



Communications
Security Establishment

Centre de la sécurité
des télécommunications

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

Cyber security and privacy risk management: A lifecycle approach

Organizational cyber security and privacy risk management activities

Practitioner

Foreword

Organizational cyber security and privacy risk management activities (ITSP.10.036) is an unclassified publication issued under the authority of the Head, Canadian Centre for Cyber Security (Cyber Centre).

This publication supersedes IT security risk management: A lifecycle approach (ITSG-33), Annex 1 - Departmental IT security risk management activities.

For more information or to suggest amendments, contact the Cyber Centre:

- by email: contact@cyber.gc.ca
- by phone: [613-949-7048](tel:613-949-7048) or [1-833-CYBER-88](tel:1-833-CYBER-88)

Effective date

This publication takes effect on September 14, 2026.

Revision history

Revision	Amendments	Date
1	First release	September 14, 2026

D97-3/10-036-2026E-PDF

ISBN 978-1-100-00240-8

Overview

This publication is part of a series of guidelines published by the Cyber Centre, under Cyber security and privacy risk management: A lifecycle approach. This publication describes a cyber security and privacy risk management process that includes activities at the organizational level.

This publication is a tool to assist security and privacy practitioners in their efforts to protect organizations in compliance with applicable legislation, policies, directives and standards. It outlines a risk management framework designed to ensure that organizations effectively manage risks and obtain approval from the appropriate authorities on those risks.

This publication focuses on 4 key objectives that guide organizations in effectively managing risks and ensuring compliance:

- Identify and understand the cyber security and privacy needs of organizational programs and services and select a set of tailored controls and activities that meet these needs
- Allocate security controls that satisfy cyber security and privacy needs and the cyber security and risk management requirements of applicable legislation, policies, directives, and standards (for the Government of Canada (GC), namely Treasury Board of Canada Secretariat (TBS) policy instruments)
- Continuously monitor and assess the performance of organizational security and privacy controls and activities to detect incidents and identify vulnerabilities and deficiencies in a timely manner
- Update implemented controls and activities to respond to incidents, correct vulnerabilities, and continuously improve the cyber security and privacy posture of organizational systems

GC-specific note

In the GC, adherence to the Cyber security and privacy risk management: A lifecycle approach guidelines has many benefits for organizations, including:

- compliance with the overall risk management strategy and objectives established by TBS
- addressing key aspects of cyber security and privacy
- managing cyber security and privacy risks, all in an efficient, consistent and cost-effective manner

Table of contents

1	Introduction	7
1.1	Purpose	7
1.2	Context in the Government of Canada	7
1.3	Scope and applicability	8
1.4	Audience.....	8
1.5	Publication taxonomy	9
1.6	Publication organization	10
2	Cyber security and privacy risk management process	11
3	Relationships with external processes	14
4	Organizational cyber security and privacy risk management activities	15
4.1	Define organizational cyber security and privacy needs.....	17
4.1.1	Define the scope of the cyber security and privacy risk assessment activities	18
4.1.2	Identify business needs for security and privacy.....	18
4.1.3	Perform injury assessment and categorization of organizational business activities.....	19
4.1.4	Select organizational cyber security threat and risk assessment methodology	19
4.1.5	Select the organizational privacy assessment methodology.....	20
4.1.6	Conduct an organizational cyber security threat assessment	20
4.2	Develop organizational security and privacy control and activity profiles	21
4.2.1	Define business domains	22
4.2.2	Define security architecture approaches	23
4.2.3	Select organizational security and privacy controls and activities	24
4.2.4	Approve the organizational profile(s)	26
4.3	Allocate security and privacy controls and activities	26
4.3.1	Allocate common controls and activities.....	26
4.3.2	Allocate system-specific controls and activities	27
4.4	Monitor and assess performance of security and privacy controls and activities	28
4.5	Maintain authorization.....	28
4.6	Update security and privacy controls and activities profile(s)	30

5	Injury assessment and categorization process	31
5.1	Concepts	31
5.1.1	National security systems	31
5.1.2	Safety	32
5.1.3	Privacy	32
5.1.4	Adversarial perspective	32
5.1.5	Post-compromise injury	33
5.2	Injury assessment and categorization process	33
5.3	Injury assessment and categorization process description	36
5.3.1	Develop organization-specific injury assessment table	37
5.3.2	Identify business processes and related information assets	39
5.3.3	Assess injuries from threat compromise	40
5.3.4	Determine injury category of each business activity	41
5.3.5	Prepare injury categorization report	42
5.4	Examples	42

List of figures

Figure 1:	Cyber security and privacy risk management process	11
Figure 2:	Organizational cyber security and privacy risk management activities	16
Figure 3:	Injury assessment and categorization process	34

List of tables

Table 1:	Examples of common controls and activities allocation	27
Table 2:	Examples of injury types and levels (GC-centric)	37
Table 3:	Examples of injury types and levels	38
Table 4:	Confidentiality – Non-national interest (Protected)	43
Table 5:	Confidentiality – National interest (Classified)	43

Table 6: Integrity and availability	43
---	----

List of annexes

Annex A Government of Canada injury levels conversion	43
---	----

1 Introduction

The process described in this publication outlines a risk management framework designed to ensure that organizations effectively manage cyber security and privacy risks and obtain approval from the appropriate authorities for those risks. This publication also provides specifications on how to conduct injury assessment and categorization as part of risk management. The process described in this publication can be adapted to fit your organization's needs.

1.1 Purpose

This publication is part of a series of guidelines published by the Cyber Centre, under Cyber security and privacy risk management: A lifecycle approach. It aims to support organizations in implementing a structured risk management approach. This publication outlines a set of activities to help organizations determine and achieve an appropriate level of security, aligned with business requirements and operational context. It also provides guidance on structuring a security assessment and authorization (SA&A) framework, which formalizes how cyber security risks are assessed, documented, and managed across an organization. It describes how to conduct an injury assessment and categorization of the organization's business processes and related information based on the potential impacts to confidentiality, integrity and availability (CIA).

1.2 Context in the Government of Canada

In the [TBS Directive on Security Management](#) (DSM), TBS assigns to senior officials in the department's security governance the responsibility for participating in and reporting to the department as well as assigning security responsibilities for programs, services and activities.

The TBS DSM instructs senior officials in a department's security governance to identify security requirements and related resource needs for programs. It also advises them to ensure that security practices and security controls are defined, documented, implemented, monitored and maintained to meet identified security requirements for programs, services and activities. These senior officials shall document or recommend actions to be taken regarding residual risks for programs, services and activities. They need to establish processes to monitor, respond to, and report threats, vulnerabilities, security incidents and other security events. They are required to address security events that could impact programs, services and activities or that require an immediate or coordinated government-wide action. They must monitor and report on the effectiveness of security practices and controls and share the results with the chief security officer (CSO).

The federal [Privacy Act](#), along with the [TBS privacy governance suite](#), assigns responsibility for ensuring compliance with legislative and policy requirements to senior officials and information custodians overseeing programs that collect and use personal information. Additionally, the responsibility for assessing compliance with these activities is assigned to the head of the government organization, although this role is often delegated in practice to a senior official.

The management of cyber security risks overlaps with the management of privacy risks as data containing personal information is increasingly present in information systems throughout the data lifecycle. Privacy breaches can arise from cyber security incidents when there is a loss of confidentiality and/or integrity during data processing. This publication addresses the privacy risks as they relate to cyber systems only.

[Security and privacy controls and assurance activities catalogue \(ITSP.10.033\)](#) now includes privacy controls and activities to ensure that government institutions protect and manage personal information. These new additions help identify, assess, monitor and mitigate compliance gaps in programs and activities involving the collection, creation, retention, use, disclosure and disposal of personal information. Additionally, they aim to ensure that privacy is architected and then engineered into the design and operation of GC information systems.

Organizations use the [TBS Directive on Privacy Practices, Appendix C: Standard on Privacy Impact Assessment](#) to support this objective by ensuring that privacy implications are appropriately identified, assessed and resolved before a new or substantially modified program or activity involving personal information is implemented. The privacy impact assessment (PIA) is the component of risk management that focuses on ensuring compliance with the *Privacy Act* requirements. It also assesses the privacy implications of new or substantially modified programs and activities involving personal information. PIAs should be conducted in a manner that is commensurate with the privacy impact identified and respects the operating environment of the government institution.

1.3 Scope and applicability

This publication provides guidelines to organizations on the cyber security and privacy risk management activities that are performed by cyber security and privacy functions as part of an organizational cyber security program. System lifecycle cyber security and privacy risk management activities (ITSP.10.037) provides guidelines on the cyber security and privacy risk management activities that are performed at the system level.

Adherence to these guidelines presents many benefits for organizations. These include adhering to established risk management strategy and objectives, addressing key aspects of cyber security and privacy in an efficient manner, and consistently and cost-effectively managing cyber security and privacy risks.

GC-specific note

The guidelines in this publication apply to departments¹ subject to the [TBS Policy on Government Security \(PGS\)](#) that rely on information systems to support non-critical to critical departmental business programs, services, and activities in Unclassified, Protected, and Classified environments. Compliance with the requirements in the PGS and its supporting instruments is mandatory for designated federal departments.

1.4 Audience

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

- individuals with enterprise-level responsibilities, including enterprise architects and enterprise security architects
- individuals with system-development responsibilities, including mission or business owners, program managers, system engineers, system security engineers, privacy practitioners, hardware and software developers, system integrators, and acquisition or procurement officials or executives

¹ Departments as defined in section 2 and entities included in Schedules IV and V of the [Financial Administration Act](#), unless excluded by specific acts, regulations or orders in council.

