Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Information Technology Security Guidance

IT Security Risk Management: A Lifecycle Approach

Departmental IT Security Risk Management Activities

ITSG-33 – Annex 1

November 2012

Canada

Foreword

Annex 1 (*Departmental IT Security Risk Management Activities*) to *IT Security Risk Management: A Lifecycle Approach* (ITSG-33) is an unclassified publication issued under the authority of the Chief, Communications Security Establishment Canada (CSEC).

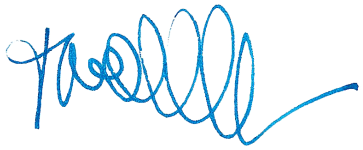
Suggestions for amendments should be forwarded through departmental communications security channels to your IT Security Client Services Representative at CSEC.

Requests for additional copies or changes in distribution should be directed to your IT Security Client Services Representative at CSEC.

For further information, please contact CSEC's IT Security Client Services area by e-mail at itsclientservices@cse-cst.gc.ca, or call (613) 991-7654.

Effective Date

This publication takes effect on 1 November 2012.



Toni Moffa

Deputy Chief, IT Security

Summary

This Annex is part of a series of guidelines on information technology (IT) security risk management that the Communications Security Establishment Canada (CSEC) issues under the Information Technology Security Guidance publication number 33 (ITSG-33) to help Government of Canada (GC) departments and agencies implement, operate, and maintain dependable information systems.

The ITSG-33 guidelines describe an IT security risk management process that includes activities at two distinct levels: the departmental level and the information system level.

This Annex provides guidelines to departments and agencies on the IT security risk management activities that are performed by a departmental IT security function as part of a departmental security program. These activities have four objectives:

- Identify and understand the IT security needs of departmental programs and services, and define security controls that satisfy these needs;
- Deploy security controls that satisfy IT security needs and the IT security risk management requirements of Treasury Board of Canada Secretariat (TBS) policy instruments;
- Continuously monitor and assess the performance of departmental security controls to detect security incidents and identify vulnerabilities and deficiencies in a timely manner; and
- Update implemented security controls based on the results of the continuous monitoring and assessment activities to respond to security incidents, correct vulnerabilities, and continuously improve the security posture of departmental information systems.

Adherence to the ITSG-33 guidelines has many benefits for departments, including compliance with the overall risk management strategy and objectives established by TBS, addressing key aspects of IT security in an efficient manner, and consistently and cost-effectively managing IT security risks.

Revision History

Document No.	Title	Release Date
ITSG-33 Annex 1	IT Security Risk Management: A Lifecycle Approach - Departmental IT Security Risk Management Activities	1 November 2012

Table of Contents

List of Figures

List of Tables

List of Abbreviations and Acronyms

BCP	Business Continuity Planning
BTEP	Business Transformation Enablement Program
CIA	Confidentiality, Integrity, Availability
CIO	Chief Information Officer
CIOB	Chief Information Officer Branch
CONOPS	Concept of Operations
CTO	Chief Technology Officer
CSEC	Communications Security Establishment Canada
DDSM	Directive on Departmental Security Management
DIM	Directive on Identity Management
DSO	Departmental Security Officer
DSP	Departmental Security Plan
FMR	Framework for the Management of Risk
GC	Government of Canada
GSRM	GC Strategic Reference Model
IA	Information Assurance
IEC	International Electrotechnical Commission
ISSIP	Information System Security Implementation Process
ISO	International Organization for Standardization
IT	Information Technology
ITSC	Information Technology Security Coordinator
ITSG	Information Technology Security Guidance
MITS	Management of Information Technology Security
MOU	Memorandum of Understanding
PDARR	Prevention Detection Analysis Response Recovery
PGS	Policy on Government Security
PWGSC	Public Works and Government Services Canada
SSC	Shared Services Canada
SLA	Service Level Agreement
TA	Threat Assessment
TBS	Treasury Board of Canada Secretariat
TRA	Threat and Risk Assessment

1 Introduction

1.1 Context

In the *Standard on the Management of IT Security* [Reference 1], Treasury Board of Canada Secretariat (TBS) assigns to information technology (IT) security coordinators (ITSCs) the responsibility for establishing and managing an IT security function as part of a coordinated departmental security program.

The *Standard on the Management of IT Security* instructs IT security coordinators to:

- Work closely with program and service delivery managers to ensure that their IT security needs are met;
- Provide advice on security controls and IT security solutions;
- Advise program and service delivery managers of potential impacts of new and existing threats; and
- Advise program and service delivery managers on the residual risk of their Government of Canada (GC) programs and departmental services.

The Communication Security Establishment Canada (CSEC) has issued guidelines under the Information Technology Security Guidance publication number 33 (ITSG-33) that describe an IT security risk management process to support those objectives.

1.2 Purpose and Applicability

This Annex provides guidelines to departments on the IT security risk management activities that are performed by an IT security function as part of a departmental security program. Annex 2 of ITSG-33 [Reference 2] provides guidelines on the IT security risk management activities that are performed by IT projects and IT operations groups.

The guidelines in this Annex apply to departments subject to the *Policy on Government Security* (PGS) [Reference 3] that rely on information systems to support non-critical to critical departmental business activities in unclassified, protected, and classified environments.

Adherence to the ITSG-33 guidelines has many benefits for departments including compliance with the overall risk management strategy and objectives established by TBS, addressing key aspects of IT security in an efficient manner, and consistently and cost-effectively managing IT security risks.

1.3 Target Audience

This Annex is intended for departmental security officers (DSOs), IT security coordinators, and security practitioners supporting departmental IT security risk management activities.

1.4 Definitions and Usage of Terms

For definitions of key terms used in this publication, refer to Annex 5 of ITSG-33 [Reference 4].

To simplify the discussion in this publication, key terms are used as follows, unless otherwise specified:

- *"departments"* is used to mean GC departments, agencies, and other organizations subject to the PGS [Reference 3];
- "*threat assessment*" is used to mean IT security threat assessment;
- *"security control"* refers to controls as defined in Annex 3 of ITSG-33 (*Security Control Catalogue*) [Reference 5]; and
- *"domain security control profile"* is used to mean business domain security control profile.

1.5 Compliance with GC Legislation and TBS Policy Instruments

The ITSG-33 guidelines provide guidance to help departments satisfy the main requirements of TBS policy instruments related to IT security and IT security risk management, and to assist security practitioners in their efforts to protect information systems in compliance with applicable GC legislation and TBS policies, directives, and standards as they relate to security controls.

1.6 Publication Taxonomy

This Annex is part of a suite of documents on IT security risk management in the GC. The other documents in the series are as follows:

- ITSG-33, Overview – *IT Security Risk Management: A Lifecycle Approach*
- ITSG-33, Annex 2 – *Information System Security Risk Management Activities*
- ITSG-33, Annex 3 – *Security Control Catalogue*
- ITSG-33, Annex 4 – *Security Control Profiles*
- ITSG-33, Annex 5 – *Glossary*

2 IT Security Risk Management Process

To manage IT security risks efficiently and cost-effectively, the ITSG-33 guidelines describe an approach that departments can adapt to fit their culture, mission and business objectives, their business needs for security, and the threats relevant to their business activities.

Figure 1 depicts the IT security risk management process that is suggested in ITSG-33. The figure shows that IT security risk management activities are orchestrated at two distinct levels in the organization: the departmental level and the information system level.

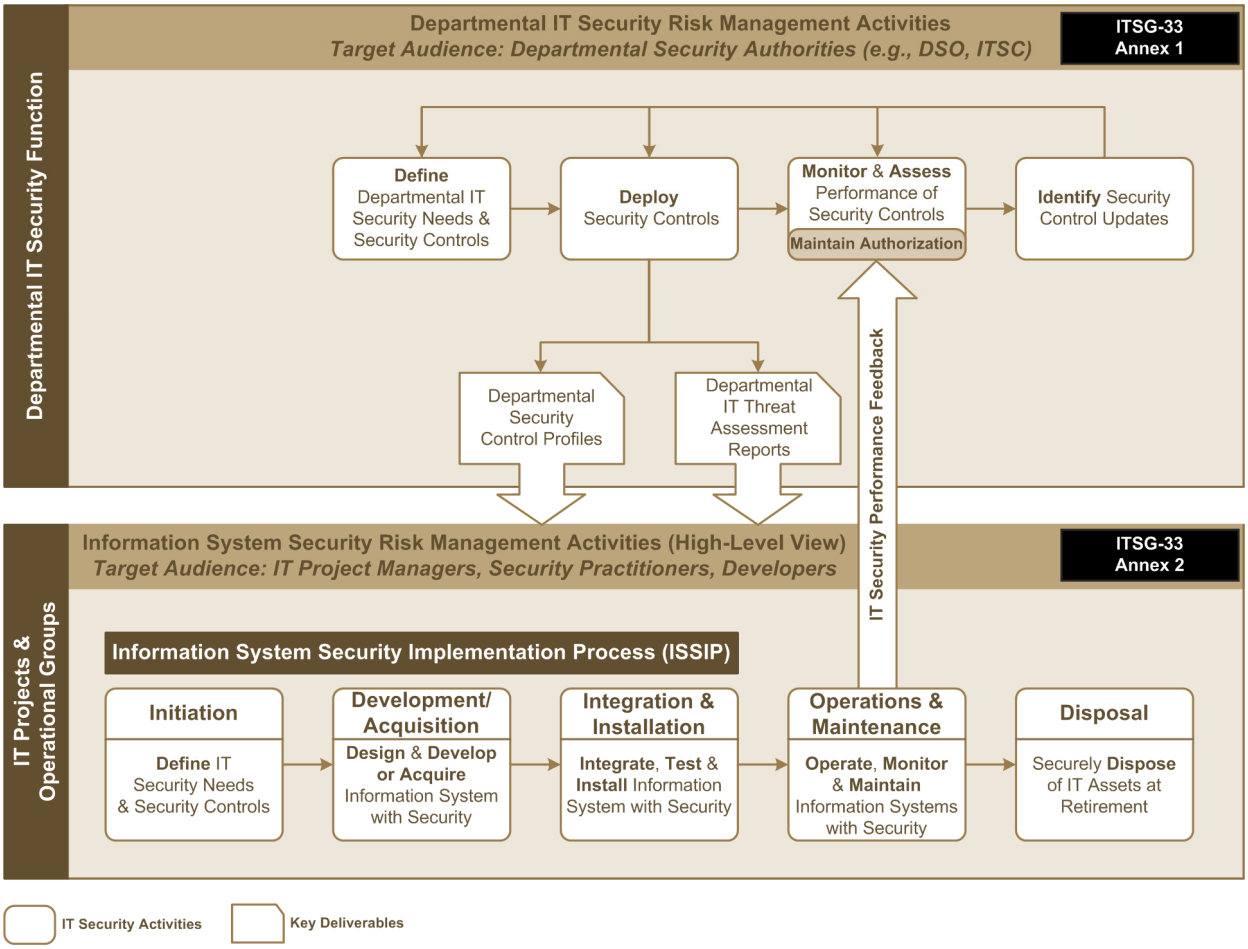


Figure 1: IT Security Risk Management Process

At the departmental level, which is the focus of this Annex, IT security risk management activities are conducted by the department's IT security function (refer to Section 4). The objectives of these activities are:

- Define departmental IT security needs and security controls;
- Deploy security controls;
- Continuously monitor and assess the performance of deployed security controls; and
- Identify required updates to security controls (changes to existing controls or addition of new controls) based on the results of the continuous monitoring, assessment, and authorization maintenance activities, and oversee the implementation of these updates.

