Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Information Technology Security Guidance

IT Security Risk Management: A Lifecycle Approach

Overview

ITSG-33

November 2012

Canada

Foreword

The *Overview* of *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). The Overview and all related Annexes supersede and replace the following CSEC publications:

- Security Risk Management for Information Technology Systems (MG-2)
- A Guide to Certification and Accreditation for Information Technology Systems (MG-4)

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.

Originally signed by

Toni Moffa

Deputy Chief, IT Security

Summary

With today's dynamic threat environment and Government of Canada (GC) fiscal constraints, information technology (IT) security can no longer be an afterthought, but rather needs to be a vital component in both your departmental and IT project plans. With that in mind, the ITSG-33 publication has been developed to help government departments ensure security is considered right from the start. By following the principles within this publication, you not only help ensure predictability and cost-effectiveness, you also help ensure that there are no hidden surprises preventing you from obtaining authority to operate and maintaining continued authorization.

The ITSG-33 publication begins by describing the roles, responsibilities and activities that will help GC departments manage IT security risks. These activities are described both at the program level (to assist Departmental Security Officers and IT Security Coordinators (ITSC) in ensuring alignment with the GC standard on the Management of Information Technology Security (MITS) and other Treasury Board of Canada Secretariat (TBS) Policies and Directives) as well as at the IT project level (for project owner, project managers and security practitioners). The project-based process described is designed to overlay on an existing departmental process. Continuous improvement is a key aspect of the recommended process to ensure that as the threat environment evolves, so do the controls that have been put into place.

To help support these activities, ITSG-33 contains a catalogue of Security Controls structured into three classes of control families: Technical, Operational and Management. Technical security controls are implemented using technology, such as a firewall, while operational security controls are implemented using human processes, such as manual procedures. Management security controls focus on the management of IT security and IT security risks. These three classes of Security Controls together represent a holistic collection of standardized security requirements that should be considered and leveraged when building and operating your IT environments.

As a further aid in developing a baseline set of departmental security controls, ITSG-33 includes several security control profiles. A profile is a collection of Security Controls from each class that have been pre-selected from the catalogue for a particular business environment. Specifically, ITSG-33 includes profiles that address the confidentiality, integrity and availability needs for the GC PROTECTED A, B and SECRET environments. These suggested profiles should be used as a starting-point and then further tailored to meet departmental specific business needs.

Departments that adhere to the ITSG-33 guidelines should reap significant benefits including compliance with the overall risk management strategy and objectives established by TBS, assurance that all aspects of IT security are addressed in an efficient manner, and predictability and cost-effectiveness with regards to IT security risk management.

Revision History

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

Table of Contents

List of Figures

List of Abbreviations and Acronyms

C&A	Certification and Accreditation
CSEC	Communications Security Establishment Canada
DSO	Departmental Security Officer
DSP	Departmental Security Plan
GC	Government of Canada
ISSIP	Information System Security Implementation Process
IT	Information Technology
ITSC	Information Technology Security Coordinator
ITSG	Information Technology Security Guidance
MITS	Management of Information Technology Security
PGS	Policy on Government Security
SDLC	System Development Life Cycle
TBS	Treasury Board of Canada Secretariat
TRA	Threat and Risk Assessment

1 Introduction

1.1 Context

Government of Canada (GC) departments rely on information systems to support their business activities. These interconnected information systems are often subject to serious threats that can have adverse effects on departmental business activities by compromising the confidentiality, integrity, or availability of information systems and their information technology (IT) assets. IT security risk management is one of several components of enterprise risk management that departments need to perform as a routine part of their ongoing operations.

1.2 Purpose

This overview provides a high-level summary of the suite of documents that comprises the ITSG-33 publication. Highlights of the IT security risk management activities that should be undertaken at both the departmental level as well as at the information system level within GC organizations are included. These activities are supported by a comprehensive Security Control Catalogue which should be used by departments to help define common security controls and by projects to help select tailored security controls.

1.3 Target Audience

This overview is intended for GC senior departmental officials and managers at all levels to understand the benefits of ITSG-33. This overview is also useful to IT Security Coordinators (ITSCs) and other departmental security officials, information system practitioners, security practitioners, certification authorities, accreditation authorities, and managers who are collectively responsible for departmental and/or project IT security risk management.

1.4 Definitions and Usage of Terms

For definitions of key terms used in this publication, refer to Annex 5 of ITSG-33 [Reference 2].