- individuals with logistical or disposition-related responsibilities, including program managers, procurement officials or executives, system integrators, and property managers
- individuals with security and privacy implementation and operations responsibilities, including mission or business owners, system owners, information custodians, system administrators, continuity planners and system security or privacy officers
- individuals with security and privacy assessment and monitoring responsibilities, including auditors, system evaluators, control assessors, independent verifiers and validators and analysts
- security and privacy officials or executives (for example, chief information officers (CIOs), CSOs, and chief privacy officers (CPOs))
- commercial entities, including industry partners, that produce component products and systems, create security and privacy technologies, or provide services or capabilities that support cyber security or privacy

GC-specific note

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

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

1.5 Publication taxonomy

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

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

1.6 Publication organization

The remainder of this publication is organized as follows:

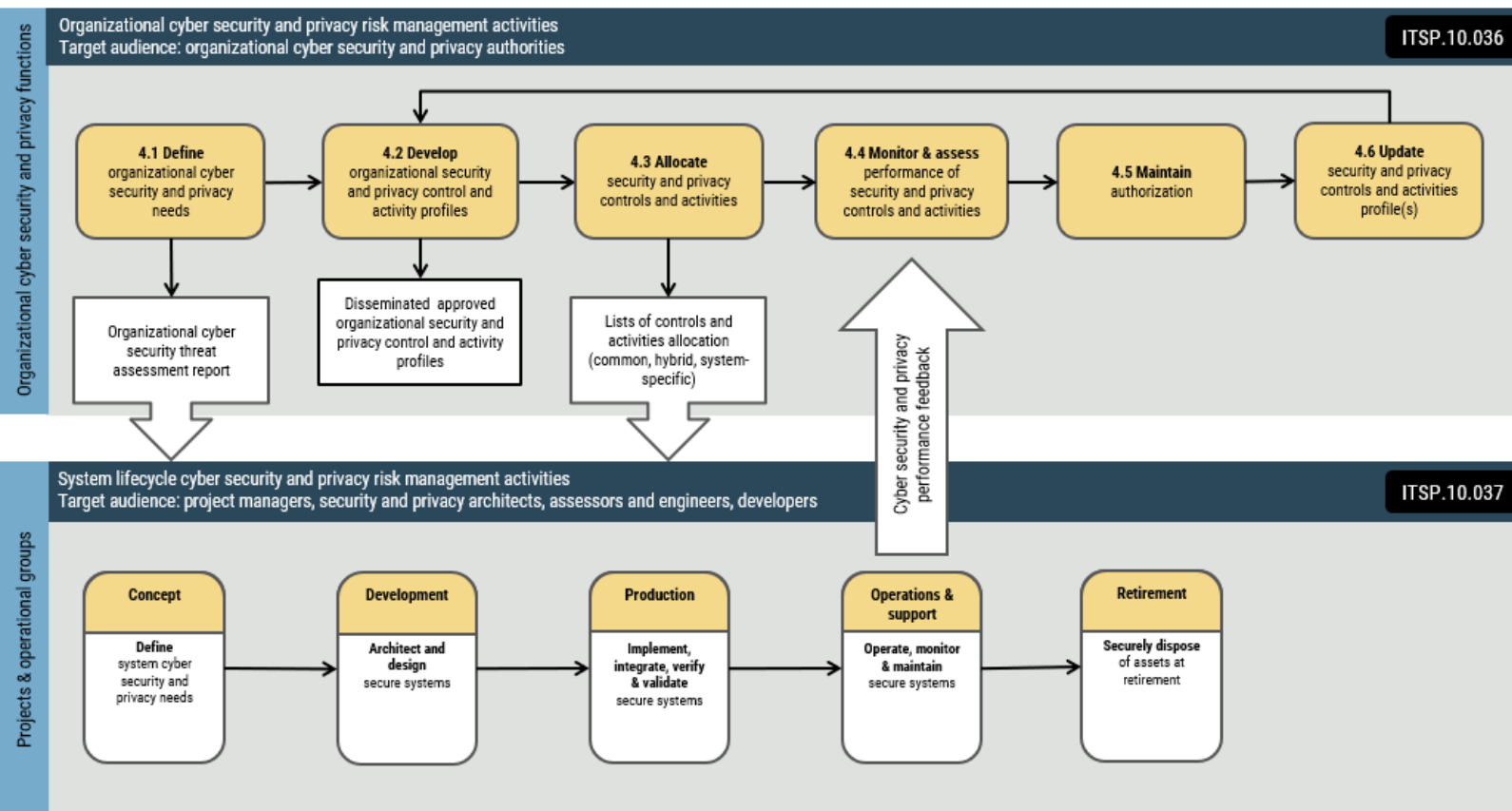
- [Section 2: Cyber security and privacy risk management process](#) introduces the cyber security and privacy risk management process at a high level and explains how it influences the system-level process presented in ITSP.10.037
- [Section 3: Relationships with external processes](#) outlines how the cyber security and privacy risk management process interfaces with external processes
- [Section 4: Organizational cyber security and privacy risk management activities](#) describes the detailed process of managing cyber security and privacy risks in an organization
- [Section 5: Injury assessment and categorization process](#) presents the injury assessment and categorization process, including definitions of key concepts and illustrative examples

2 Cyber security and privacy risk management process

To manage cyber security and privacy risks efficiently and cost effectively, ITSP.10.036 and ITSP.10.037 describe an approach that organizations can adapt to fit their culture, mission and business objectives, business needs for security and privacy, and threats relevant to their activities.

[Figure 1](#) depicts the cyber security and privacy risk management process that is suggested in ITSP.10.036 and ITSP.10.037. The figure shows that cyber security and privacy risk management activities are occurring at 2 distinct levels in an organization: the organizational level and the system level.

Figure 1: Cyber security and privacy risk management process



Long description – Figure 1: Cyber security and privacy risk management process

This figure describes the high-level organizational cyber security and privacy risk management activities. The figure also describes the system lifecycle cyber security and privacy risk management activities within projects and operational groups. It highlights how the cyber security and privacy risk management activities at both levels act together in a continuous cycle to efficiently maintain and improve the security posture of organizational systems.

The Organizational cyber security and privacy risk management activities are intended for organizational cyber security and privacy authorities and encompass the following steps:

4.1 Define the organizational cyber security and privacy needs

- Submits organizational cyber security threat assessment report to Projects and operational groups in charge of system lifecycle cyber security and privacy risk management activities

4.2 Develop organizational security and privacy control and activity profiles

- Disseminated approved organizational security and privacy control and activity profiles

4.3 Allocate security and privacy controls and activities

- Lists of controls and activities allocations (common, hybrid, system-specific) are submitted to Projects and operational groups in charge of system lifecycle cyber security and privacy risk management activities

4.4 Monitor and assess performance of security and privacy controls and activities

4.5 Maintain authorization

4.6 Update security and privacy control and activity profile(s)

- Then return to step 2, Develop organizational security and privacy control and activity profiles

The System lifecycle cyber security and privacy risk management activities enacted by projects and operational groups are aimed at project managers, security and privacy architects, assessors and engineers, and developers, among others. They encompass the following steps:

1. Concept: Define system cyber security and privacy needs
2. Development: Architect and design secure systems
3. Production: Implement, integrate, verify and validate secure systems
4. Operations and support: Operate, monitor and maintain secure systems
 - Submit Cyber security and privacy performance feedback to Organizational cyber security and privacy authorities to inform step 4, Monitor and assess performance of security and privacy controls and activities
5. Retirement: Securely dispose of assets at retirement

At the organizational level, which is the focus of this publication, cyber security and privacy risk management activities are conducted by the organization's cyber security and privacy functions (refer to [section 4](#)). To successfully carry out this process, organizational cyber security and privacy programs need to collaborate closely as their objectives can coincide and be complementary. The objectives of these activities are to:

- define organizational cyber security and privacy needs and associated controls and activities
- allocate responsibility for security and privacy controls and activities
- continuously monitor and assess the performance of allocated controls and activities
- identify required updates to controls and activities (changes to existing controls/activities or addition of controls/activities) based on the results of the continuous monitoring, assessment, and authorization maintenance activities, and oversee the implementation of these updates

At the system level, cyber security and privacy risk management activities are conducted by information technology and operational technology (IT/OT) projects and IT/OT operations groups. They follow the implementation, operation and disposal phases of systems, as outlined in System lifecycle cyber security and privacy risk management activities (ITSP.10.037). The objectives of the system-level activities are to:

- define cyber security and privacy needs as well as associated controls and activities for systems based on the activities of the cyber security and privacy functions
- design, develop, or acquire systems that satisfy defined controls and activities
- integrate, test, and install systems with security and privacy
- operate, monitor, and maintain the security and privacy of systems during the operations and maintenance phase
- securely dispose of assets when systems are retired
- securely dispose of personal information assets when they no longer are required by the organization

3 Relationships with external processes

To fully benefit from this publication, organizations need to be aware of the following important relationships between the organizational cyber security and privacy risk management activities and other processes:

- **Integrated risk management**
 - Organizational cyber security and privacy risk management activities can support organizational integrated risk management, as defined by the [TBS Framework for the Management of Risk](#)
 - These activities form a continuous, proactive, and systematic process to understand, manage, and communicate cyber security and privacy risks from an organization-wide perspective
- **Business impact analysis**
 - Business impact analyses provide valuable insights for identifying an organization's security and privacy requirements and for assessing the sensitivity and criticality of its business activities
 - Together, these factors determine the appropriate security category for those activities
- **Enterprise architecture** – An enterprise architecture function provides key inputs to help ensure that organization-wide cyber security and privacy requirements are taken into consideration when defining, allocating and updating controls and activities.

GC-specific note

In the GC, another process needs to be considered: the **algorithmic impact assessment (AIA)**. This is a mandatory risk assessment tool intended to support the [TBS Directive on Automated Decision-Making](#). It produces a risk value that reflects the potential risks of the automated decision system, and departments and agencies should consider this score as part of their risk management activities.

4 Organizational cyber security and privacy risk management activities

This section describes organizational cyber security and privacy risk management activities that the Cyber Centre recommends be incorporated into an organizational security and privacy program. It also provides guidelines on how to effectively complete them.