At the information system level, IT security risk management activities are conducted by IT projects and IT operations groups. They follow the implementation, operation, and disposal phases of information systems (see Annex 2 of ITSG-33 [Reference 2]). The objectives of those activities are:

- Define IT security needs and security controls for information systems based on the activities of the IT security function;
- Design and develop information systems that satisfy defined security controls;
- Integrate, test, and install information systems with security;
- Operate, monitor, and maintain the security of information systems during the operations and maintenance phase; and
- Securely dispose of IT assets when information systems are retired.

3 Relationships with External Processes

In order for departments to fully capitalize on the benefits of the IT security risk management process, departments need to be aware of important relationships that exist between the departmental IT security risk management activities and other key IT and risk management processes. These relationships are as follows:

- **Integrated risk management** – The departmental IT security risk management activities can support departmental integrated risk management as defined by TBS's *Framework for the Management of Risk* (FMR) [Reference 6] as these activities form a continuous, proactive, and systematic process to understand, manage, and communicate IT security risks from an organization-wide perspective.
- **Business impact analysis** – The results of business impact analyses that program and service delivery managers may conduct in support of their business activities contain useful input to determine the business needs for security and the sensitivity and criticality of departmental business activities. Business needs for security (including privacy requirements) and sensitivity and criticality serve to establish the security category of business activities.
- **Enterprise architecture** – For departments that have implemented one, an enterprise architecture function provides key inputs to help ensure that organization-wide IT security requirements are taken into consideration when defining, deploying and updating security controls.

4 Departmental IT Security Risk Management Activities

This section describes departmental IT security risk management activities that are recommended for incorporation into a departmental security program, and provides guidelines on how to effectively complete them.

Note: ITSG-33 does not include guidelines for the establishment of an IT security function as part of a departmental security program, or how to incorporate the ITSG-33 activities in such a function. Departments can achieve this by following standard departmental or TBS guidelines for the establishment of GC programs. Before incorporating ITSG-33 activities in their departmental security 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. The ITSG-33 guidelines align with this latest governance structure as documented in Section 5.

4.1 Overview

Figure 2 depicts the activities of the IT security risk management process that are conducted at the departmental level. The main goal of these activities is to deploy and maintain a set of security controls that are tailored to the specific security needs and objectives of each department.

Key outputs of departmental IT security risk management activities are departmental security control profiles and departmental IT security threat assessment reports, both of which serve as key inputs to the information system level of the IT security risk management process for the deployment of security controls in information systems.

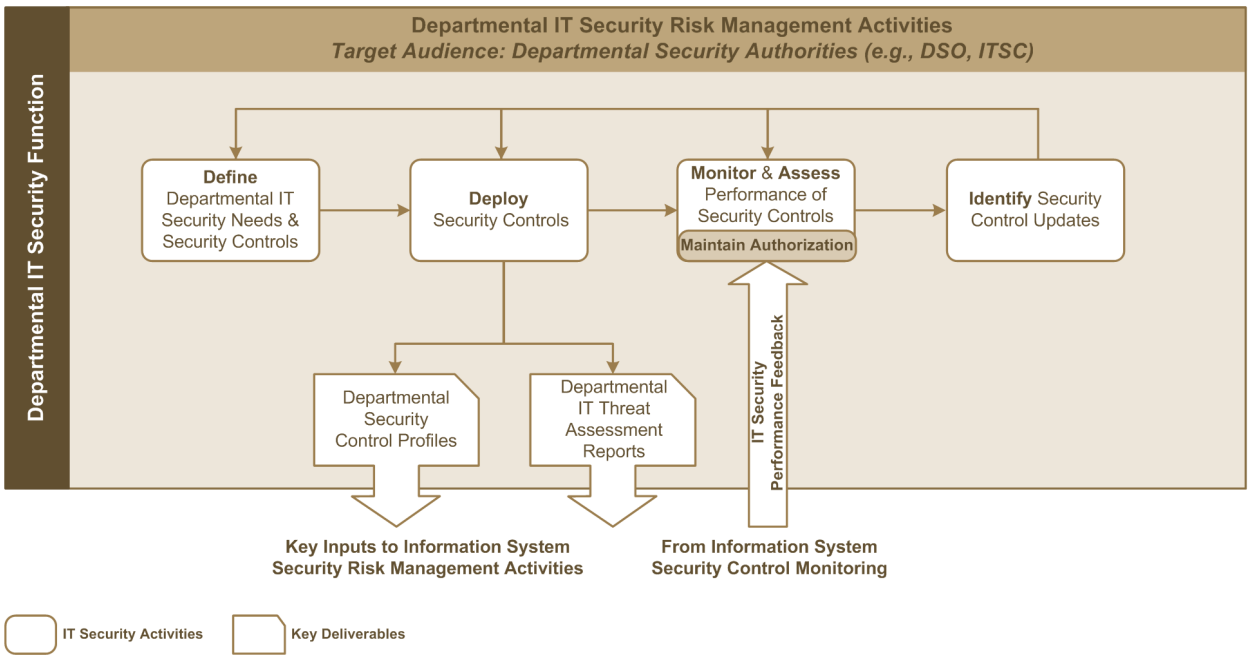


Figure 2: Departmental IT Security Risk Management Activities

The departmental IT security risk management activities seek to achieve the following objectives:

- Identify and document the business needs for security of departmental business activities;
- Define and deploy the departmental common security controls that will support the IT security function (e.g., risk assessment, incident management, performance monitoring) as well as those that will be leveraged by information systems (e.g., central authentication);
- Conduct and maintain departmental threat assessments that security authorities and security practitioners can leverage to help ensure the implementation of dependable information systems that address IT security risks in a more significant and consistent manner;
- Develop departmental security control profiles tailored to departmental business needs for security that IT projects can leverage when implementing and updating departmental information systems;
- Coordinate between other departmental security functions (e.g. physical security, personnel security) to ensure a consistent approach to building and operating dependable information systems;
- Monitor and assess, across the department, the performance of implemented security controls in protecting departmental business activities;
- Identify vulnerabilities, weaknesses, and inefficiencies; and
- Devise and implement corrective measures to improve performance and the department's overall security posture.

4.2 Departmental IT Security Needs & Security Controls

This section describes the process to define departmental IT security needs and security controls. It consists of the following sub-activities:

- Define the scope of the department's IT security risk management activities (Section 4.2.1);
- Identify the business needs for security of departmental business activities (Section 4.2.2);
- Categorize the security of departmental business activities (Section 4.2.3);
- Define the departmental IT security TRA methodology (Section 4.2.4);
- Conduct a departmental IT security threat assessment (Section 4.2.5);
- Specify security control objectives (Section 4.2.6); and
- Develop departmental security control profiles (Section 4.2.7).

Each of these activities for defining departmental IT security needs and security controls is described in the sections to follow. These activities are performed when first implementing the guidelines found in this publication, and then as required based on the assessment of the security posture of a department's information systems (refer to Section 4.6).

4.2.1 Define the Scope of the IT Security Risk Management Activities

The objective of this activity is to define the scope of the department's IT security risk management activities. The scope can be characterized by:

- The department's programs, services, and business activities requiring protection;

- The major departmental IT assets (e.g., business applications, information systems, data centers, local areas networks, data processed and stored) and their geographical locations; and
- The core technologies that are used in departmental information systems.

The scope should clearly delineate the departmental business activities and IT assets that are within the scope's boundaries, and those that are excluded and why. The scope should also identify external dependencies such as the IT services of external service providers.

The output of this activity is a definition of the scope of the department's IT security risk management activities.

4.2.2 Identify Business Needs for Security

The objective of this activity is to identify the business needs for security of departmental business activities. Within the context of IT security risk management, business needs for security come from the need to protect business activities from the risk of relying on information systems. They may originate from:

- Requirements found in regulations, policies, directives, standards, and objectives governing departmental business activities and information management (e.g. an organization Program Activity Architecture);
- Generally-recognized information system threat exposures; and
- Contractual obligations (e.g., memorandums of understanding (MOUs) and service level agreements (SLAs)).

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

Business needs for security express in business terms the protection needs of departmental business activities against adverse information system-related events that could affect the ability of departments to meet their mission, objectives, and obligations. When a regulation establishes a protection requirement that relates to information systems, the business need for security is to satisfy this regulatory requirement. In turn, business needs for security drive the development of more formal security objectives, which may use more technical terminology.

Examples of business needs for security are:

- The need to limit access to sensitive program information to authorized individuals for authorized actions;
- The need to verify the identity of citizens before disclosing program information that relates to them; and
- The need to ensure that only authorized individuals can approve a financial payment to a program recipient.

Departments should identify business needs for security with the help of business analysts and a departmental system architect or security architect (person or group, if one exists). Useful inputs to this activity include business process documentation (e.g., business process descriptions, use cases, concept of operations) and impact assessments (e.g., business impact analysis, privacy impact assessment).

The output of this activity is a set of statements of business needs for security for the department's business activities.

4.2.3 Categorize the Security of Departmental Business Activities

The objective of this activity is to determine the security categories of departmental business activities. A security category expresses the highest levels of expected injuries from threat compromise with respect to the security objectives of confidentiality, integrity, and availability. Business activities are categorized by first determining the expected injuries from IT-related threat compromise to the national and non-national interests that the business activities serve, and then determining the level of these expected injuries.

Departments can categorize their business activities following the process specified in Section 6.

The output of this activity is a security categorization report for departmental business activities.

4.2.4 Define Departmental IT Security TRA Methodology

The objective of this activity is to define the methodology by which IT security threat and risks will be assessed across the department. An IT security TRA methodology needs to be defined at this stage, as a department will use the threat assessment portion when assessing threats to departmental business activities. In addition, IT projects will use this methodology when performing TRA activities.