1.5 Publication Taxonomy

The ITSG-33 guidelines are provided in a suite of documents as follows:

- ITSG-33, Overview – *IT Security Risk Management: A Lifecycle Approach*
- ITSG-33, Annex 1 – *Departmental IT Security Risk Management Activities*
- 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 Managing IT Security Risks

2.1 Risk Management

In August 2010, Treasury Board of Canada Secretariat (TBS) promulgated a *Framework for the Management of Risk* [Reference 4] for the GC. This framework recognized that failure to effectively manage risks can result in increased program costs and missed opportunities, which can compromise program outcomes, and ultimately public trust.

One of the key principles of effective risk management is that it must be integrated. In the *Framework for the Management of Risk*, TBS defines integrated risk management as:

> *"…a continuous, proactive, and systematic process to understand, manage, and communicate risk from an organization-wide perspective. It is about supporting strategic decision-making that contributes to the achievement of an organization's overall objectives."*

An integrated risk management approach must address the different types of risks that organizations face and may include policy risk, operational risk, human resources risk, financial risk, legal risk, health and safety risk, environmental risk, reputational risk, privacy risk, and ***security risk***.

2.2 Security Risk Management

Security risks stem from the exposure of ***organizational business activities and related assets*** to the compromise of their confidentiality, integrity, availability, intended use, and monetary value by accidental or deliberate threats and natural hazards. Security risk management is the process by which organizations manage those security risks. Assets requiring security protection include people, information, business activities, facilities, office equipment, and ***information systems***.

As required by TBS' *Policy on Government Security* [Reference 3] and *Directive on Departmental Security Management* [Reference 8], the Deputy Head must document how they plan to manage security risks to departmental assets in the Departmental Security Plan (DSP).

2.3 IT Security Risk Management

IT security risks stem from the exposure of IT assets supporting departmental business activities to the compromise of their confidentiality, integrity, availability, and intended use by accidental or deliberate threats and natural hazards. These risks are the subset of the security risks above that could potentially compromise IT assets. IT security risk management is the process by which organizations manage those IT security risks and is achieved through the management and application of security controls, solutions, tools, and techniques to protect IT assets against such compromises.

In applying IT security risk management, departments should aim at striking a proper balance between the implementation of security controls and the levels of acceptable residual risk that they achieve in a manner that aligns with their departmental mission, objectives, and priorities.

As required by TBS' *Directive on Departmental Security Management* [Reference 8], the Deputy Head must also document how they plan to manage IT security risks to departmental IT assets in the Departmental Security Plan (DSP).

2.4 ITSG-33 Purpose and Applicability

Managing IT security risks is a multifaceted undertaking that requires the involvement of an entire department, from the senior officials establishing organizational objectives to individuals developing and operating information systems supporting those organizational objectives. With that in mind, the IT security risk management process documented in ITSG-33 provides a set of activities that can be fully integrated into an existing departmental security program as well as into an IT projects' system development lifecycle. These activities are clearly defined to ensure key steps are performed on an ongoing basis during the lifetime of the information systems, and to ensure risk management is applied from an enterprise perspective. As such, the ITSG-33 process replaces the GC IT security risk management process and the certification and accreditation (C&A) process promulgated in *A Guide to Security Risk Management for Information Technology Systems* (MG-2), and *A Guide to Certification and Accreditation for Information Technology Systems* (MG-4).

It should be noted that the ITSG-33 guidelines do not provide guidance on aspects of an enterprise risk management program beyond those that directly relate to IT security. Readers seeking information concerning other aspects of enterprise risk management should consult TBS's *Framework for the Management of Risk* [Reference 4].

3 IT Security Risk Management Process

The ITSG-33 guidelines suggest a set of activities at two levels within an organization; the departmental level and the information system level.

- Departmental level – Activities to be integrated into the organization's security program to plan, manage, assess and improve the management of IT security-related risks faced by the organization. These activities are described in detail in Annex 1 of ITSG-33 [Reference 5].
- Information System level – Activities to be integrated into an information system lifecycle to ensure IT security needs of supported business activities are met, appropriate security controls are implemented and operating as intended, and continued performance of the implemented security controls is assessed, reported back and acted upon to address any issues. These activities are described in detail in Annex 2 of ITSG-33 [Reference 6].