GC-specific note

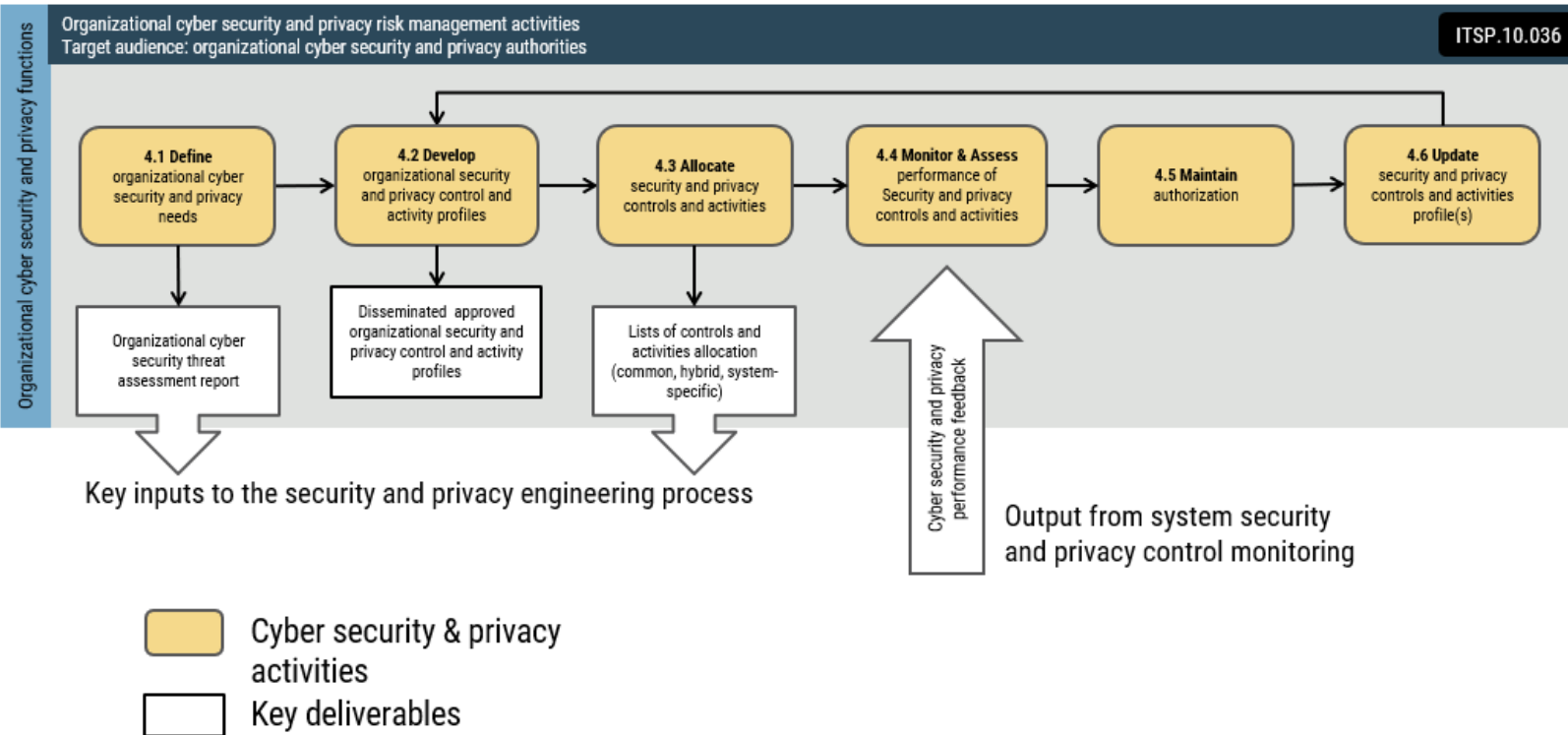
Before incorporating ITSP.10.036 activities in their departmental security and privacy program, departments should ensure that their governance structure (roles, responsibilities, and decision-making authorities) aligns with the governance structure found in the latest TBS policy instruments.

[Figure 2](#) **Organizational cyber security and privacy risk management activities** depicts the activities of the cyber security and privacy risk management process that are conducted at the organizational level. The main goal of these activities is to allocate and maintain a set of security and privacy controls and activities that are tailored to the specific security and privacy needs and objectives of an organization.

The protection of personal information² is a shared and multifaceted responsibility requiring concerted and coordinated efforts between the security and privacy functions throughout the risk management process.

Key outputs of organizational cyber security and privacy risk management activities are control and activities profiles, and organizational threat repositories both of which serve as key inputs to the information system level of the risk management process for the deployment of controls and activities in information systems.

² Personal information is defined in Section 3 of the *Privacy Act* as information about an identifiable individual, recorded in any manner.

Figure 2: Organizational cyber security and privacy risk management activities

Long description – Figure 2: Organizational cyber security and privacy risk management activities

The figure presents a horizontal process flow diagram titled “Organizational cyber security and privacy risk management activities.” There is a dark header that spans the top and states the target audience as organizational cyber security and privacy authorities. Along the left edge of the figure, a vertical side-bar says “Organizational cyber security and privacy functions.”

Across the center, there are six yellow rectangles representing the main organizational activities, arranged left to right and connected by right-pointing arrows. The activities are:

- 4.1 Define organizational cyber security and privacy needs
- 4.2 Develop organizational security and privacy control and activity profiles
- 4.3 Allocate security and privacy controls and activities
- 4.4 Monitor & Assess performance of security and privacy controls and activities
- 4.5 Maintain authorization
- 4.6 Update security and privacy controls and activities profile(s)

Each of the first 3 activities has a downward arrow to a white “key deliverable” box beneath it:

- Under 4.1: Organizational cyber security threat assessment report
- Under 4.2: Disseminated approved organizational security and privacy control and activity profiles
- Under 4.3: Lists of controls and activities allocation (common, hybrid, system-specific)

Under both 4.1 and 4.3, there is a downward pointing arrow with a caption line that reads “Key inputs to the security and privacy engineering process.”

A large white upward-pointing arrow is positioned beneath the 4.4 section. The arrow is labeled “Cyber security and privacy performance feedback” and signifies that monitoring results feed back into the organizational process. To the right of the upward arrow, a note says “Output from system security and privacy control monitoring,” to indicate that system-level monitoring produces feedback used by the organization to reassess and update, when necessary, its profiles and control allocations.

The final activity, 4.6 Update, is connected back toward the earlier step 4.2 “Develop organizational security and privacy control and activity profiles” via a looping arrow along the top of the flow.

The organizational cyber security and privacy risk management activities seek to achieve the following objectives:

- Identify and document the business needs for security and privacy of organizational business activities
- Conduct and maintain organizational threat assessments that security and privacy authorities and practitioners can leverage to identify relevant threat actors, inform risk and robustness determinations throughout the development lifecycle, and produce more consistent outcomes
- Develop organizational controls and activities profiles tailored to business needs for security and privacy
 - Leverage profile(s) in projects that implement or update organizational information systems
- Allocate the security and privacy controls and activities within the enterprise security architecture
- Define which controls and activities are common, hybrid or system-specific to support the assignment of responsibilities across the enterprise
- Coordinate between organizational security and privacy functions (for example, physical security and personnel security) to ensure a consistent approach to building and operating dependable information systems
- Monitor and assess the performance of implemented controls and activities in protecting organizational business activities Devise and implement corrective measures to improve performance and the organization’s overall security and privacy posture

4.1 Define organizational cyber security and privacy needs

This section outlines the process for defining organizational cyber security and privacy needs. It includes the following sub-activities:

- Define the scope of the organization’s cyber security and privacy risk assessment activities ([section 4.1.1](#))
- Identify the business needs for security and privacy of organizational business activities ([section 4.1.2](#))
- Perform injury assessment and categorization of organizational business activities ([section 4.1.3](#))
- Select the organizational cyber security threat and risk assessment (TRA) methodology ([section 4.1.4](#))
- Select the organizational privacy assessment methodology ([section 4.1.5](#))
- Conduct an organizational cyber security threat assessment ([section 4.1.6](#))

Each of these activities aiming to define organizational cyber security and privacy needs is described in the sections that follow. These activities are performed when first implementing the guidelines presented in this publication, and then as required based on the assessment of the security and privacy posture of an organization's information systems (refer to [section 4.6](#)).

4.1.1 Define the scope of the cyber security and privacy risk assessment activities

Objective: Define the scope of the organization's cyber security and privacy risk assessment activities.

Suggested related roles: Senior security officials (for example, CSO, chief information security officer (CISO)), senior privacy officials, cyber security advisors, enterprise security architects, privacy advisors, privacy architects, project directors

The scope can be characterized by the:

- organization's programs, services, information, and business activities requiring protection
- organization's programs, services, and activities involving the creation, collection, and handling of personal information that are under its control
- major organizational assets (for example, business applications, information systems, data centres, local areas networks, data processed and stored, information) and their geographical locations
- core technologies that are used in organizational information systems
- procurement strategies (for example, internal, outsourced)

The scope should clearly delineate the organizational business activities and assets that are within its boundaries, and those that are excluded and why. The scope should also identify external dependencies like external service providers.

Output: Definition of the scope of the organization's cyber security and privacy risk assessment activities and personal information inventory.

4.1.2 Identify business needs for security and privacy

Objective: Identify the business needs for security and privacy of organizational business activities.

Suggested related roles: Senior security officials, such as CSOs and CISOs, senior privacy officials, cyber security advisors, privacy advisors, project directors

Within the context of cyber security and privacy risk management, business needs for security and privacy refer to the need to protect organizational business activities and information against adverse events that could affect the ability of organizations to meet their mission, objectives, and obligations. Legislation or regulations that impose protection requirements for information systems and personal information, create business needs for security and privacy to ensure compliance. Business needs for security and privacy, in turn, shape formal security and privacy objectives. They may originate from:

- requirements found in legislation, regulations, policies, directives, standards, jurisprudence and objectives governing organizational business activities and information management (for example, in the GC, a departmental results framework)

- generally or organizationally recognized information system threat exposures and compliance obligations
- contractual or negotiated obligations (for example, contracts, memoranda of understanding (MOUs), service level agreements (SLAs) and information sharing agreements (ISAs))

Business needs for security include privacy-related requirements needing the support of cyber security for privacy risk management purposes.

