create an inventory of the business processes and the information assets that are relevant to the business activity supported by the cloud-based service.

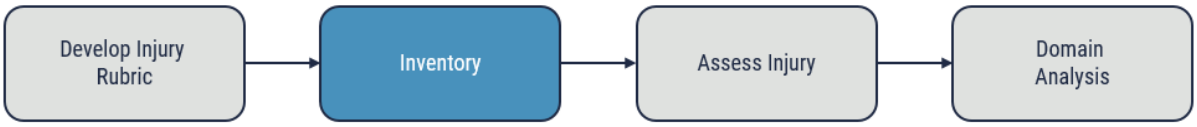


Figure 4: Security Categorization Process: Step 2 – Inventory Business Processes and Information Assets

Creating an inventory of business processes and information assets is the most important step in identifying how organizations are affected by compromises to the cloud-based services. To perform the inventory, security advisors must engage the business analyst community within the organization. The security advisor's task is to organize focus groups where possible, describe the task to be completed, emphasize the importance of contribution, and record and disseminate the results for validation.

Creating an inventory takes varying levels of preparation. If business activities are poorly documented, several focus groups may be required to obtain a coherent, valid picture of business activities. In large organizations with multiple programs, the inventory process may only be possible by dividing it up by program. If business activities are well-documented and understood, focus groups may not be required. In some cases, business processes and information assets may be well-documented, current, validated, and easily reported. In other cases, business processes and information assets must be inferred based on limited existing documentation.

Good sources to identify and describe business processes and related information assets include the following examples:

- Business cases;
- Concepts of operations;
- Business functional specifications;
- Enterprise architecture documentation which typically describes an organization's business;
- Processes and related information assets in some detail;
- Discussions or interviews with business analysts and other individuals within related business; and
- Communities.

Government of Canada departments can also look to sources such as:

- Report on plans and priorities (RPP);
- Program alignment architecture (PAA); and
- Public Accounts of Canada.

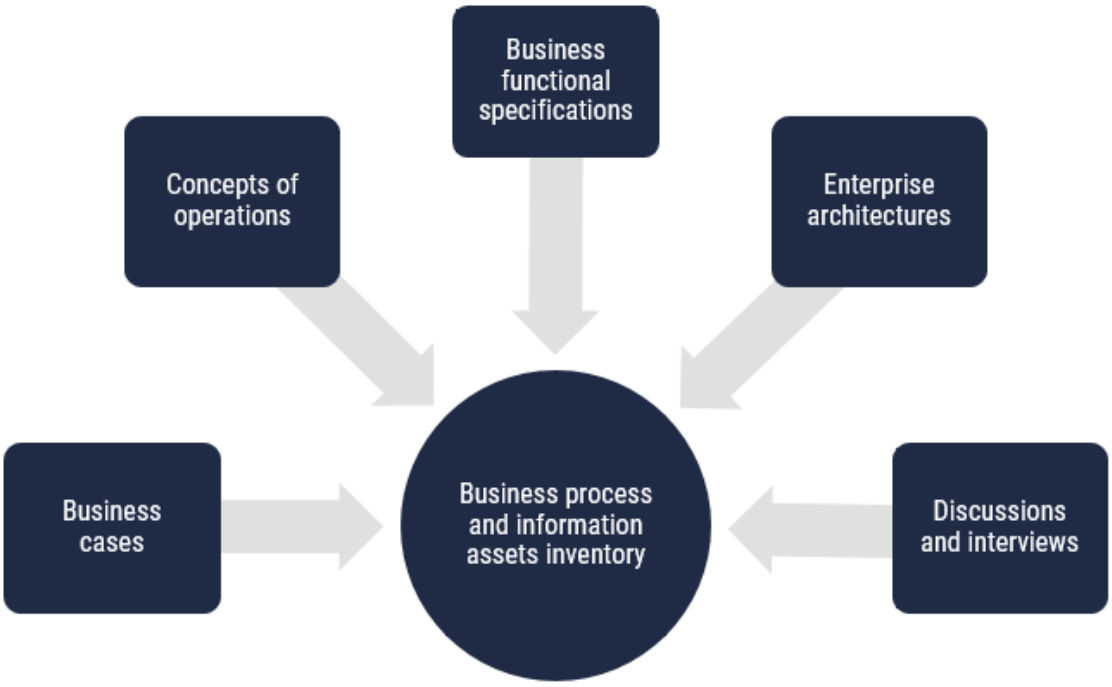


Figure 5: Inventory of Business Processes and Information Assets

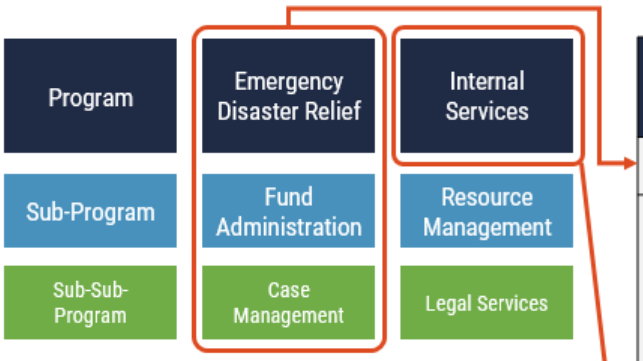
4.1 LEVEL OF DETAIL

Determining an inventory's level of detail is one complication associated with the inventory process. ITSG-33 [1] defines business activity in a generic way to give each organization the flexibility to express their business activities in the most useful way. Organizations typically determine the detail of the business process and information assets based on common factors such as the size of the organization, its range of activities, and the risk level of its business activities.

Both general and highly detailed inventory levels can provide useful insight into security categorization. While a detailed inventory might be useful in focusing security investments to the most critical business process component, it is also more sensitive to change in those business processes. A general-level inventory helps identify security requirements at the program or sub-program level, without necessarily being affected by changes to business process.

In very large organizations with multiple programs, creating an inventory of business processes and components may only be feasible by dividing it up by program, sub-program, and sub-sub-program. This provides large organizations with the required level of detail to identify security requirements at both the business process component and program levels.

Figure 6 provides an example of an inventory that is based on an organization's mission, mandate, and documented business initiatives.



Program	Sub-Program	Sub-Sub Program	Business Process	Business Process Component
Emergency Disaster Relief	Fund Administration	Case Management	Open New Case	Receive request and open new case file
			Open New Case	Requester personal information
			Open New Case	Requester non-personal information
			Open New Case	Emergency payment eligibility review
			Open New Case	Emergency payment approval
			Payment	*See payments service*
		Research and Benchmarking	Research and Benchmarking	Conduct research
			Research and Benchmarking	Research data
			Research and Benchmarking	Benchmarking data
	Appeals Management		Appeals Management	Receive and process appeal
			Appeals Management	Appeals case information
Internal Services	Resource Management	Financial Resources	Payment Service	Issue emergency payment

Figure 6: Example of a Business Process and Information Asset Inventory

4.2 ELEMENTS TO INCLUDE

Regardless of the level of detail at which the business processes and information assets are inventoried, each process and information asset is characterized by the following elements:

- Business process name or description (or even a number);
- Business process component;
- Component description;
- Type; and
- Notes.

A business activity can be a process or a grouping of processes that supports the objectives of the business. In Table 8, for example, three business processes are identified in the Case Management sub-sub-program:

- Open new case;
- Case review; and
- Payment.

Table 8: Example of a Business Activity

Inventory of Business Processes and Information Assets		
Sub-Sub Program	**Business Process**	**Business Process Component**
Case Management	Open new case	Receive request and open new case file
	Case review	Emergency payment approval
	Payment	*See Payments Service*

Business processes and information assets are described in one or more components. These components are described and given a type. In Table 9, **Requester personal information** is a component that is an information type. **Receive request and open new case file** is a process component. Your organization should define other types of business activity components to include in the inventory, as required.

Business analysts should use the **notes** column to capture assumptions, sources of inventory data, and any other information that provides context for each inventory item.