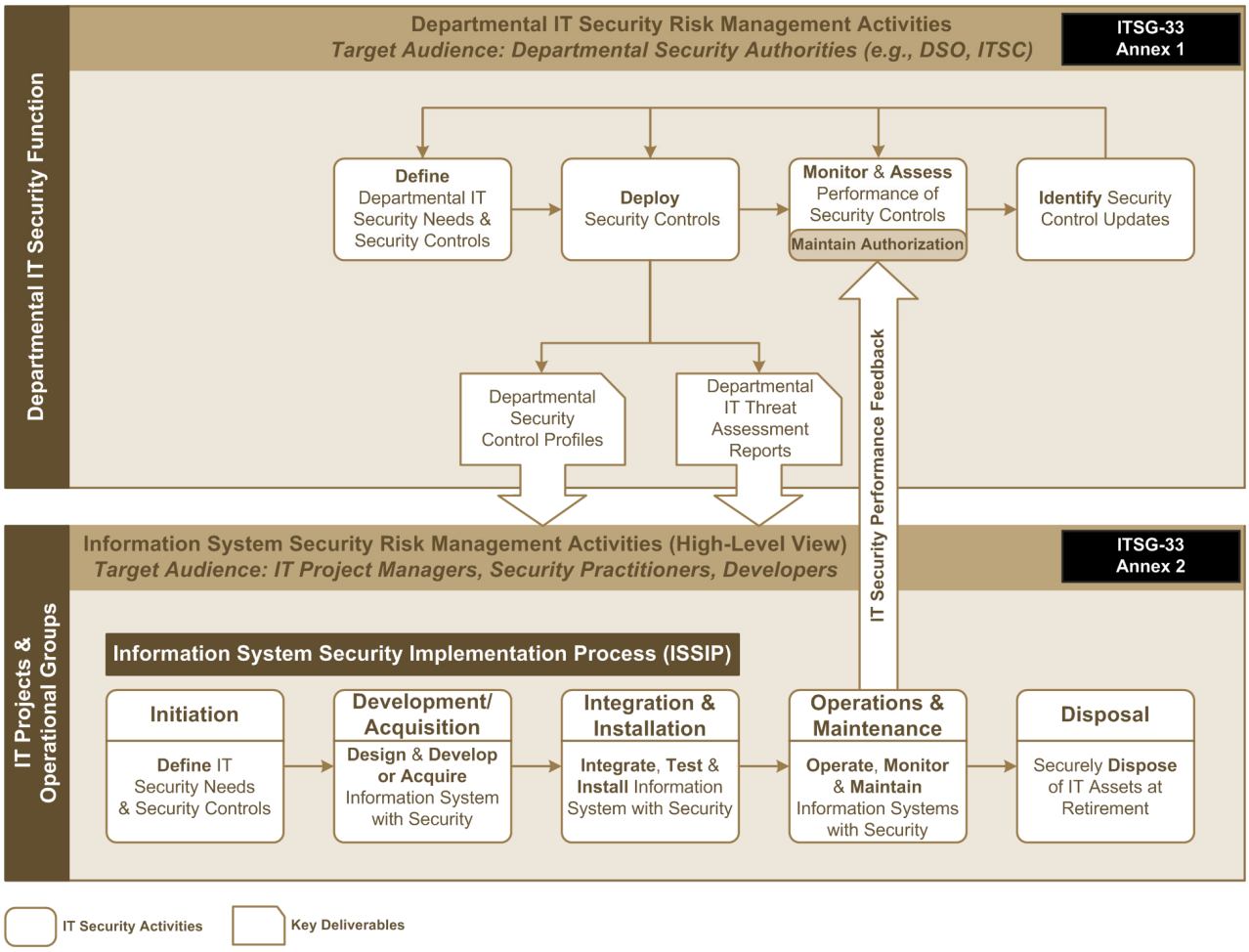

Figure 1: IT Security Risk Management Process

Figure 1 depicts the high-level departmental IT security risk management activities as well as the information system security risk management activities that will be described. It also highlights how the IT security risk management activities at both levels act together in a continuous cycle to efficiently maintain and improve the security posture of departmental information systems.

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 into 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 into 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.

3.1 Departmental IT Security Risk Management Activities

Once overall roles and responsibilities are defined, the guidelines in Annex 1 of ITSG-33 [Reference 5] further suggest and describe IT security risk management activities to define, deploy, monitor, assess the performance of, and update security controls across a department. The execution of these activities follows a standard lifecycle process to be integrated into the overall departmental security program.