Examples of business needs for security and privacy include the need to:

- limit access to sensitive program information or personal information to authorized individuals for authorized actions
- limit secondary uses or disclosures of personal information
- verify the identity of citizens before disclosing personal information that relates to them
- ensure that only authorized individuals can approve financial payment to a recipient

Organizations should identify business needs for security and privacy with the help of business analysts, system owners, system architects and security/privacy architects. Useful inputs to this activity include business process documentation (for example, business process descriptions, use cases, concepts of operations (CONOPS)) and impact assessments (for example, business impact analysis, PIA, algorithmic impact assessment).

Output: Document stating the business needs for security and privacy for the organization's business activities.

4.1.3 Perform injury assessment and categorization of organizational business activities

Objective: Perform the assessment and categorization of injuries to organizational business activities.

Suggested related roles: Security advisors, privacy advisors, project director

An injury category expresses the highest levels of expected injuries from threat compromise with respect to privacy and to the security objectives of confidentiality, integrity, and availability. Safety requirements may elevate the categorization for integrity and availability.

Business activities are categorized by first determining the expected injuries from a cyber-related threat compromise to the national and non-national interests that the business activities serve and then determining the level of these expected injuries. While the breach of personal information may result in varying levels of injury, the compliance obligations do not change based on the type of the personal information. The comprehensive security categorization of the information should include consideration of the presence of personal information.

Organizations can categorize their business activities following the process specified in [section 5](#).

Output: Injury categorization report for organizational business activities.

4.1.4 Select organizational cyber security threat and risk assessment methodology

Objective: Select the methodology by which security and privacy threats and risks will be assessed across the organization.

Suggested related roles: Senior security officials (CSO, CISO), security advisors

A cyber security TRA methodology must be selected at this stage, as an organization will use the threat assessment portion when assessing threats to organizational business activities. In addition, projects will use this methodology when performing TRA activities.

An example of a commonly used TRA methodology in the GC is the [CSE-RCMP Harmonized Threat and Risk Assessment \(HTRA\) Methodology](#).

Output: Selection of organizational cyber security TRA methodology.

4.1.5 Select the organizational privacy assessment methodology

Objective: Select the methodology by which privacy risks and compliance gaps will be assessed across the organization.

Suggested related roles: Senior privacy officials, privacy advisors

At this stage, a privacy assessment methodology needs to be selected to identify, assess, and mitigate potential privacy risks associated with new or modified programs, projects, or technologies.

In the GC, privacy assessments follow TBS policy, beginning with the completion of a privacy checklist template. This checklist helps determine whether an initiative requires a privacy protocol, a PIA, or no further privacy assessment. Each assessment methodology is built into its corresponding template, so selecting the appropriate template also determines the assessment approach.

Output: Selection of organizational privacy assessment methodology. In the GC, an additional output will be the completion of a privacy checklist that determines what template any additional privacy analysis should use.

4.1.6 Conduct an organizational cyber security threat assessment

Objective: Conduct an initial organization-wide cyber security threat assessment that will guide the selection of security and privacy controls and activities, and that projects will leverage when implementing systems.³

Suggested related roles: Intelligence analysts, cyber security threat analysts

This activity will identify and qualify threats of relevance to the in-scope organizational business activities.

The cyber security threat assessment serves 2 purposes:

- informing the TRA
- supporting threat context decisions

Organizations may specify a subset of all potential threats from which they want to protect their business activities. This implies that some threats may be identified and considered but be deemed out of scope for various reasons. For example, an organization may find that protecting against a threat would be too costly or complex, or that the protection would

³ An organizational threat assessment is an ongoing process that also supports the system cyber security and privacy risk management activities. For more details, read System lifecycle cyber security and privacy risk management activities (ITSP.10.037).

excessively limit a business activity's supporting functionality. Threat information, including decisions and justification for excluding specific threats, is documented in an organizational threat context.

An organization-wide threat assessment is a valuable tool that can be used to select, tailor, allocate, update, and improve the implemented security and privacy controls and activities. Its results, along with organizational business needs for security and privacy, form a strong foundation for developing organizational control and activity profiles.

When developing organizational control and activity profiles, more focused, domain-specific threat repositories may be created to document detailed information on threats relevant to specific business domains.

An effective organizational threat assessment should evaluate and consider:

- key organizational business activities
- the injury assessment associated with these activities
- relevant threats to the business
- general exposures that could impact business activities (for example, physical locations vulnerable to earthquakes)

In the GC, departmental threat assessments are best conducted by multidisciplinary teams with the assistance of the CSO's office, lead GC security agencies, and privacy practitioners.

Output: Organizational threat assessment repository documenting the threats and exposures of relevance to the business.

4.2 Develop organizational security and privacy control and activity profiles

Objective: Create organizational security and privacy control and activity profiles that are tailored to security and privacy needs.

Suggested related roles: Senior security officials, such as CSOs and CISOs, senior privacy officials, enterprise security architects, privacy architects, security advisors, privacy advisors

Depending on their business scope (for example, managing a single initiative, overseeing multiple projects, or operating in multiple security domains) and the complexity of their business activities, organizations may maintain a single enterprise-wide profile or several domain-specific profiles tailored to different areas of their business.

The cyber security and privacy functions of an organization are expected to collaborate on developing profiles since privacy risks may arise from unauthorized system activities. However, not all privacy risks associated with the handling of personal information in an information system falls within the scope of information security. Privacy risks can result from activities related to the creation, collection, retention, accuracy, use, disclosure, or disposition of personal information under the control of an organization. Hence, the privacy function of an organization will likewise select, allocate, monitor, and assess privacy controls in order to comply with legislative requirements.

Organizational profiles are best developed with the support of several key organization-wide information management processes. These enterprise processes complement the cyber security and privacy risk management process and can assist organizations in appropriately select and tailor security and privacy controls and activities. The supporting processes are:

- the review of the organizational business activities and their security and privacy needs

- the prioritization of organizational business activities according to strategic goals related to availability and business continuity (in general terms, this means ensuring that the most critical activities will continue or remain available)
- the definition of the types of information assets needed to successfully execute the departmental business activities, their criticality and sensitivity, and their internal and external flows
- the creation of data dictionaries that document the collections of personal information within the organization
- the definition of a conceptual enterprise architecture that includes cyber security and privacy requirements

There are 4 steps to developing organizational security and privacy control and activity profiles:

1. Define business domains
2. Define security architecture approaches
3. Select security and privacy controls and activities
4. Approve the organizational security and privacy control and activity profiles

These 4 steps are described in detail in the subsections that follow.

4.2.1 Define business domains

Objective: Define the business domains of an organization in support of developing the required organizational security and privacy control and activity profiles.

Suggested related roles: Enterprise security architects, privacy architects

A business domain is characterized by the security categories of its business activities and their relevant cyber security threats. Therefore, business domains may have differing protection needs, leading to different profiles.

For example, consider a set of business activities involving the distribution of non-sensitive publications and a second set of business activities involving high-value, critical financial transactions. In the latter scenario, the financial activities would likely have a higher injury category and face more significant threats. This analysis would lead to the definition of 2 domains requiring 2 different domain profiles.

Organizations have some flexibility in how they define their business domains. They should document in detail how these domains are defined, the injury categories of the business activities, and the significance of the threat environment. Note that the organizational business activities should have been defined earlier (in whole or in part) during the injury assessment and categorization activity (see [section 4.1.3](#)).

This activity produces business domain definitions. Each defined business domain should include

- a description of the business domain's business objectives, processes and information assets
- the injury category of the business domain
- a characterization of the threat environment of relevance to the business domain (that is, the highest deliberate threat (Td) level to be mitigated)
- a statement of the highest level of risk that the business owner deems acceptable

Output: Business domain definitions, including the objectives, processes and information assets, the injury category, the threat environment, and a statement of the level of risk deemed acceptable.

4.2.2 Define security architecture approaches

Objective: Define a set of security architecture approaches that align with the organizational cyber security and privacy philosophy, culture, objectives, and priorities.

Suggested related roles: Enterprise security architects, privacy architects

At the organizational level, security architecture approaches influence the selection of certain technical security controls and activities related to the security engineering principles applied in the approach. At the information system level, security architecture approaches play an equally important role as a guide for tailoring security controls in profiles to the specific security needs of information systems and for specifying appropriate security designs.

Enterprise security architects and privacy architects will likely seek approval from senior officials for their chosen security architecture approaches, as these decisions often have budget and capability implications.

When defining security architecture approaches, organizations should take into consideration the following inputs:

- business needs for security and privacy ([section 4.1.2](#))
- injury assessment and categorization of organizational business activities ([section 4.1.3](#))
- threats documented in the organizational threat assessment ([section 4.1.6](#))
- generally accepted cyber security principles and best practices such as
 - Sherwood Applied Business Security Architecture's (SABSA) [Enterprise Security Architecture – A Business-Driven Approach](#)
 - Cyber Centre's [Baseline security requirements for network security zones \(ITSP.80.022 v2.0\)](#)
 - National Institute of Standards and Technology's (NIST) [Special Publication \(SP\) 800-160 Vol.1 Rev.1 Engineering Trustworthy Secure Systems](#)
 - NIST's [SP 800-160 Vol. 2 Rev. 1 Developing Cyber-Resilient Systems: A Systems Security Engineering Approach](#)
- generally accepted privacy principles and best practices such as
 - Fair Information Principles
 - Generally Accepted Privacy Principles (GAPPs)

The following are examples of security architecture approaches that influence the selection of security and privacy controls and activities and the specification of security designs that organizations can use:

- Holistic versus piecemeal approach to design, where a holistic approach considers security and privacy at the various layers of an information system (for example, application, data management, middleware, platform, and communication layers) and includes an understanding of information flows between the various layers
- Defence-in-depth/layered defence versus focus on 1-layer protection
- Eggshell (hard perimeter/soft centre) versus honeycomb versus end-point protection approaches to design
- Appropriate security modes of operation (dedicated, system-high, compartmented, multilevel, multiple independent levels of security (MILS))

- Tiered application architecture (presentation, business logic, data repositories) applying security zoning versus monolithic system architecture
- Use of common security services with standardized application programming interface (for example, organizational authentication system) versus implementing custom security services
- Infrastructure security versus data asset security (for example, digital rights management)
- Societal considerations (for example, employees' privacy versus monitoring) versus enforcement of hard-to-use but more secure controls

Output: List of selected security architecture approaches and justifications.