Table 9: Example of a Business Process Component

Inventory of Business Processes and Information Assets					
Sub-Sub Program	**Business Process**	**Business Process Component**	**Component Description**	**Type**	**Notes**
Case Management	Open New Case	Receive request and open new case file	The process of receiving a request for emergency funds, creating a case file, and collecting requester information	Process	
	Open New Case	Requester personal information	Name, address, phone numbers, information about family members affected, nature of emergency, social insurance number, bank account information (for direct deposit)	Information	

5 STEP 3: ASSESS INJURY

The third step of the security categorization process is to assess injury. In this step, your organization determines the expected injuries that could result from a compromise that affects each business process and information asset that you identified in the second step (inventory).

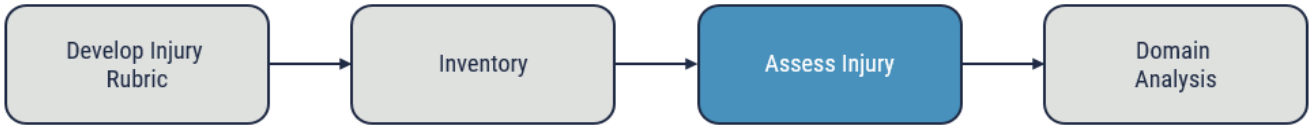


Figure 7: Security Categorization Process: Step 3 – Assess Injury

The injury assessment process should use multi-disciplinary teams that include representatives from business, legal, access to information, security, and privacy areas. You should include the business owner, or an official designate, the authorizer (if different from the business owner), the business representatives, and the analysts from each program or business line. In this document, we have given the group the collective name of **assessment committee**.

5.1 DEFINITION OF INJURY

We define *injury* in terms of the scope and scale of possible damages that result from a compromise to your organization's IT assets. Injury relates to the damages to national interests (e.g. security, political, social, economic stability) and non-national interests (e.g. safety, health, well-being, financial outcomes of Canadians and Canadian organizations). For example, in the GC, departments and agencies categorize and classify information based on the damage that could result from a compromise, which is reflected in classification and protection labels such as UNCLASSIFIED, CONFIDENTIAL, SECRET, TOP SECRET and PROTECTED A, PROTECTED B, PROTECTED C. In the private sector, injury is generally associated with profit and reputation, and information may be labelled as confidential or proprietary to reflect its level of sensitivity. Additionally, government and private industry organizations can benefit from the use of the Traffic Light Protocol (TLP) to help with information sharing. Although not defined as a level of injury, TLP is a set of colour labels (red, amber, green, and white) that are used to designate how and with whom information can be shared.

Figure 8 shows how injury is assessed with respect to the confidentiality, integrity and availability of each business activity component. See section 2.3 for definitions of each injury level (low, medium, and high).[7]

[7] This publication and the associated cloud control profile expresses injury levels as Low, Medium and High; these levels should be mapped to your classification markings. As an example, in the GC context, the injury levels are mapped in the following ways: a low injury level with UNCLASSIFIED IT assets, a medium injury level with Protected B assets, and a high injury level with Protected C assets.

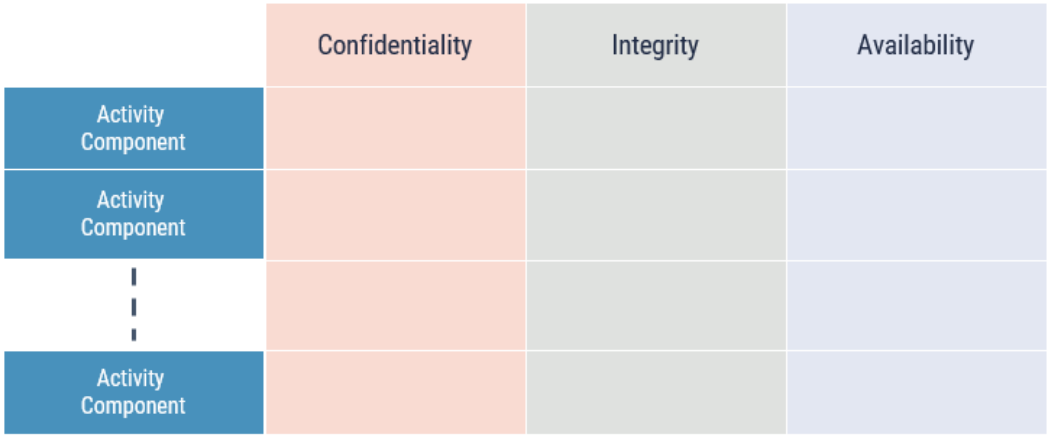


Figure 8: Injury Assessment of Security Objectives

5.2 ELEMENTS OF AN INJURY ASSESSMENT

An injury assessment includes the following steps:

1. **Failure scenario**: Identify one or more situations in which an injury could result from a failed business process or component;
2. **Injury type and level**: Select an injury type and level from the injury table;
3. **Special factors**: Modify injury level, as required, to reflect impact of special factors; and
4. **Analysis**: Provide additional notes, analysis, and justification for the selected type and level.

> **NOTE:** The four injury assessment steps are performed for each of the three security objectives (i.e. confidentiality, integrity and availability).

5.2.1 IDENTIFY FAILURE SCENARIOS

The first step you need to take when assessing injury is to document the possible failure scenarios for each business activity component. The objective of identifying these failure scenarios is to consider the possible ways in which a component can fail and cause injury. You may have more than one failure scenario for each business activity component.

You need to assess injuries for each security objective (i.e. confidentiality, integrity, and availability), but identifying the failure scenario for confidentiality does not generally apply for components that are identified as process types. In this case, the assessment committee should identify the failure scenario as not applicable (see Table 10). Note that there are exceptions if the existence of a process or its specific steps are confidential (e.g. a proprietary recipe).

Table 10: Failure Scenarios for Business Process Components

Inventory of Business Processes and Information Assets					
Business Process	**Business Process Component**	**Component Description**	**Type**	**Notes**	**Failure Scenario (in context)**
Open New Case	Receive request and open new case file	The process of receiving a request for emergency funds, creating a case file, and collecting requester information.	Process		Not Applicable
Open New Case	Requester personal information	Name, address, phone numbers, information about family members affected, nature of emergency, social insurance number, bank account information (for direct deposit)	Information		

Table 11 describes one of the most common failure scenarios: the unauthorized disclosure of information to a person with malicious intent.

Table 11: Failure Scenario – Example of Confidentiality

Inventory of Business Processes and Information Assets					
Business Process	**Business Process Component**	**Component Description**	**Type**	**Notes**	**Failure Scenario (in context)**
Open New Case	Receive request and open new case file	The process of receiving a request for emergency funds, creating a case file, and collecting requester information.	Process		Not applicable
Open New Case	Requester personal information	Name, address, phone numbers, information about family members affected, nature of emergency, social insurance number, bank account information (for direct deposit)	Information		Disclosure of personal information (including SINs) to unauthorized individual with malicious intent

The assessment committee repeats this process until the failure scenarios have been identified for all business activity components and security objectives. Table 12 provides an example of failure scenario involving the integrity of a business process component.

Table 12: Failure Scenario – Example of Integrity Objective

Inventory of Business Processes and Information Assets					
Business Process	**Business Process Component**	**Component Description**	**Type**	**Notes**	**Failure Scenario (in context)**
Open New Case	Receive request and open new case file	The process of receiving a request for emergency funds, creating a case file, and collecting requester information.	Process		Error or omission in collecting and processing information
Open New Case	Requester personal information	Name, address, phone numbers, information about family members affected, nature of emergency, social insurance number, bank account information (for direct deposit)	Information		

5.2.2 IDENTIFICATION OF INJURY TYPE AND LEVEL

The assessment committee should use an injury table to determine the possible level of injury to business activity components. Section 2 of this publication describes a process that the assessment committee can follow to develop an injury table that is representative of the organization's tolerance for injuries. That table can be used to ensure consistency when identifying injury levels. As shown in Table 13, the injury level for a business activity component is determined by the following actions:

1. Selecting the injury type related to the failure scenario (vertical axis of the injury table);
2. Selecting the qualifier on the horizontal axis that most closely represents the assessment of what could occur given the failure scenario; and
3. Selecting the injury level related to the chosen qualifier in the injury table.