The output of this activity is a definition of the departmental IT security TRA methodology.

4.2.5 Conduct Departmental IT Security Threat Assessment

The objective of this activity is to conduct an initial departmental (i.e., organization-wide) IT security threat assessment that will guide the selection of security controls, and that will be leveraged by IT projects when implementing information systems[1]. This activity will identify and qualify threats of relevance to the in-scope departmental business activities.

From all the potential threats, departments may specify a subset against which it wishes to protect its business activities. This implies that some threats may have been identified and considered, but were deemed out-of-scope for various reasons. For example, a department may find that protecting against a threat would be too costly or too complex, or that the protection would limit too much a business activity's supporting functionality. Threat information, including decisions and justification for excluding specific threats is documented in a departmental threat assessment report.

An organization-wide threat assessment is a useful tool that departments can use to define, deploy, update, and improve their implemented security controls. The results of an organization-wide threat assessment, along with departmental business needs for security, provide a good basis for establishing security control objectives and developing departmental security control profiles.

More focused, domain-specific threat assessment reports may be produced during the development of departmental security control profiles to document more detailed information concerning threats of relevance to business domains.

[1] A departmental threat assessment is an ongoing process that also supports the information system security risk management activities. See Annex 2 of ITSG-33 [Reference 2] for more detail.

Departmental threat assessments are best conducted by multidisciplinary teams with the assistance of the DSO's office and lead GC security agencies.

A useful departmental threat assessment needs to assess and document:

- Key departmental business activities;
- The security categories of the departmental business activities;
- IT-related threats of relevance to the departmental business activities; and
- Any general exposures that could affect the business activities (e.g., physical location exposed to earthquakes) and strategic options to address them.

The key output of this activity is a departmental threat assessment report, which documents the IT security threats and exposures of relevance to key departmental business activities.

4.2.6 Specify Security Control Objectives

The objective of this activity is to specify departmental security control objectives that will guide the selection of security controls. Security control objectives serve as the basis for selecting and tailoring security controls. Security controls are required to adequately protect departmental information systems and manage IT security risks. Business needs for security are usually written from a business point of view and may use a varied terminology. Security objectives can be standardized in a department and mapped to any business needs for security in a common, standardized terminology.

Examples of security control objectives are (following the examples used in Section 4.2.2):

- Ensure the security of departmental IT services accessible online, and their secure use;
- Prevent unauthorized access to IT services, data, and network resources; and
- Prevent unauthorized creation, modification, or misuse of information in applications, and detect unauthorized data processing activities.

A set of security control objectives is defined in Appendix C of the DDSM [Reference 7]. Additional security control objectives can be defined by security practitioners with help from their department's business communities. Security practitioners can also leverage security control objectives from other sources, such as Annex A of ISO 27001 [Reference 8]. As part of the specification of security control objectives, metrics are defined to enable the measurement of the controls' performance. Security practitioners can leverage security control objective metrics from sources such as ISO 27004 [Reference 9].

Inputs to this activity should include the scope definition, the business needs for security, and the results of the organization-wide threat assessment. Departments with an established enterprise architecture function should also use as input any relevant enterprise security architecture artefacts (e.g., enterprise security requirements).

The output of this activity is the list of departmental security control objectives as they relate to the support of business activities by information systems.

4.2.7 Develop Departmental Security Control Profiles

The objective of this activity is to create departmental security control profiles that are tailored to the security needs of each department. Depending on their mission (e.g., delivering a single program versus

delivering multiple programs) and the complexity of their business activities, departments may have a single, organization-wide security control profile or several domain-specific profiles called "departmental domain security control profiles" or simply "domain security control profiles".

Departmental security control profiles are best developed with the support of several key department-wide information and IT management processes. Although outside the scope of the IT security risk management process, these enterprise processes can help ensure the suitable selection and tailoring of security controls. These supporting processes are:

- The definition of the departmental business activities that are needed to support departmental missions;
- The prioritization of departmental business activities with respect to strategic goals and objectives;
- The definition of the types of information assets needed to successfully execute the departmental business activities, their criticality and sensitivity, and their flows both internally and externally;
- The incorporation of information security requirements into the mission/business processes; and
- The definition of an enterprise architecture that includes IT security requirements.

There are four steps to developing departmental security control profiles:

- Define business domains;
- Define IT security approaches;
- Develop departmental security control profiles; and
- Approve the departmental security control profiles.

These four steps to developing departmental security control profiles are described in the following sections.

4.2.7.1 Define Business Domains

The objective of this activity is to define the business domains of a department in support of developing the required departmental security control profiles. A business domain is characterized by the security categories of its business activities and their relevant IT security threats. Therefore, business domains may have differing protection needs, leading to differences in security control profiles.

For example, consider a set of business activities involving the distribution of non-sensitive GC 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 security category and face more significant threats. This analysis would lead to the definition of two domains requiring two different domain security control profiles.

Departments have some flexibility in how they define their business domains. However they are defined, the security categories of the business activities and the significance of the threat environment should be well documented. Note that the departmental business activities should have been defined earlier (in whole or in part) during the security categorization activity (see Section 4.2.3).

The outputs of this activity are business domain definitions. For each defined business domain, the business domain definition should include the following information:

- A description of the business domain's business objectives, processes and information assets;
- The security category of the business domain;
- A characterization of the threat environment of relevance to the business domain; and
- A statement of the level of risk that the business community deems acceptable when relying on information systems to support the domain's business activities.

4.2.7.2 Define IT Security Approaches

The objective of this activity is to define a set of IT security approaches for the selection of security controls that align with the departmental IT security philosophy, culture, objectives, and priorities.

At the department level, IT security approaches serve as a guide for selecting security controls for departmental security control profiles. At the information system level, IT security 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.

When defining IT security approaches, departments should take into consideration the following inputs:

- Business needs for security (Section 4.2.2);
- Security categories of the departmental business activities (Section 4.2.3);
- Threats documented in the departmental TA (Section 4.2.5);
- Documented security control objectives (Section 4.2.6); and
- Generally-accepted IT security principles and best practices (e.g., ITSG-38 [Reference 10] and ITSG-22 [Reference 11], *Enterprise Security Architecture – A Business-Driven Approach* [Reference 12], NIST SP800-27 *Engineering Principles for Information Technology Security: A Baseline for Achieving Security* [Reference 13] and NIST SP800-14 *Generally Accepted Principles and Practices for Securing Information Technology Systems* [Reference 14]).

The following are examples of IT security approaches that influence the selection of security controls and the specification of security designs that departments can use for the development of their departmental security control profiles:

- Holistic versus piecemeal security approach to design. An holistic approach considers security at the various layers of an information system (e.g., application, data management, middleware, platform and communication layers);
- Defence-in-depth/layered defence versus focus on one-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);
- Multi-tiered incident handling to prevent, detect, analyze, respond, and recover (PDARR) from attacks versus emphasis on a preventive approach;
- 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 (e.g., departmental authentication system) versus implementing custom security services;

- Securing the infrastructure versus securing data assets (e.g., digital rights management);
- Take into account societal factors (e.g., employees' privacy versus monitoring) versus mandating hard-to-use but more secure security controls; and
- Fail safely (closed) versus fail open.

Examples of IT security approach definitions can be found in the security control profiles documented in Annex 4 of ITSG-33 [Reference 15].

4.2.7.3 Develop Departmental Security Control Profiles

The objective of this activity is to develop departmental security control profiles. Departments develop a security control profile for each of its defined business domains. If a department 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.

Departmental security control profiles document the common security controls that are or will be deployed as part of the departmental IT security function, as well as the mandated security controls to be implemented in individual departmental information systems.

Departmental security control profiles are used by the IT security function to coordinate the deployment of common security controls across their organization. They also inform IT projects of the security controls that are or will be inherited by their information system, and those that they have to implement as part of their project to protect the information system that they are developing or updating.

When developing departmental security control profiles, departments select security controls from the catalogue in Annex 3 of ITSG-33 [Reference 5] and tailor them to satisfy departmental security needs (Section 4.2.2) and objectives (Section 4.2.6). The selection and tailoring of security controls is guided by the results of their departmental threat assessment (Section 4.2.5) and the defined IT security approaches (Section 4.2.7.2). For departments that have an enterprise architecture function, security practitioners should also consider IT security-related artefacts when selecting and tailoring information system-specific security controls.

Departmental security control 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;
- Security categories of in-scope business activities;
- Threat context;
- Defined IT security approaches; and
- Any other technical constraints or assumptions that might influence the selection of security controls for information systems.

A key input to the security control profile development process is the departmental threat assessment report (see Section 4.2.5). When developing domain security control profiles, departments may refine departmental threat definitions based on additional threat information that is specific to each domain's business activities. When this occurs, departments may document these refined threat definitions in domain-specific threat assessment reports.

Several of the security controls in the catalogue should be considered for deployment as common security controls. A list of candidate common security controls is provided in Section 7. Candidate common security controls are also highlighted in the security control profiles provided in Annex 4 of ITSG-33 [Reference 15]. Some common security controls may be implemented using technical solutions and operated by IT operations groups. Other common security controls may be under the operational responsibility of the departmental IT security function or other supporting functions.

Examples of common security controls are:

- The departmental personnel security screening program supporting the screening of IT personnel;
- Physical security program supporting the protection of IT facilities;
- Security incident management performed as part of the IT security function to provide a global view of departmental security incidents;
- An information system operated by an IT operations group that provides a common end user authentication solution;
- A department-wide electronic log monitoring system operated by a team of the IT security function, which provides separation of duties between the IT operations and the IT security function; and
- An IT security awareness and training program administered by the departmental learning center.

To develop their departmental security control profiles, departments may leverage applicable security control profiles provided in Annex 4 of ITSG-33 [Reference 15], which are based on the ITSG-33 Security Control Catalogue [Reference 5].

The output of this activity is one organization-wide security control profile or a set of domain security control profiles.

4.2.7.4 Approve the Departmental Security Control Profiles

Once the security control profile(s) are completed, the IT security coordinator should review them and seek their approval from departmental authorities (e.g., program and service delivery managers, DSO, deputy head, as required). As part of this process, the IT security coordinator should ensure that the departmental security controls specified in the profiles satisfy departmental security needs and security control objectives, and that they adequately address threats. The IT security coordinator should also ensure that there will be a good balance between the implementation of security controls and the levels of residual risks that the department is ready to assume.