4.2.3 Select organizational security and privacy controls and activities

Objective: Select organizational security and privacy controls and activities.

Suggested related roles: Enterprise security architects, privacy architects, security advisors, privacy advisors

Organizations develop a control and activity profile for each of their defined business domains. If an organization defines several business domains, then it can develop the profiles gradually, starting with one that is urgently needed, and then developing the others over time.

There are 3 approaches to implementing controls and activities:

- a common (inheritable) implementation approach
- a system-specific implementation approach
- a hybrid implementation approach

The implementation approaches define the scope of applicability for the control or activity, its shared nature or inheritability, and the responsibility for control or activity development, implementation, assessment, and authorization. Each implementation approach has a specific objective and focus that helps organizations select the appropriate controls and activities, effectively implement them, and satisfy security and privacy requirements. A specific implementation approach may save money by leveraging security and privacy capabilities across multiple systems and operational environments.

A common control or activity is deployed as a shared service to the organization. Implementing common controls or activities results in a capability that is inheritable by multiple systems or programs. System-specific controls and activities are the primary responsibility of the system owner. Organizations can implement a hybrid control or activity if one part of the control or activity is common (inheritable) and the other part is system-specific. For example, an organization may implement contingency planning control CP-02 using a predefined template for all organizational information systems, with individual system owners tailoring the plan for system-specific uses where appropriate. For privacy, an organization-wide policy or procedure would be an example of a common privacy control or activity. For more information, refer to [Security and privacy controls and assurance activities catalogue \(ITSP.10.033\) section 2 Implementation approaches](#).

Organizational control and activity profiles are used by the cyber security and privacy functions to coordinate the allocation of common controls and activities to the enterprise architecture. They also inform projects about the controls and activities their system inherits, as well as those they must implement to secure the system they are developing or updating.

When developing organizational control and activity profiles, organizations select controls and activities from the ITSP.10.033 catalogue, and tailor them to satisfy organizational security and privacy needs ([section 4.1.2](#)). The selection and tailoring of controls and activities is guided by the results of their organizational privacy assessment ([section 4.1.5](#)), organizational cyber security threat assessment ([section 4.1.6](#)) and the defined security architecture approaches ([section 4.2.2](#)). For organizations that have an enterprise architecture function, security and privacy practitioners should also consider cyber security-related artefacts when selecting and tailoring system-specific controls and activities.

Organizational profiles should also document the business context and assumptions under which they were developed by describing:

- in-scope business activities and related business needs for security and privacy
- injury assessment and categorization of in-scope business activities
- the threat context
- legislative and policy compliance artefacts
- defined security architecture approaches
- any other technical constraints or assumptions that might influence the selection of controls and activities

A key input to the control and activity profile development process is the organizational threat repository (see [section 4.1.6](#)). When developing domain profiles, organizations may refine organizational threat definitions based on additional threat information that is specific to each domain's business activities. When this occurs, organizations can document these refined threat definitions in domain-specific threat repositories.

Several of the controls and activities in the ITSP.10.033 catalogue should be considered for allocation as common controls and activities.

Examples of common security and privacy controls and activities are:

- an organizational personnel security screening program supporting the screening of cyber security personnel
- a physical security program supporting the protection of technological facilities
- security incident and privacy breach management performed as part of cyber security and privacy functions to provide a comprehensive situational awareness
- a system operated by an IT/OT operations group that provides a common end-user authentication solution
- an organization-wide electronic log monitoring system, operated by a team from the cyber security function, which provides separation of duties between the IT/OT operations and the cyber security function
- a cyber security awareness and training program administered by the organizational learning centre

To develop their organizational profile, organizations may leverage the medium impact profile in ITSP.10.033-01, which is based on the ITSP.10.033 catalogue.

Output: An organization-wide security and privacy control and activity profile or a set of domain security and privacy control and activity profiles.

4.2.4 Approve the organizational profile(s)

Objective: Approve the organizational security and privacy control and activity profile(s).

Suggested related roles: Senior security officials, senior privacy officials

Once the security and privacy control and activity profile(s) have been completed, senior officials in the organization's security and privacy governance should review them and seek approval from organizational authorities (for example, CEO, CIO, CSO, CISO, CPO, deputy head) as required. As part of this process, these senior officials should also ensure that the organizational controls and activities specified in the profiles satisfy organizational security and privacy needs, and that they adequately address threats and privacy compliance obligations. They should ensure that there will be a good balance between the implementation of controls and activities and the levels of residual risk that the organization is ready to assume.

Output: Approved organizational security and privacy control and activity profile(s).

4.3 Allocate security and privacy controls and activities

Objective: Coordinate the allocation of security and privacy controls and activities.

Suggested related roles: Enterprise security architects, privacy architects

Following the approval of organizational security and privacy control and activity profiles, senior officials in the organization's security and privacy governance and their staff can proceed with coordinating the allocation of controls and activities.

Developing a strategy for allocating security and privacy controls and activities starts with determining which ones are common, hybrid, or system-specific. It is also important to identify the responsible parties for delivering and operating common and hybrid controls and activities within the organization. Engaging an enterprise architecture board can help facilitate this process.

4.3.1 Allocate common controls and activities

Objective: Coordinate and document the allocation of common controls and activities.

Suggested related roles: Enterprise security architects, privacy architects

In an established organization, certain controls and activities may already be delivered through shared or common services. These should be identified and documented within the enterprise security architecture. For controls and activities that are not yet in place, responsibilities should be clearly defined and allocated as part of the enterprise security architecture function.

Organizations have several options to allocate common security and privacy controls and activities. They can be allocated:

- as part of the cyber security and privacy functions
- to an organizational IT/OT operations group
- to other groups within the organization, or outsourced to another organization or service provider
- to a new shared or common service

[Table 1](#) provides examples of how common security and privacy controls and activities can be allocated.

Table 1: Examples of common controls and activities allocation

Common controls and activities	Allocation by the enterprise security architecture function	Operational authority
CA-07 Continuous monitoring	Implement an automated monitoring infrastructure	Cyber security authorities (as a component of the cyber security function)
SC-07 Boundary protection	Implement a boundary protection infrastructure	IT/OT operations group – Network operations
CP-07 Alternate processing site	Service contract	Service provider
IA-02 End user identification and authentication	Subscribe to an existing GC shared identification and authentication service	Shared Services Canada (SSC) ⁴
PT-01 Personal information handling and transparency policy and procedures	The enterprise policy authority publishes policies and procedures for handling personal information	Privacy authorities (as a component of the privacy function)

When the allocation of a common security or privacy control or activity requires the implementation of supporting systems, organizations should implement them through projects following the process described in System lifecycle cyber security and privacy risk management activities (ITSP.10.037).

Output: Document listing the allocated common security and privacy controls and activities.

4.3.2 Allocate system-specific controls and activities

Objective: Coordinate and document the allocation of system-specific controls and activities.

Suggested related roles: Enterprise security architects, privacy architects

To implement the selected security and privacy controls and activities, the enterprise security architecture function will allocate a set of appropriate controls and activities to that system. System-specific technical controls must be identified early in the project lifecycle so they can be appropriately scoped, resourced and funded within the project budget. This proactive approach ensures that controls and activities are integrated seamlessly into system development and operations, rather than being retrofitted later at greater cost or complexity.

The allocation process includes mapping applicable controls, including hybrid ones, to system contexts and coordinating implementation responsibilities across cyber security, privacy and business stakeholders.

Projects and IT/OT operations groups implement and operate security and privacy controls and activities in systems following the cyber security and privacy risk management activities described in ITSP.10.037.

⁴ Designated provider of GC shared services.

Clear documentation of control and activity assignments also supports ongoing assurance, audit readiness, and the ability to manage the effectiveness of controls over time.

Output: A list of allocated security and privacy controls and activities in systems.

4.4 Monitor and assess performance of security and privacy controls and activities

Objective: Perform continuous monitoring and assessment of the implemented security and privacy controls and activities.

Suggested related roles: IT/OT operations groups, security assessors, privacy assessors

Organizations monitor and assess the performance of the implemented common, hybrid, and system-specific controls and activities through the collection, consolidation, and continuous analysis of performance metrics. Many of the monitoring and assessment tasks will be performed by the IT/OT operations groups, and summary reports will be provided to the cyber security and privacy functions for organization-wide analysis. Some sensitive monitoring tasks may be performed by the cyber security and privacy functions (if mandated by a security and privacy control and activity profile) when separation of duties is required.

Continuous assessment⁵ tasks consider more than just the performance of security and privacy controls and activities and should include:

- identifying vulnerabilities, weaknesses, and inefficiencies
- reviewing security and privacy-related changes
- reviewing security and privacy incidents and problems reports
- conducting security testing, which could include functional security testing, vulnerability assessments, and penetration testing
- reviewing the security configuration of system components

The monitoring and assessment results will inform organizational authorities of the current state of organizational systems' security and privacy posture. A stable and adequate security and privacy posture will allow a system to maintain its authorization to operate. A deteriorating posture may lead organizational authorities to revoke the authorization to operate until mitigating measures are put in place (see [section 4.5](#) and [section 4.6](#)).