You should record the resulting injury type, level, and qualifier in the inventory. Use these results to determine the overall security category of the cloud service that supports the business processes.

Table 13: Using an Injury Table to Select Injury Level

Injury Type	Qualifier and Level				
	Very Low	Low	Medium 3	High	Very High
Civil disorder or unrest	No reasonable or negligible expectation of injury	Civil disobedience, public obstructions	Riot	Sabotage affecting critical assets (e.g., critical infrastructure)	Large scale riot or sabotage requiring martial law
Physical harm to people	No reasonable or negligible expectation of injury	Physical discomfort	Physical pain, injury, trauma, hardship, illness	Physical disability, loss of life	Widespread loss of life
Psychological harm to people 1	No reasonable or negligible expectation of injury	Stress	Distress, psychological trauma 2	Causing a mental disorder or illness	Widespread psychological trauma
Financial loss to individuals	No reasonable or negligible expectation of injury	Causing stress or discomfort	Affecting quality of life	Financial security compromised	N/A
Financial loss to Canadian companies	No reasonable or negligible expectation of injury	Affecting performance	Reducing competitiveness	Viability compromised	N/A
Financial loss to the Canadian government	No reasonable or negligible expectation of injury	Affecting program performance	Affecting program outcomes	Program viability compromised	Key programs viability compromised
Harm to Canadian economy	N/A	N/A	Affecting performance	Reducing international competitiveness	Compromising key economic sectors
Harm to Canada's reputation	No reasonable or negligible expectation of injury	Loss of Canadian public confidence	Embarrassment (home or abroad)	Damage to federal-provincial relations	Damage to diplomatic or international relations
Loss of Canadian sovereignty	N/A	N/A	Impediment to the development of major government policies	Impediments to effective law enforcement Loss of continuity of government	Loss of territorial sovereignty

5.2.3 SPECIAL FACTORS

The next element of injury assessment involves considering special factors that may require your organization's assessment committee to adjust the injury level identified in the previous step. Some examples of these factors include aggregation, inference, and interdependency.

5.2.3.1 AGGREGATION

You can assign separate injury levels to individual business processes and related information assets. However, the injury that could result from a compromise of aggregate processes and information (considered as a whole) may be greater than the injury level assigned to any of the individual parts.

Aggregation refers to the situation where a collection of assets may be categorized at a higher level of sensitivity than its component parts due to the increased injury that could result from a compromise of the aggregate. In other words, aggregation is where the business impact of a compromise of a set of assets is greater than the impact of a compromise of an individual asset. Aggregation generally applies to confidentiality, but there are also circumstances in which it applies to availability and integrity.

For example, unauthorized disclosure of a single personnel file could be expected to cause some embarrassment to the individual and generate public anxiety about an organization's ability to protect personal information. However, if all human resource records for a major organization were released inappropriately, the adverse effects could be significantly worse.

From a confidentiality perspective, aggregation has two dimensions:

1. The sensitivity of a record tends to increase as more data elements are added to it; and
2. The sensitivity of the repository (file or database) tends to increase as more records are collected.

The confidentiality value of the whole may be greater than that of the individual parts, based upon the increased injury expected in the event of unauthorized disclosure.

Aggregation applies equally to availability and integrity values. For example, the destruction of one asset, such as a single server, might have clearly defined consequences, whereas the loss of an entire fleet would be much more serious. Unauthorized modification of a single record versus complete corruption of a large data base would be the integrity equivalent.

When dealing with aggregate information, organizations should reconsider each dimension of security with respect to any new injuries that might result from an aggregation. Organizations should reconsider each dimension of confidentiality, integrity, and availability with respect to the possible injury to national interests, people, and organizations.

Keep in mind that damage to national interests for an aggregate set of business components may not be obvious and should be assessed using strategic input from lead agencies.

5.2.3.2 INFERENCE

There are cases in which a threat actor could analyze information that is at one level of sensitivity and then make inferences to compromise more sensitive information. For example, personnel records categorized as Medium for privacy reasons might contain information that provides some indication of the individual's role. In this example, a threat actor may be able to learn and infer about the operational mission or capability of the parent organization, which could then be used to compromise organizational interests.

Organizations should try to consider the sensitivity of the categorized information and also other associated information that could be used by a threat actor.

5.2.3.3 INTERDEPENDENCY

Due to interdependencies, the loss or degradation of one business process and its associated information may impact other processes and related information. The purpose of analyzing interdependencies is to determine if there is a likelihood of a high cascading effect resulting from the compromise of a business process or information on other processes and information. The injury that would result from the cascading loss of one element may be greater than the injury level assigned to any of the independent elements (similar to the problem of aggregation). Types of interdependencies include physical (e.g. material output of one infrastructure used by another), geographic (e.g. common corridor), and logical (e.g. dependency through financial markets).

5.2.4 ANALYSIS

Once the injury level has been assessed, the security practitioner should capture as much essential dialogue as possible. This helps third parties to understand the rationale behind an injury type and level selection.

For example, in its analysis, the security practitioner could include a justification, document special factors that led to the identified injury level, whether any important time sensitive considerations exist, or if it is dictated by specific regulations or policies.

Table 14 provides an example of documenting the analysis activity for a business activity element.

Table 14: Injury Assessment – Sample Analysis of Business Activity Element

Loss of Availability			
What type of injury could reasonably be expected from a loss of availability?	**How significant is the expected injury?**	**Example of injuries at that level (representative)**	**Analysis**
Psychological harm to people	Low	Stress	Processing emergency payment requests efficiently and without delay is core to meeting the program's outcome. However, basic needs should be taken care of by other disaster relief efforts

5.3 SECURITY CATEGORIZATION REPORT

After completing the injury assessment, the assessment committee can choose to produce a complete or summary categorization report to communicate the results.

The assessment committee should document and formally accept the results of the security categorization activity. The results can be combined in a security categorization report as follows:

- A short description of the related business processes and information assets;
- A description of the expected injuries from threat compromise;
- The levels of expected injury as they relate to confidentiality, integrity and availability;
- The rationale for attributing the levels of injury;
- The security category of each business activity;
- The security category of a specific offering from a cloud-based service; and
- An explicit statement of acceptance of the security category from the cloud-based service owner.

Table 15 provides an example of a summary categorization report.

Table 15: Sample Summary Categorization Report

Business Domain			Security Category		
			Confidentiality	Integrity	Availability
Emergency Disaster Relief Program			Medium	Low	Low
Breakdown by Components		**Type**			
1	Receive request and open new case	Process		Low	Low
2	Requester personal information	Information	Medium	Low	Low

6 STEP 4: ANALYZE BUSINESS DOMAINS

The fourth step of security categorization is to analyze and identify business domains. A business domain is an operational environment where an organization performs business activities supporting common organizational objectives. A business domain security control profile is developed for a specific business domain as opposed to an organization as a whole. Depending on how the assessment committee has chosen to perform categorization, they may end up with several categorization reports.

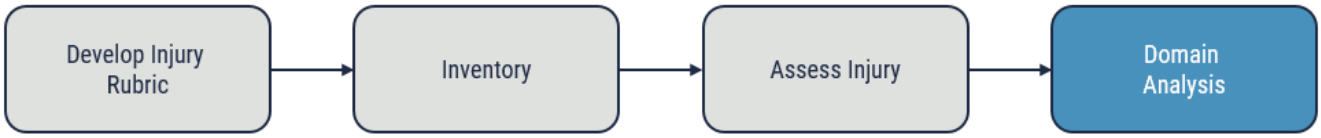


Figure 9: Security Categorization Process: Step 4 – Analyze Domains

At the end of the categorization process, the assessment committee will have one or more tables of business processes and information assets. Each process or information component will have an injury assessment with respect to confidentiality, integrity, and availability.