As per the DDSM [Reference 7], departmental security officers (DSOs) must include the business needs for security, the security control objectives, and the set of security controls that are necessary to meet these objectives in their DSP for approval by their deputy head.

The outputs of this activity are approved departmental security control profiles.

4.3 Deploy Security Controls

Following the deputy head's approval of departmental security control profiles, IT security coordinators and their staff can proceed with coordinating the deployment of security controls. Deployment activities are performed when first implementing the guidelines found in this publication, and then as required

based on the assessment of the security posture of a department's information systems (refer to sections 4.4, 4.5 and 4.6).

4.3.1 Deploy and Operate Common Security Controls

Departments have several options to deploy common security controls:

- They can be deployed as part of the IT security function and operated by the function's personnel;
- They can be deployed by a departmental IT operations group;
- They can be deployed by other groups within the department, or outsourced to another department or private sector service provider; and
- They can be provided by an already existing GC shared or common IT service.

Table 1 provides examples of how common security controls can be deployed.

Table 1: Examples of Common Security Control Deployments

Common Security Control	Deployment Option Selected by IT Security Authorities	Operational Authority
CA-7 Continuous monitoring	Implement an automated monitoring infrastructure	IT security authorities (as a component of the IT security function)
SC-7 Boundary protection	Implement a boundary protection infrastructure	IT operations group - Network operations
CP-7 Alternate processing site	Service contract	Private sector service provider
IA-2 End user identification and authentication	Subscribe to an existing GC shared identification and authentication service	Shared Services Canada (SSC)[2]

When the deployment of a common security control requires the implementation of a supporting information system, departments should implement the supporting information systems through IT projects following the process described in Annex 2 of ITSG-33 [Reference 2].

4.3.2 Deploy Security Controls in Information Systems

To deploy the mandated security controls in information systems, the IT security coordinator promulgates the use of the departmental security control profiles by IT projects and IT operations groups. To that end, IT security coordinators implement a process to disseminate their departmental security control profiles along with departmental threat assessment reports to communities across their organization that are responsible for the implementation and operation of information systems. The promulgation can be done through various means (e.g., monthly IT security bulletins, departmental IT or IT security steering committee or review board).

IT security coordinators also inform program and service delivery managers and security assessors of the availability of departmental security control profiles. Program and service delivery managers and security

[2] Designated provider of GC shared services.

assessors in turn can mandate the use of these appropriate departmental security control profiles by IT projects and IT operations group that relate to their area of responsibility.

IT projects and IT operations groups implement and operate security controls in information systems following the IT security risk management activities described in Annex 2 of ITSG-33 [Reference 2].

4.4 Monitor and Assess Performance of Security Controls

Departments monitor and assess the performance of the implemented common security controls and the security controls implemented in information systems, through the collection, consolidation, and continuous analysis of performance metrics. Many of the monitoring and assessment tasks will be performed by the IT operations groups, and summary reports will be provided to the IT security function for department-wide analysis. Some sensitive monitoring tasks may be performed by the IT security function (if mandated by a security control profile), when separation of duties is required.

Continuous assessment[3] tasks go beyond the performance of security controls and should include:

- The review of security-related change and problem management records;
- The review of security incident reports;
- The conduct of security testing, which could include functional security testing, vulnerability assessments, and penetration testing; and
- The review of the security configuration of information system components.

The monitoring and assessment results will inform departmental authorities of the current state of departmental information systems security posture. A stable and adequate security posture will allow an information system to maintain its authorization to operate. A deteriorating security posture may lead departmental authorities to revoke the authorization to operate until mitigating measures are put in place (see sections 4.5 and 4.6).

4.5 Maintain Authorization

When following the suggested IT security risk management process, departments initially authorize the operation of their information systems as part of the implementation process described in Annex 2 of ITSG-33 [Reference 2]. Then, by continuous monitoring, assessing, and updating security controls, departments maintain the authorization state of their information systems.

The authorization maintenance process consists of the following activities:

- Periodically review the security category of supported business activities;
- Re-assess the threat environment and the security performance of technical environments;
- Review the results of security control performance assessments; and
- Review the activities of IT operations group to ensure that they have adequately maintained the security posture of their information systems according to the security provisions of their operations plans.

[3] Continuous assessment does not necessarily mean real-time assessment. Some assessment activities, such as, for example, 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.

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

- Implementing temporary security measures to protect supported business activities (e.g., disconnect an information system from the Internet, activate a portion of a contingency plan);
- Updating implemented security controls to correct security deficiencies and return the information system to its authorized state of operation (see Section 4.6); and/or
- Accepting the new level of residual risk.

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

Departments should establish in their departmental security plan the frequency of periodic security assessment and review activities (e.g., review of security incident reports, review of threat environment, review of IT operations group security activities). Alternatively, authorizers could establish the frequency of such activities during an information system's initial implementation according to such factors as security category, threats, residual risk levels, and outstanding security deficiencies.

The outputs of authorization maintenance activities include updated residual risk assessments, and updated security provisions of operations plan. The security provisions of the operations plan should include mitigation plans and schedules for any outstanding security deficiencies discovered as a result of the security assessment work (see Section 4.6).

4.6 Identify Security Controls Update

The objective of this activity is to ensure that the security posture of the information systems remain adequate by keeping the implemented security controls (common and those part of information systems) up-to-date, and, if required, adding security controls to increase the security posture of the information systems.

Departments may need to update their implemented security controls for various reasons, including when there is:

- A change in departmental missions or objectives;
- A change in a departmental business activity (e.g., collection of new, more sensitive information under an existing departmental program);
- A change in business needs for security (e.g., as a result of legislative or policy changes);
- A requirement for change as a result of a departmental threat assessment update. (i.e., a program is targeted by more sophisticated threat agents); and
- A requirement for change as a result of performance monitoring (e.g., a security control has proven ineffective in adequately protecting related information systems).

Key inputs to this activity include existing departmental security control profiles and threat assessment reports and the results of performance monitoring and assessment and authorization maintenance

activities (see sections 4.4 and 4.5). This activity can identify the need for improving existing security controls or for adding new ones, and may lead back to an earlier activity of the IT security function to redefine the required security controls and produce an updated security control profile and threat assessment report (see, for example, sections 4.2.3, 4.2.5, 4.2.7), deploy new security controls (see Section 4.3), or conduct further monitoring and assessment Section 4.4.

5 Related Roles and Responsibilities

This section summarizes the responsibilities of departmental roles as they relate to both the departmental and information system security risk management activities.

In support of IT security risk management, TBS policy instruments task departmental senior officials, managers, and individuals within departments with responsibilities pertaining to IT security and risk management. TBS policy instruments governing IT security within the GC (shown in Figure 3) address the organization of IT security at both levels of the suggested IT security risk management process by establishing senior departmental security and IT security roles, and attributing IT security responsibilities across the department.

The ITSG-33 guidelines are aligned with this role-based structure. To help individuals appointed to these roles to adequately fulfill their IT security risk management responsibilities, the ITSG-33 guidelines also suggest more refined roles.

For each GC role defined in this section, a table is provided that maps the IT security risk management responsibilities attributed by TBS policy instruments to the department-level activities of the suggested IT security risk management process. These tables provide additional guidance on the tasks that need to be performed under the department-level activities described in Section 4.

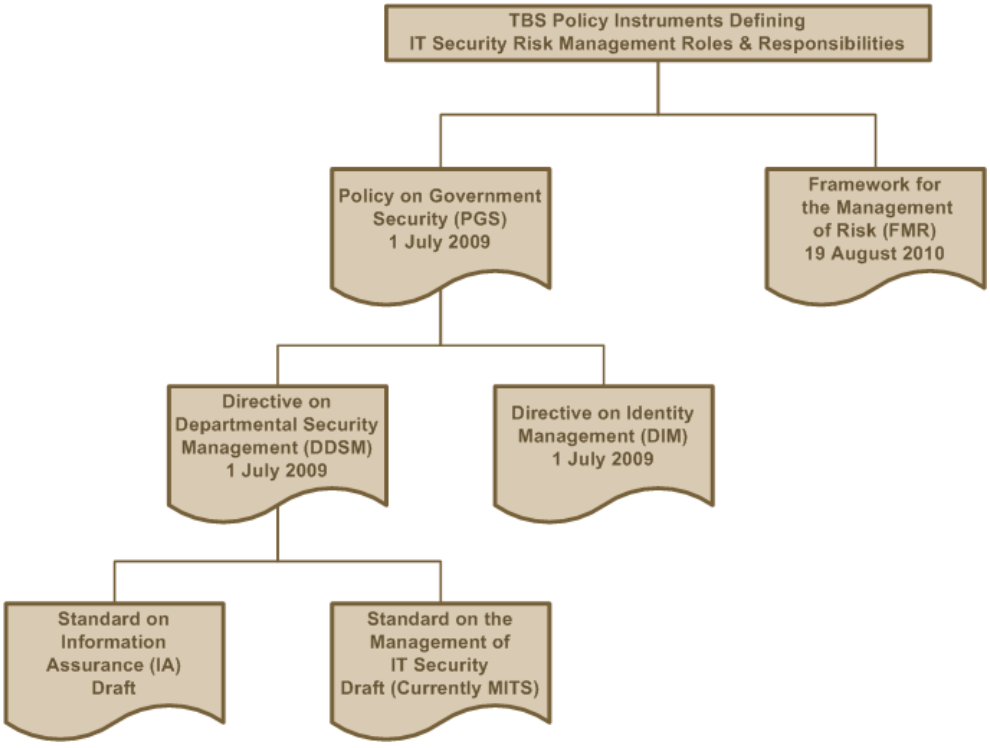


Figure 3: TBS IT Security-related Policy Instruments

5.1 Deputy Heads

The PGS [Reference 3, Section 6.1.1] charges deputy heads with the overall responsibility to establish a security program for the coordination and management of departmental security and IT security activities. As per the PGS, deputy heads must ensure that their departmental security program has a governance structure with clear accountabilities, that it defines objectives that align with departmental and government-wide policies, priorities, and plans, and that it is monitored, assessed, and reported on to measure management efforts, resources, and success toward achieving expected results.

As per the PGS, deputy heads must appoint a DSO to manage the departmental security program. Deputy heads must also ensure that managers at all levels integrate security requirements into departmental plans, programs, activities, and services.

The FMR [Reference 6] instructs deputy heads to:

- Manage their organization's risks by leading the implementation of effective risk management practices;
- Ensure that risk management principles and practices are understood and integrated into the various organizational activities; and
- Monitor risk management practices in their organization.

Table 2 identifies the IT security risk management responsibilities of deputy heads that are supported by the IT security risk management process, and maps those responsibilities to the supporting activities.