Output: Report on the performance of security and privacy controls and activities and on the security and privacy posture of the systems.

4.5 Maintain authorization

Objective: Maintain the authorization state of the systems.

⁵ Continuous assessment does not necessarily mean real-time assessment. Some assessment activities, such as log event review, can be performed automatically in real time, while other assessment activities, such as the review of system backup procedures, would usually be done manually on a pre-established schedule.

Suggested related roles: Authorizers, business analysts, security advisors, privacy advisors, enterprise security architects, privacy architects

When following the suggested cyber security and privacy risk management process, organizations initially authorize the operation of their systems as part of the process described in ITSP.10.037. Subsequently, organizations maintain the authorization state of their systems by continuously monitoring, assessing, and updating security and privacy controls and activities.

The authorization maintenance process consists of the following activities:

- periodically reviewing the injury assessment and categorization of supported business activities
- reassessing the threat environment and the security performance of technical environments
- reassessing collection and use of personal information to understand any changes to the initial program design
- reviewing the performance assessment result for security and privacy controls and activities
- reviewing the activities of IT/OT operations group to ensure that they have adequately maintained the security and privacy posture of their systems according to the security and privacy provisions of their operations plans

When the results of authorization maintenance activities show that a system is no longer operating within acceptable levels of residual risk, there are several avenues that organizations can pursue to remediate the situation, including:

- implementing temporary security measures to protect supported business activities (for example, disconnecting an information system from the Internet, activating a portion of a contingency plan)
- updating privacy artefacts (for example, privacy notice statements and associated personal information banks, subject to required approvals)
- updating implemented controls and activities to correct security and privacy deficiencies and return the system to its authorized state of operation (see [section 4.6](#))
- accepting the new level of residual risk

If the level of residual risk remains unacceptable after initial remedial action, authorizers may choose to revoke the authority to operate pending further remedial action. The revocation of authorization would lead to additional security and privacy analysis activities to identify specific deficiencies within the operational context, followed by the application of corrective measures or improvements to implemented controls and activities to return the system to its authorized state.

Organizations should establish in their organizational security plan the frequency of periodic security assessment and review activities (for example, review of security incident reports, review of threat environment, review of IT/OT operations group security activities). Alternatively, authorizers could establish the frequency of such activities during a system's initial implementation according to factors such as security injury categorization, threats, residual risk levels, and outstanding security deficiencies.

The outputs of authorization maintenance activities include updated residual risk assessments and updated security provisions in an operations plan. The security provisions of the operations plan should include mitigation plans and schedules for any outstanding security deficiencies discovered because of the security assessment work (see [section 4.6](#)).

In the GC, there is an obligation for programs to annually review any risks identified during the privacy assessment process and update risk mitigation measures.

Outputs: Updated residual risk assessments and updated security provisions of operations plan.

4.6 Update security and privacy controls and activities profile(s)

Objective: Ensure that the security and privacy posture of the program, including the system, remains adequate by keeping all implemented controls and activities up to date. If required, add controls and activities to increase the security and privacy posture.

Suggested related roles: Enterprise security architects, privacy architects

Organizations may need to update their implemented security and privacy controls and activities for various reasons, including when there is a:

- change in organizational missions or objectives
- change in an organizational business activity (for example, collection of new, more sensitive information under an existing organizational program)
- change in business needs for security and privacy (for example, because of legislative or policy changes)
- change in the collection, use or disclosure of personal information
- requirement for change because of an organizational threat assessment update (that is, when a program is targeted by more sophisticated threat actors)
- requirement for change because of performance monitoring (for example, a security or privacy control or activity has proven ineffective in adequately protecting related systems or personal information)

Key inputs to this activity include existing organizational control and activity profiles, threat repositories, performance monitoring results, as well as assessment and authorization maintenance activities (see [section 4.4](#) and [section 4.5](#)). This activity can reveal gaps in existing controls and activities, prompting updates or the addition of new ones. It may also lead to revisiting earlier cyber security and privacy activities to redefine requirements, update control and activity profiles and threat repositories (see, for example, [section 4.1.3](#), [section 4.1.6](#), [section 4.2](#)), allocate new controls or activities (see [section 4.3](#)), or conduct further monitoring and assessment (see [section 4.4](#)).

Output: Report on the need for improved or new security and privacy controls and activities or updated profile(s).

5 Injury assessment and categorization process

This section describes how organizations can perform injury assessments and categorization of their organizational business activities to help define their security and privacy control and activity profiles. Business activities refer to business processes and related information assets, including personal information.

Injury assessment and categorization is an instrument to establish the relative importance of organizational business activities. At the organizational level, injury categories of business activities serve as input for conducting threat assessments and developing control and activity profiles. At the system level, injury categories of business activities serve as input for establishing security assurance requirements, selecting and tailoring security and privacy controls and activities, and conducting TRA activities.

5.1 Concepts

When business activities are compromised by cyber-related threats, there may be injury to the national interests⁶ or the non-national interests⁷ that the business activities serve. Injury can occur because of the unauthorized use, disclosure, modification, or denial of information, or the corruption or interruption of business processes. Injury due to the unauthorized use or disclosure of information relates to the **confidentiality objective** of information security. Injury due to the modification of information or the corruption of business processes relates to the **integrity objective** (that is, accuracy, completeness, authenticity, intended use) of information security. Injury due to the denial of information or the interruption of business processes relates to the **availability objective** of information security.

The injury assessment and categorization process determines an injury level for each security objective associated with a business activity. The designation of an injury level assumes a successful compromise by a threat actor which allows the assessment to focus on the injuries that could reasonably result from this event.

5.1.1 National security systems

A national security system (NSS) is any system whose compromise, whether in terms of confidentiality, integrity or availability, would result in harm to national security. While NSS designation often aligns with classification levels (such as confidential, secret, top secret), classification alone is not determinative. Some systems may be unclassified yet still qualify as NSS if their compromise could reasonably cause injury to national security.

In Canada, TBS defines unclassified as not being sensitive. However, a system's classification status does not negate its potential impact. For example, a military weapon system onboard a naval vessel or armoured vehicle, if compromised, could result in a national security injury. As such, it should be identified as an NSS during the injury categorization process. The key consideration in NSS designation is the potential for national security injury, not classification status. Injury assessments should prioritize the consequences of compromise over whether a system is labelled as classified or unclassified.

⁶ National interests: The security and the social, political, and economic stability of Canada.

⁷ Non-national interests: The safety, health, and well-being of individuals, and the financial position and reputation of individuals and Canadian companies.

5.1.2 Safety

When assessing safety-critical systems, where failure could lead to outcomes such as health impacts, loss of life, property damage or loss, or environmental harm, it is essential to consider both the classification of information and how safety requirements influence the potential for harm in the event of system compromise. In such cases, safety requirements can elevate the potential impact on availability, integrity and, in some contexts, confidentiality, resulting in higher injury levels during the injury categorization process. Safety-critical systems usually have stringent expectations for availability and integrity, and confidentiality may also be important depending on the operational context. Ultimately, the severity of injury assigned should be commensurate with the level of harm that could realistically result from a compromise of the system.

5.1.3 Privacy

Injury assessments must account for the potential impact on individual privacy when business activities involve personal information. Compromised personal information can cause injury to individuals and organizations and can result in:

- identity theft or fraud
- reputational or emotional harm
- loss of public trust
- legal and regulatory consequences

The level of injury depends on the sensitivity, volume, and context of the personal information. In addition to breaches of personal information, privacy injuries may also arise from corrupted personal data leading to incorrect decisions or disruption of services affecting access to benefits or critical support. This is especially significant in safety-critical or service-critical systems (for example, health or emergency services). Privacy risks should be considered alongside confidentiality, integrity, and availability objectives during the injury categorization process. Where personal information is used to make administrative decisions, a PIA should be conducted in parallel with threat and risk assessments to ensure appropriate privacy and security controls and activities are selected.

5.1.4 Adversarial perspective

Injury assessment and categorization require framing the compromise from an adversarial perspective. Security and privacy practitioners should evaluate injuries under the assumption that a threat actor has successfully compromised the system, including scenarios where they obtained significant control. Most organizations tend to underestimate potential injuries because they approach risk with good faith and reasonable assumptions. However, some threat actors are willing to engage in extraordinary and unconscionable actions to achieve their objectives.

For example, a business process such as operating life support systems in a hospital should be assumed to potentially negatively impact patient health, including causing bodily harm and loss of life. Another example would be a department with a security mandate which, if compromised, could be leveraged as a criminal or hostile tool controlled by a threat actor, in complete opposition to their mandate.

The question here is: What is the worst case-scenario?

5.1.5 Post-compromise injury

The injury assessment must be based on the assumption that an attack has occurred and has been successful. At this stage, the likelihood of the threat and the presence of mitigating controls should not be considered. When evaluating potential injury, even scenarios deemed exceedingly unlikely must be treated as if they have already occurred.