If all activities are to be supported by a single information system in a single domain, then the overall categorization is the high water mark[8] (the highest level of injury in each injury column as shown in Table 16).

[8] For a detailed description of the high water mark concept, see section 3.2.1 of the *Government of Canada Cloud Security Risk Management Approach and Procedures* [3]

Table 16: High Water Mark of Injury Assessment

Loss of Confidentiality				
Failure Scenario	**Reasonable Injury From Loss of Confidentiality**	**Expected Level of Injury**	**Injury Example**	**Analysis**
Release of personal information (including SIN) to unauthorized individuals with malicious intent	Psychological harm to people	**Medium**	Distress, psychological trauma	Could lead to distress and important financial losses
Release of information to unauthorized individuals with malicious intent	Psychological harm to people	**Low**	Stress	Release may include some personal information but not SIN and banking details
Loss of Integrity				
Failure Scenario	**Reasonable Injury From Loss of Integrity**	**Expected Level of Injury**	**Injury Example**	**Analysis**
Error or omission in collecting and processing information	Psychological harm to people	**Medium**	Distress, psychological trauma	Payment could be delayed as a result and lead or contribute to distress. Could also cause or increase pain and suffering
The information collected is inaccurate or incomplete	Psychological harm to people	**Medium**	Distress, psychological trauma	See above
Loss of Availability				
Failure Scenario	**Reasonable Injury From Loss of Availability**	**Expected Level of Injury**	**Injury Example**	**Analysis**
Unable to or delay in processing initial request.	Psychological harm to people	**Low**	Stress	Processing emergency payment requests efficiently and without delay is core to success of business activity
Loss or destruction of information	Psychological harm to people	**Medium**	Distress, psychological trauma	See above

A business domain can have only one security category assigned to it. The controls in a business domain security control profile are chosen to respond to a single categorization (e.g. {M, M, M}, {M, L, L}). Therefore, if organizations have several categorization reports for business activities within a domain, they will need to carefully analyze the implications of merging them.

6.1 IDENTIFICATION OF BUSINESS DOMAINS

In general, choosing the high water mark within a business domain is a reasonable approach to merging different categorization reports. However, choosing the high water mark as the categorization levels implies the need to apply more security controls, which translates into higher costs. As depicted in Figure 10, activities with unusually high categorizations can be dealt with as follows:

- **Option A:** Assuming the same threat context, develop a specific security control profile for the exception and support the business activities using a tailored information system; or
- **Option B:** Assuming the same threat context, develop a security control profile for the higher categorization and implement all other business activities on the same information system.

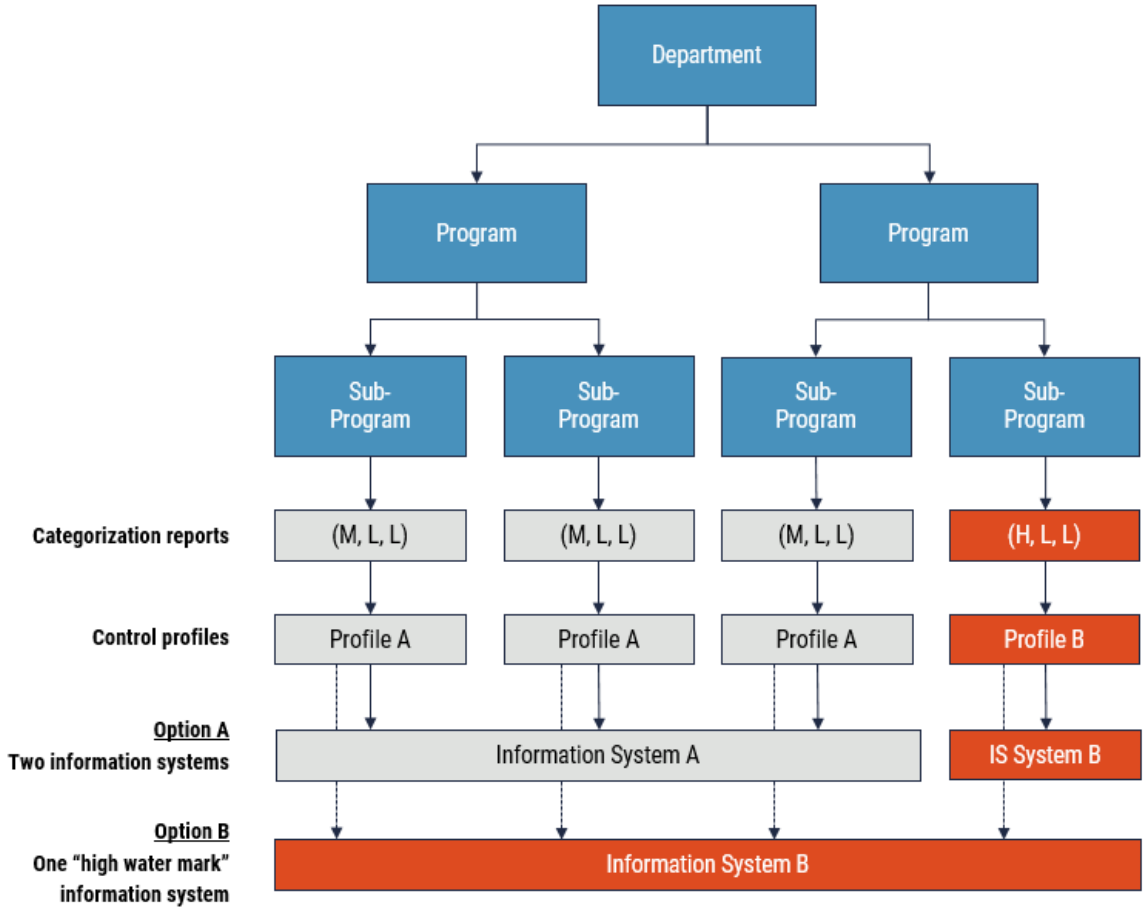


Figure 10: Security Domain Options

6.2 ENTERPRISE SERVICES

An enterprise architecture may identify applications to be used by multiple organizations (e.g. email, HR, supply).

Service providers may also offer multiple organizations or domains for the same services (e.g. Platform as a Service [PaaS], Software as a Service [SaaS]). Providers can use either the push or pull approach with respect to security categorization.

6.2.1 THE PULL APPROACH

When using the pull approach, the service provider seeks out security categorization information from each potential client and develops a profile to address the highest level of expected injury. Collecting security categorization information from multiple organizations requires time and careful planning. This effort should be carried out as part of project initiation to determine the following aspects:

- Feasibility;
- Scope; and
- Schedule and funding envelopes.

If using the pull approach, your organization should consider the following:

- Ensuring that all organizations use the same categorization template;
- Ensuring that all organizations assess injury in a consistent way; and
- Achieving the overall categorization may not be possible given the budget or schedule. Significant changes in proposed scope may be required (e.g. off-boarding organizations, securing additional funding).

6.2.2 THE PUSH APPROACH

When using the push approach, the service provider sets the categorization of the application or service and develops a profile to address the highest level of expected injury. The application or service is categorized as a business decision. For non-essential applications or services, organizations can compare their needs against the offering and on-board as appropriate. For essential applications or services (e.g. corporate driven initiatives), organizations must compare their needs against the service offering and address areas of risk.

If using the push approach, your organization should consider the following:

- That providers must supply **all** security assurance artefacts or client organizations cannot determine areas of residual risk.
- That for essential applications or services, it is important that the security category be established based on a comprehensive understanding of the business domain (this may be achieved by exercising a pull approach).

7 SELECT A SECURITY CONTROL PROFILE

Security control profiles have been developed for the cloud-based services that were derived from the baseline profiles in Annex 4 of ITSG-33 [1]. The cloud security control profiles identify the recommended security controls that the CSPs and cloud consumers should jointly implement for the assessed security category of each respective business domain. The selected cloud control profile also serves as the basis for assessment of the security controls.