Table 2: IT Security Risk Management Responsibility Mapping for Deputy Heads

TBS Policy Instruments			IT Security Risk Management Process (Annex 1)		
Title	**Section**	**Responsibility**	**Section**	**Activity**	**Related Task**
PGS	6.1.4	Approve the DSP that details decisions for managing security risks and outlines strategies, goals, objectives, priorities, and timelines for improving departmental security and supporting its implementation	4.2.7.4	Approve departmental security control profiles	Ensure that the departmental security control objectives and security controls are incorporated into their departmental security plan.
PGS	6.1.5	Ensure that managers at all levels integrate security and identity management requirements into plans, programs, activities, and services	4.2.2	Identify business needs for security	Ensure that managers provide their business needs for security in support of the development of departmental security control profiles.
PGS	6.3	Ensure that periodic reviews are conducted to assess whether the departmental security program is effective, whether the goals, strategic objectives and control objectives detailed in their DSP were achieved, and whether their DSP remains appropriate to the needs of the department and the government as a whole	4.4	Monitor and assess the performance of security controls	Ensure that departmental security officials have implemented the departmental activity for the continuous performance monitoring and assessment of implemented security controls.

TBS Policy Instruments			IT Security Risk Management Process (Annex 1)		
Title	**Section**	**Responsibility**	**Section**	**Activity**	**Related Task**
FMR	6	Manage their organization's risks by leading the implementation of effective risk management practices, both formal and informal	4	All departmental IT security risk management activities	Lead the implementation of the IT security risk management activities.
FMR	6	Ensure that risk management principles and practices are understood and integrated into the various activities of their organization			
FMR	6	Ensure that issues affecting the organization's risk management approach, whether identified through assessments or internal and external monitoring, are examined, reviewed, and addressed effectively			

5.2 Departmental Security Officers

As per the PGS [Reference 3, Section 6.1.2], deputy heads must each appoint a Departmental Security Office (DSO) to manage their departmental security program. The *Directive on Departmental Security Management* (DDSM) [Reference 7, Section 6.1.1] instructs DSOs to develop, implement, monitor, and maintain a departmental security plan (DSP) that:

- Provides an integrated view of departmental security requirements;
- Identifies security threats, risks, and vulnerabilities to determine an appropriate set of security control objectives;
- Identifies and establishes minimum and additional security controls to meet security control objectives and achieve an acceptable level of residual risk; and
- Outlines security strategies, objectives, priorities, and timelines for improving the department's security posture.

The DSO must coordinate with security practitioners the implementation of security controls and other activities necessary to achieve the objectives and priorities of the DSP. DSOs must update their DSP based on the results of performance measurement, evaluation, and risk assessments.

As per the DDSM, DSOs must:

- Ensure that accountabilities, delegations, reporting relationships, and roles and responsibilities of departmental employees with security responsibilities are defined, documented, and communicated to relevant persons;
- Establish security governance mechanisms (e.g., committees, working groups) to ensure the coordination and integration of security activities with departmental operations, plans, priorities, and functions to facilitate decision making; and
- Evaluate the achievement of objectives outlined in their DSP and report the results to the appropriate governance committees.

Table 3 identifies the IT security risk management responsibilities of DSOs that are supported by the IT security risk management process, and maps those responsibilities to the supporting activities.

Table 3: IT Security Risk Management Responsibility Mapping for DSOs

TBS Policy Instruments			IT Security Risk Management Process (Annex 1)		
Title	**Section**	**Responsibility**	**Section**	**Activity**	**Related Tasks**
DDSM	6.1.1.1	Ensure that the DSP provides an integrated view of departmental security requirements	4.2.2	Identify business needs for security	Incorporate business needs for security in the DSP for approval by their deputy head
DDSM	6.1.1.2	Ensure that the DSP identifies security threats, risks, and vulnerabilities to determine an appropriate set of security control objectives	4.2.5	Conduct the departmental IT security threat assessment	Incorporate departmental IT threats assessment results in the DSP for approval by their deputy head
			4.2.6	Specify security control objectives	Incorporate departmental security control objectives in the DSP for approval by their deputy head
DDSM	6.1.1.3	Ensure that the DSP identifies and establishes minimum and additional security controls to meet security control objectives and achieve an acceptable level of residual risk	4.2.7	Develop departmental security control profiles	Oversee the development of departmental security control profiles Incorporate departmental security controls in the DSP for deputy head approval by their deputy head
DDSM	6.1.2	Coordinate with security practitioners the implementation of security controls and other activities necessary to achieve the objectives and priorities of the DSP	4.3.1	Deploy common security controls	Coordinate with security practitioners the deployment of common security controls
DDSM	6.1.4	Update the DSP based on the results of performance measurement, evaluation, and risk assessments	4.6	Identify security control updates	Update the DSP to reflect changes in business needs for security, security control objectives, and security control requirements
DDSM	6.1.7	Develop, document, implement, and maintain processes for the systematic management of security risks to ensure continuous adaptation to the changing needs of the department and threat environment	4	All departmental IT security risk management activities	Oversee the implementation of the suggested IT security risk management activities
DDSM	6.2.1	Monitor the implementation of security activities within the department and recommend appropriate remedial action to the deputy head or senior management committee (as appropriate) to address any deficiencies			

TBS Policy Instruments			IT Security Risk Management Process (Annex 1)		
Title	**Section**	**Responsibility**	**Section**	**Activity**	**Related Tasks**
DDSM	6.1.9	Monitor the effectiveness of the security controls to ensure that they remain current and address the security requirements identified in risk assessments	4.4	Monitor and assess the performance of security controls	Oversee the monitoring and assessment of implemented security controls (common and information systems)
DDSM	6.1.10	In liaison with security practitioners, monitor for changes in the threat and vulnerability environments to ensure that security controls remain current and corrective action is taken when necessary			
DDSM	6.1.11	Measure performance on an ongoing basis to ensure that an acceptable level of residual risk is achieved and maintained			

5.3 IT Security Coordinators

According to the *Standard on the Management of IT Security* [Reference 1], IT security coordinators are responsible for establishing and managing, on behalf of their DSO, a departmental IT security function within the departmental security program. The IT security coordinator must:

- Review and recommend approval by the DSO of departmental IT security policies and standards, and all policies that have IT security implications;
- Ensure the review of the IT security related portions of departmental request for proposals and other contracting documentation, including security requirements checklists; and
- Recommend approval of all contracts for external providers of IT security services.

The *Standard on the Management of IT Security* instructs IT security coordinators to:

- Work closely with program and service delivery managers to ensure that their IT security needs are met;
- Provide advice on security controls and their implementation; and
- Advise program and service delivery managers of potential impact.

Table 4 identifies the IT security risk management responsibilities of IT security coordinators that are supported by the IT security risk management process, and maps those responsibilities to the supporting activities.

Table 4: IT Security Risk Management Responsibility Mapping for IT Security Coordinators

TBS Policy Instruments			IT Security Risk Management Process (Annex 1)		
Title	**Section**	**Responsibility**	**Section**	**Activity**	**Related Tasks**
MITS	9.1	Establish and manage a departmental IT security program as part of a coordinated departmental security program	4.2	Define departmental IT security needs and security controls	Coordinate the activities to define departmental IT security needs and security controls
			4.3.1	Deploy and operate common security controls	Coordinate the deployment of, and manage the operations of common security controls
MITS	9.1	Establish an effective process to manage IT security incidents, and monitor compliance with it	4.4	Monitor and assess the performance of security controls	Coordinate the establishment of the departmental monitoring and assessment process and monitor its operations
MITS	9.1	Review and recommend approval by the DSO of departmental IT security policies and standards, and all policies that have IT security implications	4.2.7.4	Approve the departmental security control profiles	Review and recommend approval of the departmental security control profiles
MITS	9.1	Work closely with program and service delivery managers to ensure that their IT security needs are met	4.2.2	Identify business needs for security	Coordinate the identification of departmental business needs for security
MITS	9.4	Ensure that appropriate security measures are applied to all departmental information management and IT assets, activities, and processes	4.3.2	Promulgate departmental security control profiles	Promulgate the use by IT projects of departmental security control profiles for the implementation of departmental information systems
MITS	9.1	Advise program and service delivery managers of potential impacts of new and existing threats, and to advise them on the residual risk of a program or service	4.2.5	Conduct the departmental IT security threat assessment	Disseminate the results of departmental threat assessments to business communities across the department

5.4 BCP Coordinators and CIOs

As per the *Standard on the Management of IT Security* [Reference 1], business continuity planning (BCP) coordinators and chief information officers (CIOs) must ensure a comprehensive approach to continuous service delivery. To that end, BCP coordinators and CIOs, in collaboration with their IT security coordinator, can leverage the IT security risk management process to ensure that departmental information security and business continuity requirements are reflected in departmental business needs for security (Section 4.2.2), and that these requirements are adequately addressed by departmental security control profiles (Section 4.2.7).

5.5 Managers

As per the DDSM [Reference 7], managers must ensure that security requirements are integrated into business planning, programs, services, and other management activities. In support of risk management, managers must:

- Assess security risks;
- Formally accept residual risks or recommend acceptance of residual risks as defined in the DSP;
- Periodically reassess and re-evaluate risks in light of changes to programs, activities, or services and
- Take corrective action to address identified deficiencies.

Table 5 identifies the IT security risk management responsibilities of managers that are supported by the IT security risk management process, and maps those responsibilities to the supporting activities.

Table 5: IT Security Risk Management Responsibility Mapping for Managers

TBS Policy Instruments			IT Security Risk Management Process (Annex 1)		
Title	**Section**	**Responsibility**	**Section**	**Activity**	**Related Tasks**
DDSM	6.1.22	Ensure that security requirements are integrated into business planning, programs, services, and other management activities	4.2.2	Identify business needs for security	Provide their information security requirements to help identify business needs for security
			4.2.3	Categorize the security of departmental business activities	Provide the security categorization of their information assets to help categorize business activities
DDSM	6.1.23	Assess security risks, formally accept residual risks or recommend acceptance of residual risks as defined in the DSP, and periodically reassess and re-evaluate risks in light of changes to programs, activities, or services, and taking corrective action to address identified deficiencies	4.2.5	Conduct the departmental IT security threat assessment	Inform their IT security coordinator of threats of relevance to their business activities

TBS Policy Instruments			IT Security Risk Management Process (Annex 1)		
Title	**Section**	**Responsibility**	**Section**	**Activity**	**Related Tasks**
DDSM	6.1.24	Monitor the implementation and effectiveness of security controls and report accordingly to the DSO or security practitioner, as appropriate	4.4	Monitor and assess the performance of security controls	Inform their IT security coordinator of the effectiveness of implemented security controls in information systems supporting their business activities

5.6 Program and Service Delivery Managers

As per the *Standard on the Management of IT Security* [Reference 1], program and service delivery managers[4] must ensure an appropriate level of security for their programs and services. They must work with the departmental IT security community to manage on an ongoing basis the risk to their programs and services. Program and delivery managers must determine the IT security needs of their programs and services.