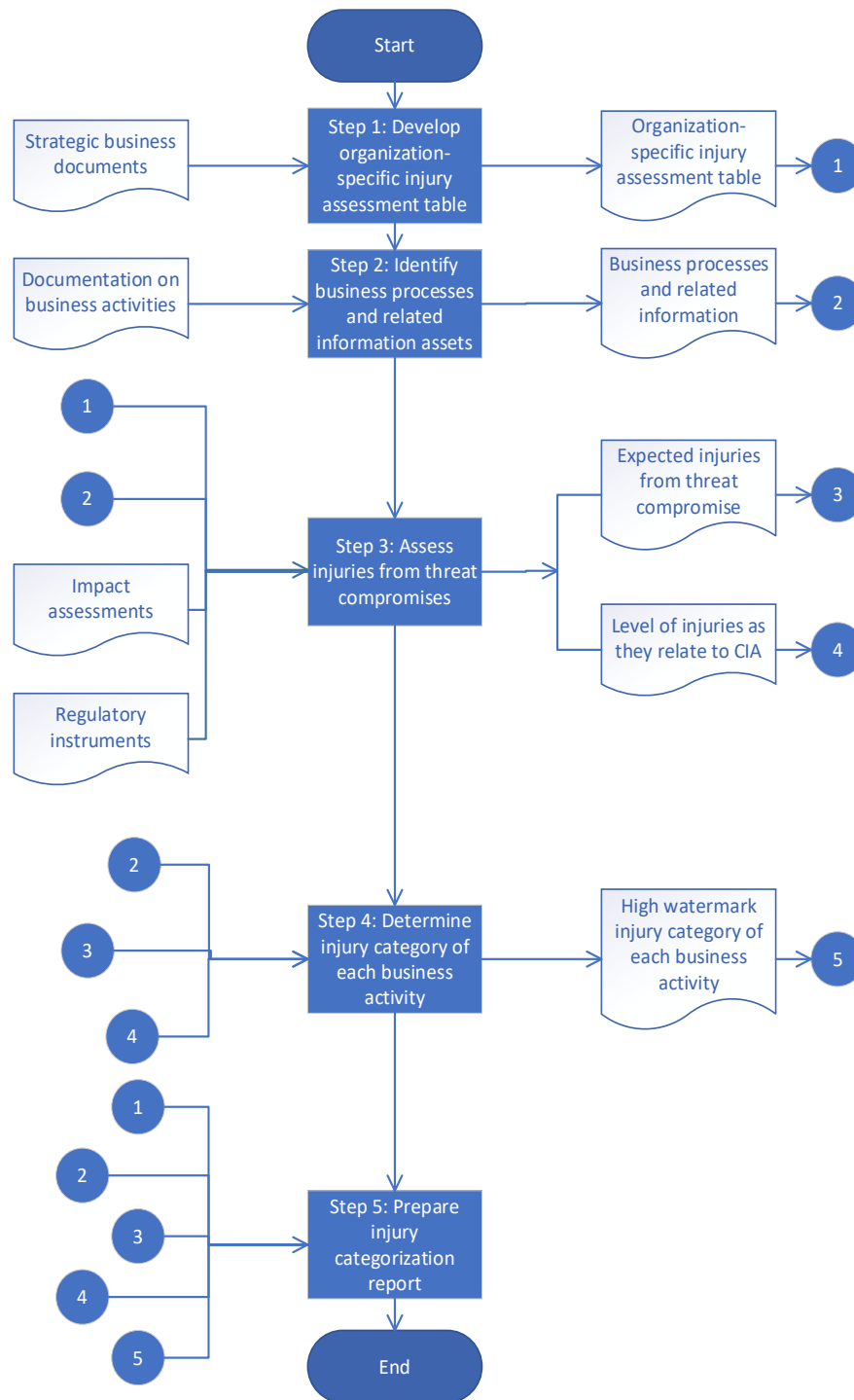
For example, while the bombing of a data centre may be considered highly unlikely, the resulting injury – complete loss of all onsite functionality – remains a valid consideration in the assessment. Similarly, the existence of redundant data centres does not reduce the severity of the injury at this stage of the process.

The question here is: What happens if that worst-case scenario occurred?

5.2 Injury assessment and categorization process

As illustrated in [figure 3](#), the injury assessment and categorization process for a business activity can be summarized in 5 steps:

1. Develop a custom injury assessment table
2. Identify the business processes and information assets, including personal information, that relate to the business activity
3. Assess expected injuries from assumed threat compromise of the business activity, and determine their severity in terms of confidentiality, integrity, and availability
4. Determine the injury category of the business activity by identifying the highest expected level injury across confidentiality, integrity, and availability
5. Prepare an injury assessment and categorization report

Figure 3: Injury assessment and categorization process**Long description – Figure 3: Injury assessment and categorization process**

This figure represents a vertical flow chart explaining the injury assessment and categorization process. A single central column shows the five numbered steps of the process from top to bottom, each in a blue rectangle, connected by downward-pointing arrows. The process begins at a blue oval labeled “Start” and ends at a blue oval labeled “End.” At

several steps, inputs appear on the left side of the flow with arrows feeding into the step, and outputs appear on the right side as white document-shaped callouts. Each output callout has a small, numbered circle that serves as a persistent reference label used later in the diagram to show where that output is consumed as an input.

The central sequence from top to bottom is:

- Start: An oval labeled “Start,” with a downward arrow to Step 1.
- Step 1: “Develop organization-specific injury assessment table”
 - Left input: A rectangular label “Strategic business documents” points to Step 1.
 - Right output: A white document-shaped callout labeled “Organization-specific injury assessment table,” marked with a small circle labeled “1.” This creates Output 1.
 - Note on reuse: Output 1 is later reused as an input to Step 3, indicated by a small circle “1” shown on the left side feeding into Step 3.
- Step 2: “Identify business processes and related information assets”
 - Left input: A rectangular label “Documentation on business activities” points to Step 2.
 - Right output: A white document-shaped callout labeled “Business processes and related information,” marked with a small circle “2.” This creates Output 2.
 - Note on reuse: Output 2 is later reused as an input to Step 3 and Step 4, indicated by the small circle “2” on the left side of those steps.
- Step 3: “Assess injuries from threat compromises”
 - Left inputs:
 - Two rectangular sources feed into Step 3: “Impact assessments” and “Regulatory instruments.”
 - In addition, two small numbered circles also feed into Step 3 from the left margin: circle “1” (Output 1 from Step 1) and circle “2” (Output 2 from Step 2). These icons visually indicate that the organization-specific assessment table and the identified business processes/information assets are used within the injury assessment.
 - Right outputs:
 - A white callout labeled “Expected injuries from threat compromise,” marked with circle “3.” This creates Output 3.
 - A second white callout labeled “Level of injuries as they relate to CIA,” marked with circle “4.” This creates Output 4.
 - Note on reuse: Outputs 3 and 4 are used as inputs to Step 4, indicated by small circles “3” and “4” on the left side of Step 4.
- Step 4: “Determine injury category of each business activity”
 - Left inputs:
 - One vertical stack shows circles “2,” “3,” and “4,” to indicate the reuse of Outputs 2, 3, and 4, to determine the injury category.

- Right output:
 - A white callout labeled “High watermark injury category of each business activity,” marked with circle “5.” This creates Output 5. “High watermark” conveys that the injury category is set to the highest expected severity across confidentiality, integrity, and availability.
- Note on reuse: Output 5 is used as an input to Step 5, indicated by circle “5.”
- Step 5: “Prepare injury categorization report”
 - Left inputs: A vertical sequence of small circles “1, 2, 3, 4, 5” shows that the final report compiles all earlier outputs: Output 1 (organization-specific table), Output 2 (business processes/information), Output 3 (expected injuries), Output 4 (CIA-level severity), and Output 5 (high watermark injury category).
 - No right-side callout is drawn; the flow continues to the end.
- End: A blue oval labeled “End” below Step 5 marks the conclusion of the process.

GC-specific note

The goal of the security categorization process is to determine the sensitivity and criticality of business activities based on an injury test. This is similar to the goal of the sensitivity assessment questionnaire that is found in the statement of sensitivity (SoS) of many departments and agencies. An SoS captures the types of information assets that an information system will store and process and the classification of that information (for example, Protected B). The SoS also collects the general importance of integrity, as well as the criticality of the program or services, which is often expressed as the maximum permissible downtime.

Although injury is reflected in the information classification marking, the security categorization process makes the injury test for confidentiality explicit. Moreover, the security categorization process extends this explicit injury test to integrity and availability. The result is a security marking that reflects the expected level of injury for confidentiality, integrity, and availability (for example, Protected B, medium integrity, medium availability or PBMM).

In departments and agencies where the SoS process has been successfully implemented and has been in use for many years, completely abandoning a familiar process may not be the best approach to transition from the SoS process to the security categorization process. Departments and agencies could leverage familiarity and acceptability of their SoS process by simply incorporating an injury test in the confidentiality, integrity, and availability sections of their sensitivity assessment questionnaire.

5.3 Injury assessment and categorization process description

The organization should establish a dedicated working group to effectively carry out the injury assessment and categorization process. This group should typically include executives with operational responsibilities, senior security officials (such as the CSO or their delegates), senior privacy officials (such as the CPO or their delegates), security and privacy advisors, and business analysts. Depending on the organization and context, other roles could include a risk

management lead, a legal counsel, a compliance officer, security and privacy architects, and a communications or public relations lead.

5.3.1 Develop organization-specific injury assessment table

To conduct injury assessments and categorization, organizations should create their own injury tables. Small organizations with 1 or few programs serving common interests may only need 1 injury table while large organizations with several programs serving different interests may require several injury tables. If financial thresholds are incorporated into the tailored injury table, the specified dollar amounts should be proportionate to the organization's overall budget to ensure contextual relevance. For example, in the GC, Public Services and Procurement Canada (PSPC)'s Federal Pension Administration program serves very different interests than PSPC's Linguistic Services.

To develop an organization-specific injury assessment table that will inform future risk assessments, it is recommended to consult strategic business documents, such as corporate plans, performance commitments, and priority-setting frameworks, that articulate the organization's objectives and obligations. Business analysts should be closely involved in this process, as they possess critical contextual knowledge and can help identify realistic and relevant injury scenarios. Additional sources, such as regulatory filings, stakeholder reports, and internal audit findings, may also provide valuable insight into business impacts and priorities.

[Table 2](#) contains examples of injury types and injury levels to help GC departments develop injury tables. Departments should include in their injury tables only those types and levels that relate to the interests served by their programs, services, and activities.