You organization should select one of the cloud security control profiles that the Cyber Centre has developed. These control profiles are included in Annex A and Annex B of this publication. When selecting a cloud security control profile, your organization's project authorities, with the support of security practitioners, should perform the following four tasks[9]:

1. Validate the applicability of the business context;
2. Validate the applicability of the technical context;
3. Validate the applicability of the threat context; and
4. Tailor the security controls within their scope of responsibility according to their needs.

The business context documented for each cloud security control profile identifies security category that can be supported by the profile. After completing the security categorization of the business activities, the cloud consumers select the security control profile that matches the security category of the applicable business domain.

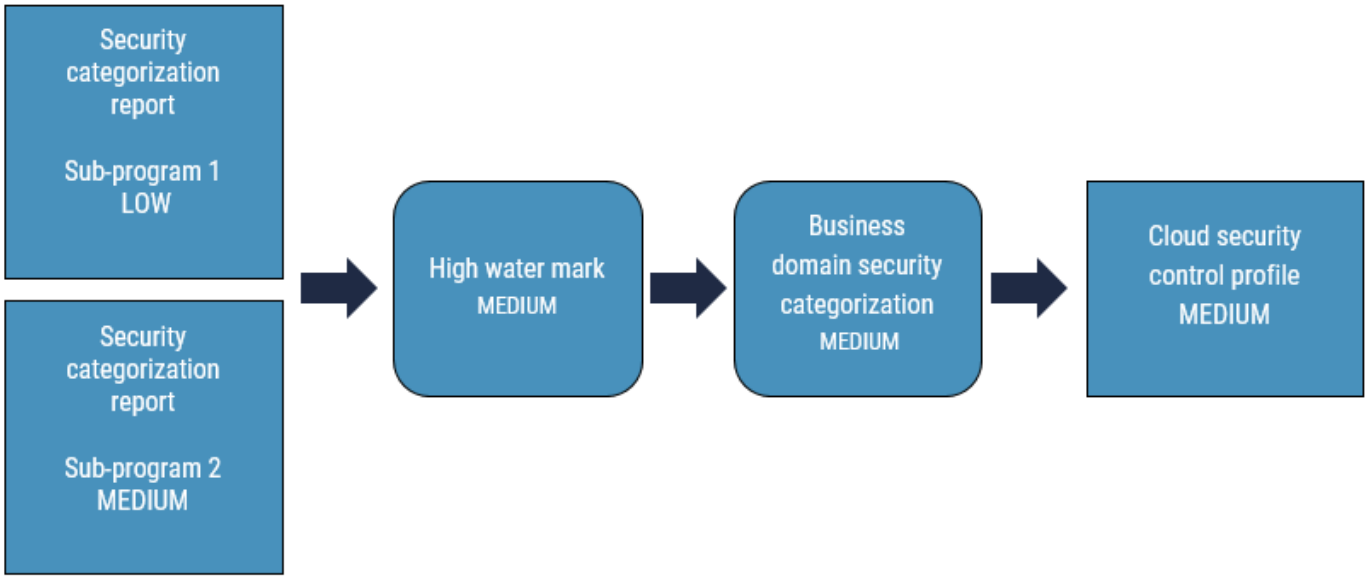


Figure 11: Selection of Cloud Security Control Profile

[9] Government of Canada *Cloud Security Risk Management Approach and Procedures* [3]

7.1 BUSINESS CONTEXT

Two cloud control profiles are included that you can use if you are implementing cloud-based services to support business activities that you have categorized as Low and Medium. If you have business activities that you have categorized with a high security category, contact the Cyber Centre for the recommended cloud security control profile.

7.2 TECHNICAL CONTEXT

The appendices include technical context for the cloud control profiles, which are defined by the cloud deployment and service models, the CSP offerings, and the organizational cloud-based services.

The technical context is dictated largely by the CSP cloud service offerings. There are no limits to what that context may be. The cloud control profiles neither recommend nor exclude any particular technologies, and it should generally be suitable for any technical context provided by CSPs in their cloud service offerings.[10]

7.3 THREAT CONTEXT

Currently, there are few public CSPs that provide information security services with sufficient assurance to defend consistently against threats higher than Td4 deliberate threat actors, Ta3 accidental and natural threats as defined in ITSG-33 [1]. Briefly, Td4 represents risk-adverse threat actors such as sophisticated hackers who have the knowledge, abilities, and experience required to customize and use available tools to exploit system weaknesses, find unknown vulnerabilities, or develop limited exploits for organizational exposures. Ta3 accidental threats and natural hazards include incidents such as significant disruption of telecommunication services, long-term power failures, localized flooding, and facility damage from earthquakes.

If your organization needs to protect business activities against threat actors categorized as higher than Td4 and Ta3, you should take one of the following actions.

- Apply additional tailoring to the control profiles included in the annexes;
- Accept higher levels of residual risk; or
- Select a different control profile.

For further guidance, contact the Cyber Centre.

[10] *Government of Canada Security Control Profile for Cloud-Based GC Services*

7.4 TAILORING

The cloud security control profiles included in this publication represent baseline security controls for protecting your organization's business activities. You should tailor the cloud security control profile to address unique threats, technical limitations, business requirements, legislation, regulations, or policies that apply to your business context.

Your organization should consider filling in CSP security control gaps with your own controls or by choosing a different CSP. Your ability to fill the gaps with your own controls is very high for Infrastructure as a Service (IaaS) and less so for Software as a Service (SaaS).[11] For the PaaS model, the security control gap is similar to IaaS.

You should tailor the security control profile to address unique threats, requirements, and gaps. This is done by incorporating compensating controls, control enhancements or organization specific control parameters. You should document the rationale for all tailoring activities and associated tailoring decisions.

The cloud security control profiles included in annexes A and B contain control allocations. The allocations indicate who is responsible (either CSP or consumer) for the security requirements of the control profile. Control allocations by service model are also provided.

7.5 CONTROL ALLOCATIONS

Annexes A and B, an "X" in columns K, L, M, or N of the spreadsheets indicates whether the CSP or your organization is responsible for the security requirements described in the selected security control.

With IaaS and PaaS service models, your organization is responsible for the security requirements of organizationally configured and managed systems in the cloud, and all customer information systems used to access, manage, protect, or defend the associated cloud services. With a SaaS service model, you are responsible for the security requirements for all your organization's information systems that are used to access and manage the associated cloud services.

CSP responsibilities for each service model also include the security requirements for the supporting services. For example, the CSP's responsibilities for its SaaS also include the security requirements for the IaaS and PaaS systems that support that SaaS. However, it is likely that other, existing assessments of the supporting services can be re-used when determining if the CSP has met their IT security responsibilities for the supported service.

[11] Cloud Security Alliance. *Security Guidance for Critical Areas of Focus in Cloud Computing V4.0* [9].

8 SELECT A CLOUD DEPLOYMENT MODEL AND A CLOUD SERVICE MODEL

When moving to the cloud, you need to determine the appropriate cloud deployment model and cloud service model for your organization's IT services. Cloud deployment models describe the relationship between you and the CSP. There are four cloud deployment models identified by NIST: public, private, community, and hybrid. There are three cloud service models defined by NIST: Infrastructure as a Service, Platform as a Service, and Software as a Service. Figure 12 outlines the three cloud service models. *Special Publication 800-145 NIST Definition of Cloud Computing* [10] defines the cloud deployment models and cloud service models.