As described in Section 5.13, managers are, in general, responsible for authorizing the operations of the information systems that are supporting their programs and services under a specific set of security conditions. By means of this authorization, program and service delivery managers assume responsibility for relying on these information systems, and therefore, accept the risks associated with doing so[5].

Table 6 identifies the IT security risk management responsibilities of program and service delivery managers that are supported by the IT security risk management process, and maps those responsibilities to the supporting activities.

Table 6: IT Security Risk Management Responsibility Mapping for Program and Service Delivery Managers

TBS Policy Instruments			IT Security Risk Management Process (Annex 1)		
Title	**Section**	**Responsibility**	**Section**	**Activity**	**Related Tasks**
DDSM	6.1.23	Assess security risks, formally accept residual risks or recommend acceptance of residual risks as defined in the departmental security plan, and periodically reassess and re-evaluate risks in light of changes to programs, activities, or services, and taking corrective action to address identified deficiencies	4.5	Maintain authorization	Maintain authorization to operate for the information systems for which they are the responsible manager or authorizer, by actively participating in all authorization maintenance activities

[4] A program or service delivery manager is responsible for the continued delivery of a GC program, service, or other type of business activity.

[5] For information systems impacting several business activities from different programs, impacting other departments, or third parties, senior departmental authorities, including the deputy head, could assume responsibility for authorizing such information systems.

TBS Policy Instruments			IT Security Risk Management Process (Annex 1)		
Title	**Section**	**Responsibility**	**Section**	**Activity**	**Related Tasks**
MITS	9.6	Ensure an appropriate level of security for their programs and services	4.2	Define departmental IT security needs and security controls	Participate in the definition of departmental security needs and security controls to: • Provide the business needs for security for the departmental business activities under their responsibility (Section 4.2.2) • Provide, with the collaboration of managers, information security requirements relating to the departmental business activities under their responsibility (Section 4.2.3) • Provide input to the departmental threat assessment (Section 4.2.5) • Provide input to the specification of security control objectives (Section 4.2.6)
MITS	9.6	Determine the IT security requirements of their programs and services	4.2.7	Develop departmental security control profiles	Participate in the development of departmental security control profiles that relate to their business activities
MITS	9.6	Work with departmental security specialists to risk manage their programs or services			
MITS	9.6	Ensure that, within their areas of responsibility, the requirements stated in this standard, the *Policy on Government Security* and other related policies, standards and technical documentation, are met			

5.7 Common Security Control Providers

A common security control provider is a program or service delivery manager who implements and operates a security control that is common to, or supports several information systems on behalf of the department. Common security controls are described in Section 4.2.7.3.

Common security control providers contribute to the departmental IT security risk management activities by:

- Participating in the conduct of departmental threat assessments (Section 4.2.5);
- Participating in the development of departmental security control profiles (Section 4.2.7);
- Implementing and operating common security controls (Section 4.3.1);
- Participating in the monitoring and assessment of security controls (Section 4.4); and
- Participating in the update of security controls (Section 4.6).

5.8 IT Project Managers

As per the *Standard on the Management of IT Security* [Reference 1], IT project managers must ensure that project security requirements are met. Guidelines to support IT project managers in achieving this objective are provided in Annex 2 of ITSG-33 [Reference 2].

5.9 Security Practitioners

The DDSM [Reference 7] establishes that security practitioners are responsible for the selection, implementation, and maintenance of security controls related to their area of responsibility to ensure that control objectives are achieved. Depending on the structure of the departmental security program, the DDSM states that security practitioners must maintain a functional or direct reporting relationship with the DSO to ensure that departmental security activities are coordinated and integrated.

As per the DDSM, security practitioners must:

- Evaluate the implementation and effectiveness of security controls, report on the achievement of control objectives to the DSO, and recommend corrective action to address deficiencies identified in performance measurement and assessments;
- Provide the DSO, managers at all levels, and employees with expert advice on the application and effectiveness of security controls related to their area of responsibility; and
- Participate in threat and risk assessment (TRA) activities and contribute to the development of the DSP, as required.

Table 7 identifies the IT security risk management responsibilities of security practitioners that are supported by the IT security risk management process, and maps those responsibilities to the supporting activities.

Table 7: IT Security Risk Management Responsibility Mapping for Security Practitioners

TBS Policy Instruments			IT Security Risk Management Process (Annex 1)		
Title	**Section**	**Responsibility**	**Section**	**Activity**	**Related Tasks**
DDSM	6.1.17	Select, implement, and maintain security controls related to their area of responsibility to ensure that control objectives are achieved	4.2	Define departmental IT security needs and security controls	Participate in the definition of departmental IT security needs and security controls by: • Assisting their IT security coordinator with the definition of the scope of the department's IT security risk management activities (Section 4.2.1) • Participating in the identification of business needs for security (Section 4.2.2) • Categorizing the security of departmental business activities (Section 4.2.3) • Defining the departmental IT security TRA methodology (Section 4.2.4) • Specifying security control objectives (Section 4.2.6) • Developing departmental security control profiles (Section 4.2.7)
			4.3.1	Deploy and operate common security controls	Participate in the deployment and operation of common security controls
			4.6	Identify security control updates	Identify security control updates and participate in their implementation
			4.2.7	Develop departmental security control profiles	Ensure that the selection of security controls satisfy business needs for security
DDSM	6.1.18	Evaluate the implementation and effectiveness of security controls, reporting on the achievement of control objectives to the DSO, and recommending corrective action to address deficiencies identified in performance measurement and evaluations	4.4	Monitor and assess the performance of security controls	Monitor and assess the performance of implemented security controls (departmental and information systems)
DDSM	6.1.21	Participate in threat and risk assessments and contributing to the development of the DSP, as required	4.2.5	Conduct the departmental IT security threat assessment	Conducting the departmental threat assessment

5.10 Security Assessors (Internal and External)

The purpose of the security assessor role is to execute the security assessment activities[6] of the IT security risk management process. Security assessors should also proactively participate in other departmental IT security activities to help ensure that key outputs satisfy departmental security needs and objectives up front instead of relying on security assessments to identify deficiencies and non-compliances later in the process. Security professionals in various fields can assume this role.

Security assessors support the departmental IT security risk management process by:

- Participating in the conduct of departmental threat assessments (Section 4.2.5);
- Participating in the development of departmental security control profiles (Section 4.2.7);
- Assessing the performance of security controls (Section 4.4); and
- Participating in the update of security controls (Section 4.6).

Security assessors also conduct security assessment activities at the information system level of the IT security risk management process. These security activities are described in Annex 2 of ITSG-33 [Reference 2].

More sensitive or critical departmental business activities or information systems may require a higher level of independence from the security assessment activities than can be provided by resources internal to a department or an IT project. Where there is such a requirement, a departmental official or an authorizer can appoint an external security assessor to complete security assessment activities. The external security assessor may come from another area of the organization or be hired under contract from a qualified external firm.

The role of an external security assessor is not equivalent to the role of a certification authority. A certification authority is one type of security assessor. Where a department or agency has appointed a certification authority to act as an external security assessor on IT projects, the certification authority will be responsible for completing security assessment and approval activities in coordination with security practitioners, authorizers, and IT project managers.

5.11 Enterprise Security Architects

An enterprise security architect is an individual responsible for ensuring that the information security requirements necessary to protect a department's business activities are adequately addressed in all aspects of information system design. Although beyond the scope of the ITSG-33 guidelines, CSEC recommends that departments implement an enterprise security architecture function to support IT security risk management. Some departments may have an enterprise security architect on staff. The function may also be the responsibility of a senior manager such as a CIO or a chief technology officer (CTO).

In support of IT security risk management, enterprise security architects should provide guidance and advice to their DSO, their IT security coordinator, managers, program and service delivery managers, and IT operations managers on a range of security-related issues (e.g., establishing information system boundaries, assessing the severity of weaknesses and deficiencies in departmental information systems,

[6] These activities are analogous to quality assessment activities in an industrial manufacturing process.

the security provisions of operations plans, risk mitigation approaches, security alerts, and potential adverse effects of identified vulnerabilities).

Enterprise security architects can contribute useful input to the following departmental IT security risk management activities:

- The conduct of departmental threat assessments (Section 4.2.5);
- The specification of security control objectives (Section 4.2.6);
- The development of departmental security control profiles (Section 4.2.7); and
- The update of security controls (Section 4.6).

5.12 IT Operations Managers and Personnel

An IT operations manager is a program or service delivery manager who is responsible for the operations, maintenance, and disposal of one or more information systems. With respect to IT security risk management, IT operations managers are generally responsible for addressing the operational interests of the user community (i.e., users who require access to information systems to satisfy business operations or operational requirements) and for ensuring on-going compliance with IT security requirements.

IT operations managers and personnel participate in departmental IT security risk management activities by operating common security controls (Section 4.3.1) and providing performance metrics for the security controls implemented in the information systems for which they have operational responsibility (Section 4.4).

IT operations managers and personnel are also responsible for the secure operations and maintenance of information systems, and the secure disposal of IT assets. These activities are described in Annex 2 of ITSG-33 [Reference 2].

In general terms, IT operations managers and their personnel, in coordination with their departmental IT security coordinator, should:

- Participate in the development of operations plans addressing security concerns for their information systems;
- Apply and maintain operations plans addressing security concerns;
- Ensure that their information systems are implemented and operated in accordance with the agreed-upon security controls;
- In coordination with program and service delivery managers, determine who should have access to information system resources, and with what types of privileges or access rights;
- Ensure that information system users and support personnel receive the requisite security training (e.g., instruction in rules of behaviour); and
- Based on guidance from authorizers, inform appropriate managers of the need to conduct on-going assessments, ensure that the necessary resources are available for the effort, collaborate with security assessors from the IT security function, and provide the required information system access, information, and documentation to security assessors, as required.