Table 2: Examples of injury types and levels (GC-centric)

Injury type	Very low injury level	Low injury level	Medium injury level	High injury level	Very high injury level
Civil disorder or unrest	No reasonable or negligible expectation of injury	Civil disobedience, public obstructions	Riot	Sabotage of critical assets (for example, critical infrastructure)	Large-scale civil unrest 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	Psychological distress	Mental health disorder	Widespread or severe mental health harm
Financial loss to individuals	No reasonable or negligible expectation of injury	Stress or discomfort	Reduced quality of life	Loss of financial security	Not applicable
Financial loss to Canadian companies	No reasonable or negligible expectation of injury	Reduced performance	Reduced competitiveness	Loss of viability	Not applicable

Injury type	Very low injury level	Low injury level	Medium injury level	High injury level	Very high injury level
Financial loss to the Canadian government	No reasonable or negligible expectation of injury	Reduced program performance	Degraded program outcomes	Loss of program viability	Loss of viability of key programs
Harm to the Canadian economy	Not applicable	Not applicable	Reduced performance	Reduced international competitiveness	Compromise of 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	Not applicable	Not applicable	Impediments to the development of major government policies	Impediments to effective law enforcement Loss of continuity of government	Loss of territorial sovereignty

[Table 3](#) presents examples of injury types and injury levels that are more generally applicable. Organizations should include in their injury tables only those types and levels that relate to the interests served by their programs, services, and activities.

Table 3: Examples of injury types and levels

Injury type	Very low injury level	Low injury level	Medium injury level	High injury level	Very high injury level
Protest against the organization	No reasonable or negligible expectation of injury	Civil disobedience, public obstructions	Riot	Destruction of property assets	Not applicable
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	Psychological distress	Mental health disorder	Widespread or severe mental health harm
Financial loss to individuals	No reasonable or negligible expectation of injury	Stress or discomfort	Reduced quality of life	Loss of financial security	Not applicable
Financial loss to the organization	No reasonable or negligible expectation of injury	Reduced performance	Reduced competitiveness	Loss of viability	Bankruptcy

Injury type	Very low injury level	Low injury level	Medium injury level	High injury level	Very high injury level
Legal/regulatory actions against the organization	No legal or regulatory actions expected Warning notices	Small fines Small redress expenses	Moderate fines Stop work orders Moderate redress expenses	Significant fines Temporary licence revocation Limitations on activities Significant redress expenses	Severe fines Permanent licence revocation Cessation order
Civil actions	No reasonable or negligible expectation of liability Settlement with client for a nominal amount	Minimal liability Out-of-court settlement	Moderate liability Compensation	Significant liability High-profile lawsuit Significant financial settlements	Severe liability Class-action lawsuit Severe financial penalties Loss of clients' trust
Reputational harm	No reasonable or negligible expectation of injury	Minimal reputational impact Minimal reputational management costs Limited negative media or social media coverage	Moderate reputational impact requiring corrective action Increased costs to maintain and attract clients Sustained negative media or social media coverage	Significant reputational harm requiring immediate corrective action Significant costs to maintain and attract clients Widespread or prolonged negative media or social media coverage Loss of clients expected	Severe and potentially irreparable reputational harm Loss of key clients Long-term decline in brand reputation

5.3.2 Identify business processes and related information assets

The second step of the injury assessment and categorization process is to identify the business processes and related information assets, including personal information, relevant to the business activity.

There are several sources from which to identify and describe business processes and related information assets. Good sources include:

- business cases
- CONOPS
- functional business requirements
- enterprise architecture documentation which typically describes an organization's business processes and related information assets
- discussions or interviews with business analysts and other individuals within related business communities

The output of this step is a brief description of the business processes and related information assets of relevance to the business activity.

5.3.3 Assess injuries from threat compromise

The third step of the process is the injury assessment. The objective is to determine the potential injuries from threat compromises for each of the business processes and related information assets identified in the previous step. This is achieved by first determining the injuries that could possibly occur as a result of threat actors compromising the confidentiality, integrity, and availability of the business processes and related information assets, and then attributing appropriate levels to these injuries.

Generally, confidentiality, integrity, and availability apply to information assets, while integrity and availability apply to business processes. In the GC, in some exceptional cases where national security or national defence is involved, confidentiality can apply to business processes. In the private sector, those exceptions would usually be related to trade secrets.

Injury levels that apply to business activities may already be documented in organizational deliverables such as business impact analyses, PIAs, SoS, business risk assessments, and TRAs. It may also be helpful to review regulatory instruments such as laws, policies, and regulations that may apply to specific business processes or information. Non-compliance with regulatory requirements could, under certain circumstances, lead to penalties or sanctions that could increase injury. Organizations can leverage this information when assessing injuries related to a failure of their business activities.

When assessing injuries, security practitioners should consider several factors that may influence the results, including aggregation, inference, and interdependency.

5.3.3.1 Aggregation

As the number of assets increases, the injuries arising from compromise may also grow. For example, the unauthorized disclosure of a single personnel file might be expected to cause some embarrassment to the individual and generate public anxiety regarding an organization's ability to protect personal information. However, if all human resources records for a major organization were released inappropriately, the adverse effects could be significantly worse.

From a confidentiality perspective, aggregation has 2 dimensions:

- increased sensitivity as more data elements are added to a record
- increased sensitivity as more records are collected in a file or database

In each case, the confidentiality value of the whole may be greater than that of the individual parts, based on the increased injury expected in the event of unauthorized disclosure.

Aggregation applies equally to availability and integrity values. For example, the destruction of 1 asset, such as a single vehicle, might have clearly defined consequences, whereas the loss of an entire fleet would be much more serious. Unauthorized modification of a single record or complete corruption of a large database would be the integrity equivalent.

5.3.3.2 Inference

By its very nature, inference applies only to confidentiality, where access to seemingly innocuous data of little or no sensitivity may allow a knowledgeable individual to draw much more damaging conclusions regarding another organization's

capabilities or intentions. For example, studying personnel movements to identify the qualifications and affiliations of executives and other employees selected for different positions may provide useful indicators of future policy platforms or business plans.

Unfortunately, the relationships among various data and data sources may be very subtle, even tenuous, so opportunities for inference are generally far more difficult to identify and assess. From a practical point of view, inference must be assessed cautiously because complex scenarios can exaggerate the risk and lead to needless overclassification. The inference scenarios of concern are the ones where aggregations in a non-national security system lead to national security injuries.

5.3.3.3 Interdependency

Due to interdependencies, the loss or degradation of 1 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 on other processes and information resulting from the compromise of a business process or information.

Similar to the problem of aggregation, the injury that would result from the cascading loss of 1 element may be greater than the injury level assigned to any of the independent elements. Types of interdependencies include:

- physical (for example, material output of an infrastructure used by another)
- geographic (for example, a common corridor)
- logical (for example, dependency through financial markets)

The output of this step is a list of expected injuries and injury levels for confidentiality, integrity, and availability by business process and related information assets.

GC-specific note

For consistency within and across departments, security and privacy practitioners should adopt a common categorization marking scheme. As a guideline, it is recommended that injury categories be expressed using the following marking format:

- Confidentiality: Protected/Classified Level
- Integrity: Very low/Low/Medium/High/Very high
- Availability: Very low/Low/Medium/High/Very high

For example: Protected B, Medium, Medium (PBMM)

5.3.4 Determine injury category of each business activity

The fourth step in the injury assessment and categorization process is to determine the injury category of each business activity.

In normal circumstances, the injury category of a business activity should express the highest levels of injury of all related business processes and information assets for each of the security objectives. Individually, these elements may be attributed different levels of injury for a given protection objective. For example, a business activity may involve 1 type of information with an assessed injury level of low for confidentiality and another type of information with an assessed injury

level of medium for the same security objective (both for non-national interest). These individual values are important and should be documented. However, the injury category of the business activity should reflect the highest level of injury. For the preceding example, the business activity's confidentiality level would be marked as "Medium".

Notwithstanding, there may be circumstances where more analysis is required to determine the most appropriate injury category. For example, security and privacy practitioners may attribute a higher level than the "High" benchmark because of the aggregate effects of threat compromise, or an interdependency involving a critical process outside of a business activity's boundary.

The output of this step is the injury category of each business activity, which can be expressed using the same categorization marking format as for individual business processes and information.

5.3.5 Prepare injury categorization report

The final step of the injury assessment and categorization process is to prepare the injury categorization report.

Security and privacy practitioners should summarize in a report the results of the injury assessment for reporting purposes and to serve as input to the organizational security and privacy control and activity profile development. For each business process and related information, the injury categorization report should include:

- a short description of the business process and related information asset(s)
- a description of the expected injuries from threat compromise
- the levels of expected injury as they relate to the loss of confidentiality, integrity, and availability
- the rationale for attributing the levels of injury

5.4 Examples

A spreadsheet with simple examples that help illustrate the injury assessment and categorization process for business activities is available. To request a copy of this spreadsheet, [contact the Contact Centre](#).

Annex A Government of Canada injury levels conversion

Other injury assessment frameworks may use a “3-level” scale of Low, Medium, and High instead of the 5-level scale presented in this publication. Where this is the case, departments can use the scale conversions specified in Table 4, Table 5 and Table 6 to convert injury levels from their 3- or 4-level scale to the 5-level scale outlined in ITSP.10.036.

In conversion Table 6, the “Low” category from the 3-level injury scale may correspond to either “Very low” or “Low” on the 5-level scale, while “High” may map to either “High” or “Very high”. To ensure appropriate categorization, it is recommended to re-evaluate the injury assessment using the 5-level scale directly, considering the specific context and desired level of granularity.

Table 4: Confidentiality – Non-national interest (Protected)

4-level scale value	5-level scale value
No expected injury – Unclassified	Very low
Low – Protected A	Low
Medium – Protected B	Medium
High – Protected C	High
N/A	Very high

Table 5: Confidentiality – National interest (Classified)

4-level scale value	5-level scale value
No expected injury – Unclassified	Very low
NA	Low
Low - Confidential	Medium
Medium – Secret	High
High – Top Secret	Very high

Table 6: Integrity and availability

4-level scale value	5-level scale value
No injury expected	Very low
Low	
Low	Low
Medium	Medium
High	High
High	Very high