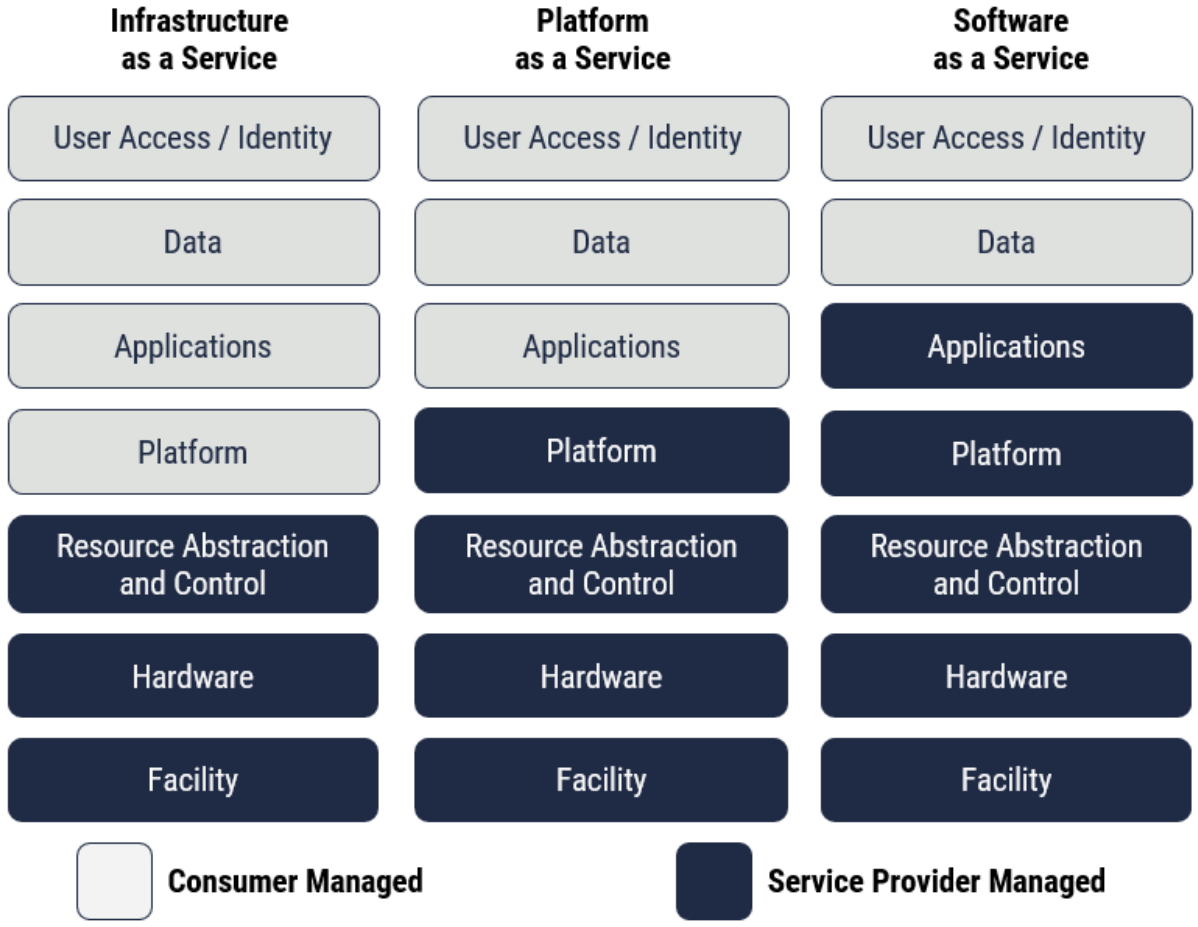


Figure 12: Cloud Service Models

Your selection of a cloud deployment model and a service model will depend on the nature of the services you require, the amount of control you want to retain, and the level of expertise and maturity the consumer has in operating and maintaining cloud-based information system environments.

The information aggregated during the security categorization step helps the cloud consumer select the cloud deployment model and the cloud service model that best match its internal expertise and required assurance levels. Your organization should select models that have been assessed to meet your required security category requirements.

Your organization should select a deployment model and a service model that require the least amount of control tailoring and compensating controls to address shortcomings in the CSP security control implementation. As identified in section 6.1, your ability to address CSP security control gaps with your organization's controls is very high for IaaS and less so for SaaS.

As shown in Figure 13, you should select or confirm which a deployment model and a service model that best suits your organization based on the following considerations:

- The consumer organization's information system strategies;
- The CSP cloud services capabilities and security control gaps;
- The security category of the business process to be supported by the cloud service;
- The selected security control profile requirements; and
- Other aspects of the information system workloads.

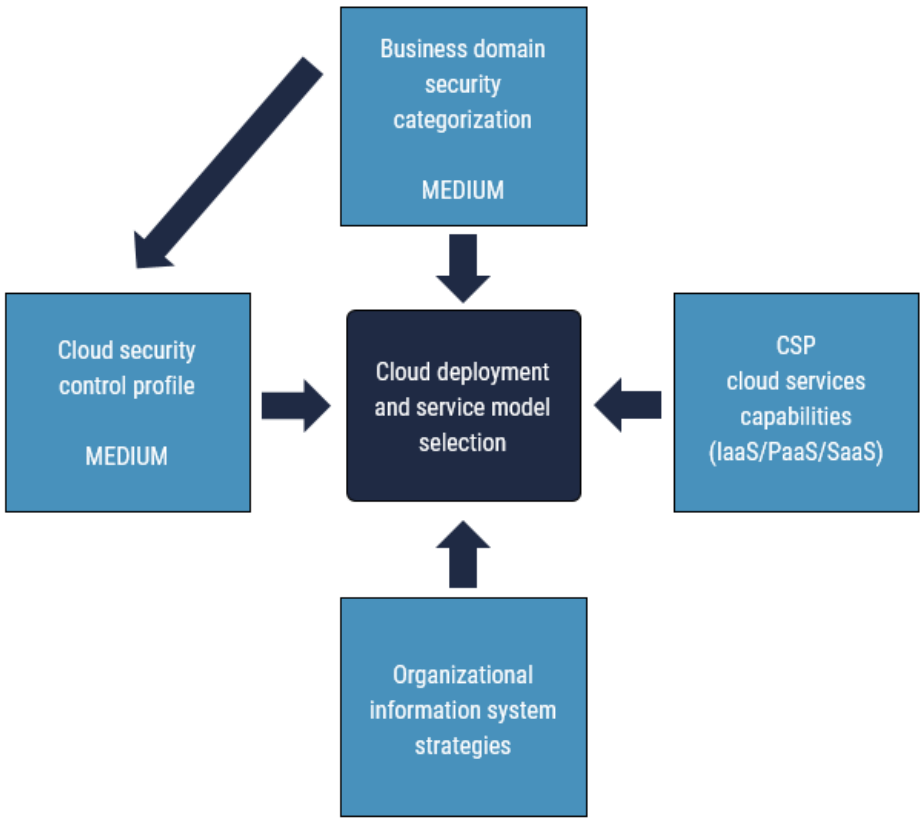


Figure 13: Cloud Deployment and Service Model Selection

8.1 CLOUD DEPLOYMENT MODELS

When selecting a cloud deployment model, you should consider a number of factors, including: flexibility, security, scalability, cost, automation, level of control over the infrastructure, locality, and service levels offered by each deployment model[12]. In figure 14, on premises refers to the software and technology located within the physical confines of your organization. Off premises refers to the software and technology located outside the physical confines of your organization.

The following sections provide definitions, advantages and disadvantages for each deployment model. A summary of advantages and disadvantages for each deployment model is provided in Annex C.