5.13 Authorizers

The authorizer is the party that grants the "Authority to Operate" an information system, and in so doing accepts the risk to the business associated with running that system within the current operational context. Depending upon the relative importance or scope of a business system, a more senior official may be named the authorizer for that system, since the level of the authorizer must be commensurate with the residual risk being accepted, and with the level of responsibility for the supported program and its successful delivery. For departmental information systems, the authorizer is normally the Program or Service Delivery Manager (refer to Section 5.6 above). For common systems or services (including SSC services) within the Government of Canada Enterprise, the CIO of the GC (i.e., TBS Chief Information Officer Branch (CIOB)) acts as the authorizer and performs the same functions as program and service delivery managers for that enterprise-wide context. For systems or services shared by two or more organizations, the manager of the program or service acts as the authorizer.

6 Security Categorization Process

6.1 Introduction

This section describes how departments can perform a security categorization of their departmental business activities (i.e., business processes and related information assets) to support the definition of their departmental security control profiles in a manner that is consistent with applicable TBS policies, directives, and standards.

Security categorization is a tool to establish the relative importance of departmental business activities. At the departmental level, security categories of business activities serve as input for conducting threat assessments, specifying security control objectives, and developing departmental security control profiles. At the information system level, security categories of business activities serve as input for establishing security assurance requirements, selecting and tailoring security controls, and conducting TRA activities.

This suggested security categorization process aligns with the *Framework for the Management of Risk* (FMR) [Reference 6].

6.2 Concepts

When business activities are compromised by IT-related threats, there may be injury to the national interests[7] or the non-national interests[8] that the business activities serve. Injury can occur because of the unauthorized use, disclosure, modification, or destruction 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 IT security. Injury due to the modification of information or the corruption of business processes relates to the integrity objective (i.e., accuracy, completeness, authenticity, intended use) of IT security. Injury due to the destruction of information or the interruption of business processes relates to the availability objective of IT security.

Security categorization is a process to determine the expected injuries from threat compromise, and the level of these expected injuries with respect to the security objectives of confidentiality, integrity, and availability. The result of this process is a security category for a business activity, which expresses the highest levels of expected injury for all three IT security objectives.

[7] National interests: The security and the social, political, and economic stability of Canada.

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

6.3 Security Categorization Process

As illustrated in Figure 4, the security categorization process for a business activity can be summarized in four steps:

- Identify the business processes and information assets that relate to the business activity;
- For each business process and related information assets, determine the expected injuries from threat compromise to the national or non-national interests that the business activity serve, and determine the levels of these injuries as they relate to confidentiality, integrity, and availability;
- Determine the security category of the business activity by determining the highest levels of expected injury for confidentiality, integrity, and availability (CIA); and
- Prepare a security categorization report.

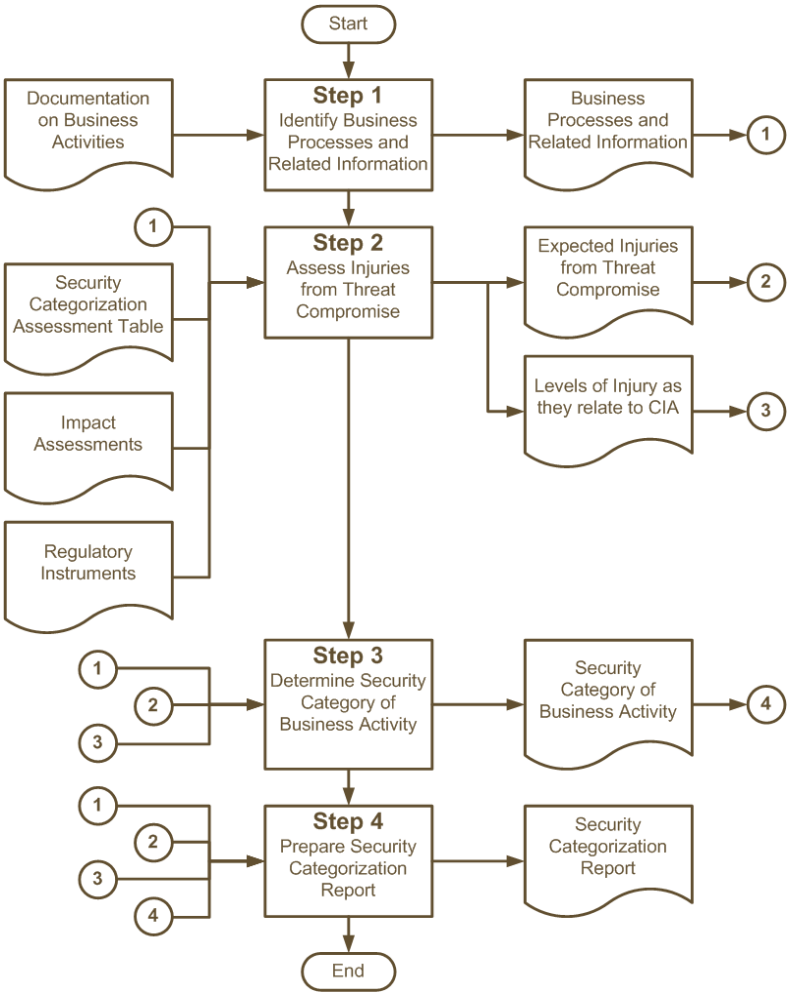


Figure 4: Security Categorization Process

6.4 Security Categorization Process Description

6.4.1 Identify Business Processes and Related Information Assets

The first step of the security categorization process is to identify the business processes and related information assets 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;
- Concepts of operations (CONOPS);
- Business functional specifications;
- Enterprise architecture documentation which typically describes an organization's business processes and related information assets in some detail;
- Discussions or interviews with business analysts and other individuals within related business communities; and
- TBS's *Government of Canada Strategic Reference Model (GSRM) Service Reference Patterns* [Reference 16] may also be useful in identifying and describing business processes.

As illustrated in Figure 4, the output of this step is a brief description of the business processes and related information assets of relevance to the business activity.

6.4.2 Assess Injuries from Threat Compromise

The second step of the security categorization process is the injury assessment.

The objective of the injury assessment is to determine the expected injuries from threat compromise for each of the business processes and related information assets identified in the previous step. This is achieved by first determining, using Table 8 as a guide, the injuries that are likely to occur as a result of threats compromising the confidentiality, integrity, and availability of the business processes and related information assets, and then attributing appropriate levels of these injuries. Confidentiality, integrity, and availability apply to information assets, while integrity and availability apply to business processes.

Ideally, departments should assess injury for their business processes and related information assets through a departmental process using multidisciplinary teams that include representatives from business, legal, access to information, and privacy areas.

Table 8: Examples of Injury Types and Levels

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

Injury levels that apply to business activities may already be documented in departmental deliverables such as business impact analyses, privacy impact assessments, statements of sensitivity, business risk assessments, and threat and risk assessments. Reviewing regulatory instruments such as laws, policies, and regulations that may apply to specific business processes or information may also be helpful as non-compliance to regulatory requirements could, under certain circumstances, lead to penalties or sanctions that could increase injury. Departments can leverage this information when assessing injuries related to a failure of their business activities.

These deliverables may present injury levels using a three-level scale of low, medium, and high instead of the five-level scale used in ITSG-33 guidelines. Where such is the case, departments can use the scale conversion specified in Table 9 to convert injury levels from their three-level scale to ITSG-33's five-level scale. Note that this conversion table was derived from the expanded injury table contained in the *Harmonized TRA Methodology* [Reference 17].

Table 9: Converting Injury Levels from Three-level to Five-level Scale

Three-level Scale	Five-level Scale				
	Very Low	**Low**	**Medium**	**High**	**Very High**
Confidentiality – Non-national Interest (Protected)					
No expected injury (Unclassified)	X				
Low – Injury expected (Protected A)		X			
Medium – Serious injury expected (Protected B)			X		
High – Extremely grave injury expected (Protected C)				X	
Confidentiality – National Interest (Classified)					
No injury expected – Unclassified	X				
Low - Injury expected (Confidential)			X		
Medium – Serious injury expected (Secret)				X	
High – Exceptionally grave injury expected (Top Secret)					X
Integrity and Availability					
No injury expected	X				
Low - Injury expected	Very low or low based on re-assessment				
Medium – Serious injury expected			X		
High – Extremely grave injury expected				High or very high based on re-assessment	

When assessing injuries, security practitioners should consider several factors that may influence the results, including:

- **Aggregation** – Individual business processes and related information assets can each be assigned an injury level. However, the injury that would result from compromise of an aggregate of processes and information, considered as a whole, may be greater than the injury level assigned to any of the individual parts.
- **Inference** – In some cases, the analysis of information categorized at one level of sensitivity may allow an informed individual to draw and act upon conclusions that could compromise more sensitive information. For example, personnel records categorized as Protected B for privacy reasons might contain information that provides some indication of the individual's role, and therefore, the operational mission or capability of the parent organization—information that in certain circumstances might compromise national interest.
- **Interdependency** – Due to interdependencies, the loss or degradation of one business process and its associated information may impact other processes and related information. The purpose of analyzing interdependencies is to determine if there is a likelihood of a high cascading effect resulting from the compromise of a business process or information on other processes and information. Similar to the problem of aggregation, the injury that would result from the cascading loss of one element may be greater than the injury level assigned to any of the independent elements. Types of interdependencies include physical (e.g., material output of one infrastructure used by another); geographic (e.g., common corridor); and logical (e.g., dependency through financial markets).

As shown in Figure 4, 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. For consistency within and across departments, security practitioners should adopt a common marking scheme. As a guideline, it is recommended that security categories be expressed using the following marking format:

> (Protected/Classified Level, Very low/Low/Medium/High/Very high Integrity, Very low/Low/Medium/ High/Very high Availability).

6.4.3 Determine Security Category of Business Activity

The third step in the security categorization process is to determine the security category of the business activity.

In normal circumstances, the security 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 one 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 security category of the business activity should reflect the highest level of injury. For the preceding example, the business activity's confidentiality would be marked as Protected B.

Notwithstanding, there may be circumstances where more analysis is required to determine the most appropriate security category. For example, security practitioners may attribute a higher level than the

high watermark 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 security category of the business activity, which can be expressed using the same marking format as for individual business processes and information.

6.4.4 Prepare Security Categorization Report

The fourth step of the security categorization process is the preparation of the security categorization report.

Security practitioners should summarize in a report the results of the injury assessment for reporting purposes and to serve as input to two downstream activities (the IT security function definition process and the departmental security control profile development process). For each business process and related information, the security categorization report should include:

- A short description;
- A description of the expected injuries to threat compromise;
- The levels of expected injury as they relate to confidentiality, integrity, and availability; and
- The rational for attributing the levels of injury.

6.5 Examples

Table 10, Table 11 and Table 12 provide simple examples that help illustrate the security categorization process for business activities.