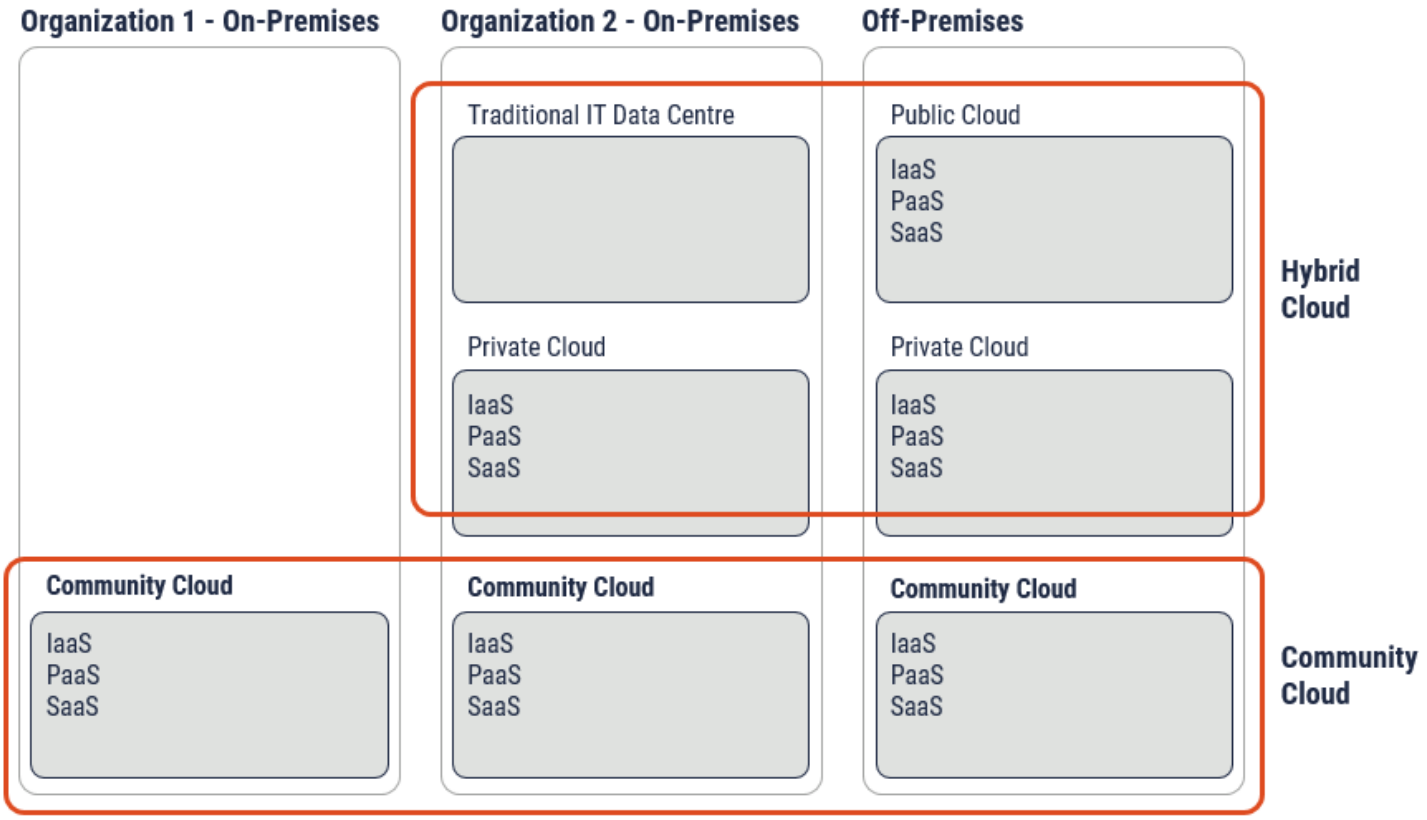


Figure 14: Cloud Deployment Models

8.1.1 PUBLIC DEPLOYMENT MODEL

In the public cloud deployment model, the cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

[12] Cloud Standard Customer Council. *Practical Guide to Hybrid Computing* [11].

The scalability (scale up) and elasticity (scale out) capabilities offered by public deployment provides the most flexibility to meet organizations sudden peak in demands and will translate into increased reliability upon hardware failures.

In this deployment model, CSPs have well defined, standardized cloud services, security capability offerings and service level agreements. While the standardized nature of these services allows CSPs to provide the services at a lower cost, organizations are not likely to find very much flexibility in negotiating the customization of services, operational processes, or service level agreements. If your organization has very strict security, operational, or governance requirements, you may need to implement compensatory controls to address gaps in the CSP's offerings. You should consider other deployment models if possible.

The public cloud deployment model offers a multi-tenant environment. Multi-tenancy does not allow for your organization to audit the security posture of the CSP environment. Instead, you must rely on third-party assessments when considering the use of public clouds.

The services offered by public cloud providers can change very rapidly. These new services may be assessed by third party assessors only in the next assessment cycle. Before using these new services, you should ensure that the security of the new services being offered by the CSPs have been assessed by third-party assessors.

8.1.2 PRIVATE DEPLOYMENT MODEL

In the private cloud deployment model, the cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g. business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

In this deployment model, organizations will find more flexibility in negotiating services, operational processes, service level agreements, security, and governance requirements. This flexibility usually comes at a higher cost and organizations may be restricted to what was negotiated in the contract.

Organizations requiring very high scalability, elasticity, or advanced features too costly to implement on premises may want to consider the public deployment model.

8.1.3 HYBRID DEPLOYMENT MODEL

NIST describes the hybrid model as an environment composed of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability. The combination of on-premises IT infrastructure with one or more of public, private or community cloud is sometimes referred to as hybrid cloud.

Hybrid clouds provide some of the benefits of both public and private clouds and are often used by organizations as the first step in their migration to the cloud. It allows organizations to deploy workloads with more stringent security requirements on premises while deploying workloads requiring significant IT resources processing, scalability and elasticity on public cloud.

The hybrid cloud model comes with added complexity. For example, organizations will have to perform a security assessment of multiple CSPs, determine which security features to use from each cloud, how to manage resources from different CSPs, determine location of resources, and how to interconnect the different cloud environments securely.

8.1.4 COMMUNITY DEPLOYMENT MODEL

A community cloud is provisioned for the exclusive use of a specific community of consumers from organizations that have shared concerns (e.g. mission, security requirements, policy, or compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises. The costs are spread over fewer users than a public cloud but more than would be for a private cloud, so only some of the potential cost savings of cloud computing are achieved.

Despite not offering the same savings as the public deployment model, community clouds can provide considerable economies of scale advantages and some of the flexibility found in private clouds.

If your organization is considering a community cloud, you should determine how, and by who, availability and service outages will be managed. You should also consider the implications of having your organization's data spread across multiple organizations and, possibly, different locations.

8.2 CLOUD SERVICE MODELS

Your selection of a cloud deployment and service model may be motivated by the following considerations:

- The nature of the service;
- The amount of control your organization wants to retain; and
- The level of expertise and maturity of the consumer organization has in operating and maintaining cloud-based information system environments.

NIST defines the following three service models:

- **SaaS** provides the consumer with the capability 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.
- **PaaS** provides the consumer with the capability to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming, libraries, services, and tools supported by the provider.
- **IaaS** provides the consumer with the capability to provision processing, storage, networks, and other fundamental computing resources where the consumer can deploy and run arbitrary software, which can include operating systems and applications.

In the IaaS model, cloud consumers carry more responsibilities then in the PaaS and SaaS models.
Also, the ability for organizations to tailor, implement and manage their own security controls is very high for IaaS, and lower for PaaS and SaaS.[13]

9 SUMMARY

Your organization is required to perform security categorization of your business processes and information assets. By categorizing your business processes and information assets, you can better select a security control profile and cloud deployment and service models.

This document outlines the required security categorization activities that you need to perform when adopting cloud services. This publication also recommends security control profiles to support Low and Medium security category business domains.

9.1 CONTACTS AND ASSISTANCE

If your organizations needs more guidance on cloud services, please contact us:

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

[13] The annexes in this document include security control profiles, which provide control allocations to indicate where the CSP or cloud customer are responsible for the security requirements described in the selected security control profile. Control allocation by service model is also provided.

10 SUPPORTING CONTENT

10.1 LIST OF ABBREVIATIONS

Term	Definition
Cyber Centre	Canadian Centre for Cyber Security
CSE	Communications Security Establishment
CSP	Cloud Service Provider
GC	Government of Canada
IaaS	Infrastructure as a Service
IT	Information Technology
ITSP	Information Technology Security Practitioner
PAA	Program Alignment Architecture
PaaS	Platform as a Service
RPP	Report on Plans and Priorities
SaaS	Software as a Service
SDLC	System Development Lifecycle
SLA	Service level agreement
SPIN	Security Policy Implementation Notice

10.2 GLOSSARY

Term	Definition
Assessment committee	Multidisciplinary team that includes representatives from business, legal, access to information, security, and privacy areas. It should include the business owner or her/his official designate; the authorizer (if different from the business owner); business representatives and analysts from each program or business line.
Availability	The state of being accessible and usable in a timely and reliable manner.
Business domain	A business domain is an operational environment where a department performs business activities supporting common organizational objectives.
Business domain security control profile	A business domain security control profile is developed for a specific business domain as opposed to an organization as a whole.
Cloud consumer organization	Any organization that wishes to acquire cloud based services through a CSP.
Cloud service provider	Any commercial provider of cloud services that wishes to offer its services to consumers.
Compromise	The intentional or unintentional disclosure of information, which adversely impacts its confidentiality, integrity, or availability.
Confidentiality	The state of being disclosed only to authorized principals.
Impact	A term that is generally taken to imply both injury and consequence. Business impact and mission impact are often used in this sense.
Injury	The damage to the national interests and non-national interests that business activities serve resulting from the compromise of IT assets.
Integrity	The ability to protect information from being modified or deleted unintentionally or when it is not supposed to be. Integrity helps determine that information is what it claims to be. Integrity also applies to business processes, software application logic, hardware, and personnel.
National interest	The damage affects the security and the social, political, and economic stability of Canada.
On premises	Refers to the software and technology located within the physical confines of your organization.
Off premises	Refers to the software and technology located outside the physical confines of your organization.
Non-National Interest	The damage affects the safety, health, and well-being of individuals, and the financial position and reputation of individuals and Canadian companies.
Security advisor	An individual or team possessing the broad knowledge and experience required to make and elaborate risk management recommendations to a departmental authorizer.
Security categorization	Process of identifying the potential injuries that could result from compromises of business processes and related information assets.

10.3 REFERENCES

Number	Reference
1	Canadian Centre for Cyber Security. *ITSG-33 IT Security Risk Management: A Lifecycle Approach*. December 2014.
2	Canadian Centre for Cyber Security. *ITSM.50.062 Cloud Security Risk Management*. March 2019.
3	Treasury Board of Canada Secretariat. *Government of Canada Cloud Security Risk Management Approach and Procedures*. 25 June 2018.
4	Treasury Board of Canada Secretariat. *Government of Canada Cloud Adoption Strategy*. n. d.
5	Treasury Board of Canada Secretariat. *Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice (SPIN)*. 1 November 2017.
6	Treasury Board of Canada Secretariat. *Policy on Service and Digital*. 1 April 2020.
7	*Personal Information Protection and Electronic Documents Act.* S.C. 2000, c.5.
8	National Institute of Standards and Technology. *Special Publication 800-60 Guide for Mapping Types of Information and Information Systems to Security Categories.* Vol 1, Rev 1. August 2008.
9	Cloud Security Alliance. *Security Guidance for Critical Areas of Focus in Cloud Computing*. v4.0. 2017.
10	National Institute of Standards and Technology. *Special Publication 800-145 The NIST Definition of Cloud Computing*. September 2011.
11	Cloud Standard Customer Council. *Practical Guide to Hybrid Computing*. February 2016.
12	National Institute of Standards and Technology. *Special Publication 800-146 Cloud Computing Synopsis and Recommendations*. May 2012.

Annex A Cloud Control Profile – Low

For more information, please see Annex A Cyber Centre LOW Cloud Profile Recommendations.

Annex B Cloud Control Profile – Medium

For more information, please see Excel file, Annex B Cyber Centre MEDIUM Cloud Profile Recommendations.

Annex C Summary of Considerations for Cloud Deployment Model Selection[14]

	Public	Private (on-premises)	Hybrid	Community (on-premises)
Location	• Hidden from the cloud consumer unless the provider has offered (optional) location restriction policies and the consumer has configured their account to request specific location restrictions.	• The cloud consumer chooses the physical infrastructure in which the private cloud operates and determines the possible geographical locations of workloads	• The cloud consumer determines geographical locations of workload via on-premises hosting or CSP location restriction policies	• Workloads normally remain within participant organizations (unless outsourced)
Upfront investment	• Low	• Significant-to-high[15]	• Investment minimized by hosting non-mission critical workloads requiring high elasticity and scalability in public clouds	• Significant-to-high
Complexity	• Significant	• Modest to significant	• Significant to high	• Identity and access control configurations among the participant organizations may be complex
Contract and service level agreement (SLA)	• The default SLA specify limited promises, remedies to cloud consumers • Limited room for negotiation	• More flexibility for SLA and contract negotiation • May be restricted to what was negotiated in the contract	• May require management of multiple contracts and SLA	• More flexibility for SLA and contract negotiation • May be restricted to what was negotiated in the contract • The cloud consumer should determine how, and by who, availability and service outages will be managed

[14] Based on NIST *Special Publication 800-146 Cloud Computing Synopsis and Recommendations* [12].

[15] In the outsourced private cloud model, the resources are provisioned by the provider. Upfront costs for the consumer organization can be modest to significant and include SLA negotiation, network connectivity costs, application conversion to cloud, and training.

	Public	Private (on-premises)	Hybrid	Community (on-premises)
Required IT skills	• Cloud consumers will need the traditional IT skills required to manage user devices and will require new cloud IT skills as well	• Cloud consumers will need the traditional IT skills required to manage user devices and will require new cloud IT skills as well • Provider organization requires skills to implement and manage cloud infrastructure	• Cloud consumers will need the traditional IT skills required to manage user devices and will require new cloud IT skills for multiple clouds	• Cloud consumers will need the traditional IT skills required to manage user devices and will require new cloud IT skills as well • Provider organization will require skills to implement and manage cloud infrastructure
Risks from multi-tenancy	• A single machine may be shared by the workloads of any combination of consumers. In practice, this means that a consumer's workload may be co-resident with the workloads of competitors or adversaries	• Risks somewhat mitigated by restricting the number of possible attackers • All of the clients would typically be members of the consumer organization or authorized guests or partners	• Cloud consumers can host mission critical workloads on premises and other workloads in other cloud deployment models to lower costs and benefit for elasticity, bursting capabilities	• Mitigates some of the multi-tenancy risks by restricting the number of possible attackers. • The cloud encompasses more organizations and so may restrict the set of potential attackers less than in the case of the on-site private cloud
Security from external threats	• Cloud consumers with very strict security, operational or governance requirements may require implementation of compensating controls to address gaps in the CSP offering	• The cloud consumer has the option of implementing an appropriately strong security perimeter to protect private cloud resources against external threats to the same level of security achieved for non-cloud resources[16]	• The cloud consumer typically deploys workloads with more stringent security requirements on premises. The consumer has the option of implementing an appropriately strong security perimeter for these workloads	• The security from external threats depends on the security of all the security perimeters of the participant organizations and the strength of the communications links
Visibility and control	• Limited	• High	• High for on-premises hosted workloads.	• High

[16] The main difference with the outsourced private cloud is that the techniques need to be applied both to a consumer's perimeter and to a provider's perimeter, and that the communications link needs to be protected.

	Public	Private (on-premises)	Hybrid	Community (on-premises)
Elasticity	• Generally, unrestricted in location or size. • Unique advantages in achieving elasticity, or the illusion (to consumers) of unlimited resource availability	• Fixed computing and storage capacity that has been sized to correspond to anticipated workloads and cost restrictions	• Cloud consumers typically deploy more stringent security requirements on premises while deploying workloads requiring significant IT resources processing, scalability and elasticity on public cloud	• Fixed computing and storage capacity that has been sized to correspond to anticipated workloads and cost restrictions