Table 10: Security Categorization of a Vaccination Campaign's Publication Activity

Business Processes		**Information Assets**	
Name	**Description**	**Name**	**Description**
Prepare awareness material	The process to develop the vaccination campaign's awareness material.	Vaccination campaign awareness information	Unclassified information concerning the availability of the vaccine and its health benefits to Canadian families.
Promote awareness	Promote awareness of the vaccination campaign by making the awareness material available to Canadians.	Vaccination campaign awareness information	Same as above.

Example Failure of Business Activity	**Example Consequences of Failure**	**Injuries that can Reasonably be Expected**	**Injury Level**
Information published under the program is maliciously modified	Citizens targeted by the campaign make the wrong decision based on incorrect information and the unavailability of the required information. Citizens are not vaccinated as a result.	Physical illness	Confidentiality = Very Low (Unclassified) Integrity = Medium Availability = Medium
Security Category of business activity = (Unclassified, Medium Integrity, Medium Availability)			

Table 11: Security Categorization of the Payment Activity of a Home Renovation Program for People with Reduced Mobility

Business Processes		Information Assets	
Name	**Description**	**Name**	**Description**
Determine eligibility	Accept program applications and determine eligibility of applicants to receive a payment.	Applicant information	Protected B applicant information, including full name, home address, phone number, date of birth, citizenship, SIN, and direct deposit bank account information.
		Information concerning the reduced mobility	Protected B medical information describing the nature of the reduced mobility.
		Benefit information	The approved amount of the financial benefit and the payment schedule.
Provide direct deposit payment	Issue direct deposit payments in accordance with the schedule	Payment information	Protected B payment information, including bank account number, date of payment, and payment amount.

Example Failure of Business Activity	Example Consequences of Failure	Injuries that can Reasonably be Expected	Injury Level
The payment activity is interrupted for several weeks	The completion of required renovations are delayed while program recipients await their payment	Physical discomfort Stress	Availability = Low
The payments issued to program recipients are lower than the approved entitlement due to processing errors	Program recipients have to compensate for the financial loss using their own savings	Financial loss causing psychological stress	Integrity = Low
Program recipient records, which include SIN, date of birth, and mailing address, are stolen by criminals engaged in identity theft	The privacy of program recipients has been violated, and their financial security may be at risk	Financial losses affecting quality of life Distress	Confidentiality = Medium (Protected B)
Security category of business activity = (Protected B, Low Integrity, Low Availability)			

Table 12: Security Categorization of a Troop Deployment Management Activity

Business Processes		Information Assets	
Name	**Description**	**Name**	**Description**
Collect information	Collect intelligence information from various sources	Intelligence information	Information concerning the location and intentions of hostile forces.
Conduct analysis	Analyze the intelligence information and determine targets.	Intelligence information	Same as above.
		Target information	Information concerning attack targets, including nationality, coordinates, and defense capabilities.
Provide deployment instructions	Give deployment instructions to troops in the field.	Target information	Same as above.

Example Failure of Business Activity	Example Consequences of Failure	Injuries that can Reasonably be Expected	Injury Level
Some troop deployment information is intercepted by hostile forces	Combat forces are at risk of an ambush	Loss of life	Confidentiality = High (Secret)
Inaccurate information or no information concerning a strike against civilian targets is received by combat forces	Combat forces make the wrong decision or are unaware of the strike and are not in a position to protect civilians	Loss of life	Integrity = High Availability = High
Security Category of business activity = (Secret, High Integrity, High Availability)			

7 Candidate Common Security Controls

Table 13 lists the security controls from the Security Control Catalogue in Annex 3 of ITSG-33 [Reference 5] that may be considered for implementation, in whole or in part, as common security controls in organizations. This list is not exhaustive and other security controls may be selected as common security controls (refer to Section 4.2.7.3 for related guidelines).

The profiles in Annex 4 of ITSG-33 [Reference 15] provide additional, suggested common security controls that can be deployed and operated by the departmental IT security function, by IT operations groups, and by various other groups to support departmental information systems (refer to Section 4.3 for related guidelines).

Table 13: Candidate Common Security Controls

ID	Family	Title
Technical Class		
AC-1	Access Control	Access control policy and procedures
AC-2		Account management
AC-17		Remote access
AC-18		Wireless access
AU-1	Audit & Accountability	Audit and accountability policy and procedures
AU-6		Audit review, analysis, and reporting
AU-11		Audit record retention
AU-13		Monitoring for information disclosure
IA-1	Identification & Authentication	Identification and authentication policy and procedures
IA-4		Identifier management
IA-5		Authenticator management
SC-1	System & Communications Protection	System and communications protection policy and procedures
SC-12		Cryptographic key establishment and management
SC-17		Public key infrastructure certificates
Operational Class		
AT-1	Awareness & Training	Security awareness and training policy and procedures
AT-2		Security awareness
AT-3		Security training
AT-4		Security training records
AT-5		Contacts with security groups and associations
CM-1	Configuration Management	Configuration management policy and procedures
CM-2		Baseline configuration

ID	Family	Title
CM-3		Configuration change control
CM-4		Security impact analysis
CM-5		Access restrictions for change
CM-6		Configuration settings
CM-7		Least functionality
CM-8		Information system component inventory
CM-9		Configuration management plan
CP-1	Contingency Planning	Contingency planning policy and procedures
CP-2		Contingency plan
CP-3		Contingency training
CP-4		Plan testing and exercises
CP-6		Alternate storage site
CP-7		Alternate processing site
CP-8		Telecommunications services
CP-9		Information system backup
CP-10		Information system recovery and reconstitution
IR-1	Incident Response	Incident response policy and procedures
IR-2		Incident response training
IR-3		Incident response testing and exercises
IR-4		Incident handling
IR-5		Incident monitoring
IR-6		Incident reporting
IR-7		Incident response assistance
IR-8		Incident response plan
MA-1	Maintenance	System maintenance policy and procedures
MA-2		Controlled maintenance
MA-3		Maintenance tools
MA-4		Non-local maintenance
MA-5		Maintenance personnel
MA-6		Timely maintenance
MP-1	Media Protection	Media protection policy and procedures
PE-1	Physical & Environmental	Physical and environmental protection policy and procedures
PE-2		Physical access authorizations

ID	Family	Title
PE-3		Physical access control
PE-4		Access control for transmission medium
PE-5		Access control for output devices
PE-6		Monitoring physical access
PE-7		Visitor control
PE-8		Access records
PE-9		Power equipment and power cabling
PE-10		Emergency shutoff
PE-11		Emergency power
PE-12		Emergency lighting
PE-13		Fire protection
PE-14		Temperature and humidity controls
PE-15		Water damage protection
PE-16		Delivery and removal
PE-17		Alternate work site
PE-18		Location of information system components
PE-19		Information leakage
PS-1	Personnel Security	Personnel security policy and procedures
PS-2		Position categorization
PS-3		Personnel screening
PS-4		Personnel termination
PS-5		Personnel transfer
PS-6		Access agreements
PS-7		Third-party personnel security
PS-8		Personnel sanctions
SI-1	System & Information Integrity	System and information integrity policy and procedures
SI-2		Flaw remediation
SI-3		Malicious code protection
SI-4		Information system monitoring
SI-5		Security alerts, advisories, and directives
SI-8		Spam protection
Management Class		

ID	Family	Title
CA-1	Security Assessment & Authorization	Security assessment and authorization policies and procedures
CA-2		Security assessments
CA-6		Security authorization
CA-7		Continuous monitoring
PL-1	Planning	Security planning policy and procedures
RA-1	Risk Assessment	Risk assessment policy and procedures
RA-2		Security categorization
RA-3		Risk assessment
RA-5		Vulnerability scanning
SA-1	System & Services Acquisition	System and services acquisition policy and procedures
SA-2		Allocation of resources
SA-3		Life cycle support
SA-4		Acquisitions
SA-9		External information system services

8 References

[Reference 1] Treasury Board of Canada Secretariat. *Operational Security Standard: Management of Information Technology Security (MITS)*. 31 May 2004.

[Reference 2] Communications Security Establishment Canada. *IT Security Risk Management: A Lifecycle Approach – Information System Security Implementation Process*. ITSG-33, Annex 2. 1 November 2012.

[Reference 3] Treasury Board of Canada Secretariat. *Policy on Government Security*. 1 July 2009.

[Reference 4] Communications Security Establishment Canada. *IT Security Risk Management: A Lifecycle Approach – Glossary*. ITSG-33, Annex 5. 1 November 2012.

[Reference 5] Communications Security Establishment Canada. *IT Security Risk Management: A Lifecycle Approach – Security Control Catalogue*. ITSG-33, Annex 3. 1 November 2012.

[Reference 6] Treasury Board of Canada Secretariat. *Framework for the Management of Risk*. 19 August 2010.

[Reference 7] Treasury Board of Canada Secretariat. *Directive on Departmental Security Management*. 1 July 2009.

[Reference 8] International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC). *Information Technology – Security Techniques – Information Security Management Systems – Requirements*. Reference Number ISO/IEC 27001:2005. October 2005.

[Reference 9] International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC). *Information Technology – Security Techniques – Information Security Management Systems – Measurement*. Reference Number ISO/IEC 27004:2009. December 2009.

[Reference 10] Communications Security Establishment Canada. Information Technology Security Guideline (ITSG). *Network Security Zoning: Design Considerations for Placement of Services within Zones*. ITSG-38. May 2009.

[Reference 11] Communications Security Establishment Canada. Information Technology Security Guideline (ITSG). *Baseline Security Requirements for Network Security Zones in the Government of Canada*. ITSG-22. June 2007.

[Reference 12] John Sherwood, Andy Clark, David Lynas. *Enterprise Security Architecture: A Business-Driven Approach*. San Francisco, CMP Books, 2005.

[Reference 13] National Institute of Standards and Technology. Computer Security. *Engineering Principles for Information Technology Security: A Baseline for Achieving Security*. Special Publication 800-27, Revision A. June 2004.

[Reference 14] National Institute of Standards and Technology. *Generally Accepted Principles and Practices for Security Information Technology Systems*. Special Publication 800-14. September 1996.

[Reference 15] Communications Security Establishment Canada. *IT Security Risk Management: A Lifecycle Approach – Security Control Profiles*. ITSG-33, Annex 4. 1 November 2012.

[Reference 16] Treasury Board of Canada Secretariat. Business Transformation Enablement Program (BTEP). *GSRM Service Reference Patterns*. September 2004.

[Reference 17] Communications Security Establishment Canada and the Royal Canadian Mounted Police. *Harmonized Threat and Risk Assessment (TRA) Methodology*. 23 October 2007.