The first step in this process is to **define** the business needs for security[1] and the corresponding mandated security controls (see Section 3.3) required to protect the business activities and related information when supported by information systems. This activity includes the identification of common security controls and the identification of the organizational areas responsible for their implementation and delivery. The nature of the business needs for security and security controls for a department depend largely on the type of business activities, their sensitivity and criticality, and the departmental threat environment.

Once defined, these security controls need to be **deployed**. Some controls may be assigned to various groups in the department, such as physical and personnel security. Other controls may leverage already existing infrastructures, such as a common authentication system. In some cases, departments may need to implement common security controls by initiating IT projects (e.g., a new departmental user authentication system or a centralized logging and monitoring infrastructure). For security controls to be implemented in information systems, IT security officials promulgate the use of departmental security control profiles by IT projects (see Section 3.4). In turn, IT projects implement the required security controls in information systems, and IT operations groups operate and maintain them by following the information system risk management activities.

To be effective, the departmental IT security risk management activities need to include steps to **continuously monitor and assess**[2] the performance of the implemented security controls, review the security category of supported business activities, and re-assess relevant threats and technical environments. These activities allow departmental security officials to obtain an ongoing status of the information systems' security posture. Security assessment activities are analogous to quality assurance

[1] Business needs for security are derived from applicable GC legislation, TBS policies, business objectives, and other departmental business and legal requirements. Business needs for security also include privacy-related requirements needing the support of IT security for privacy risk management purposes.

[2] Continuous monitoring and assessment does not necessarily mean real-time assessment. Some monitoring activities (e.g., audit event review) can be performed automatically in real-time, while other assessment activities (e.g., review of system backup procedures) would usually be done manually on a pre-established schedule.

activities in the industrial world. These activities allow departments to react in a timely manner to changes in business, security, threat, and technology environment.

Based on the results of the monitoring and assessment activities, and changes in the environment, departments will then be able to **identify** required updates to appropriately and efficiently respond to new security requirements, new and evolving threats and vulnerabilities, and security incidents. Updates may require changes to business needs for security or the mandated security controls (**define** activity), the deployment of new security controls or changes to implemented security controls (**deploy** activity), and changes in the monitoring and assessment aspects of the IT security function (**monitor and assess** activity). The departmental IT security activities are therefore acting together in a continuous cycle to maintain and efficiently improve the security posture of the departmental information systems.

3.2 Information System Security Risk Management Activities

The guidelines found in Annex 2 of ITSG-33 [Reference 6] suggest IT security risk management activities to implement, operate, and maintain dependable information systems. These activities apply to the life cycle of information systems, which consist of phases for their implementation, operations and maintenance, and disposal. To assist departments, Annex 2 of ITSG-33 [Reference 6] suggests a secure system development lifecycle (SDLC) process referred to as the *information system security implementation process* or the ISSIP.

To apply the ISSIP efficiently and cost-effectively, IT projects need to integrate the ISSIP activities with system engineering, system testing, and other activities of their specific SDLC process. Accordingly, the ISSIP maps the security-related activities to the phases of a reference SDLC process.

The ISSIP begins at the **initiation** phase of the system lifecycle. The first steps are to identify and engage security stakeholders, incorporate the security aspects of the IT project into project planning, and **define** the security controls that must be implemented to adequately protect the information system. The system-specific security controls are derived from mandated security controls defined at the departmental level, based on the sensitivity and criticality of the business activities that the information system will support.

The next steps occur during the **development** or **acquisition** phase. The objective is to **design and develop** or **acquire** information systems with the required security controls. This is achieved by incorporating security controls in system designs, conducting threat and risk assessments, and developing and testing security. If acquiring the information system, security controls need to be included as mandatory requirements in statements of work.

With the development completed, IT projects move into the **integration and installation** phase where it is time to **integrate**, **test**, and **install** information systems with their implemented security controls. At the conclusion of this phase, information systems are attributed authority to operate.

In the **operations and maintenance** phase of the system lifecycle, information systems are now under the control of IT operations groups who **operate**, **monitor**, and **maintain** information systems and their implemented security controls. Continuous monitoring is undertaken as part of this phase to not only ensure that the currently implemented security controls are operating as expected, but to also ensure that as the threat environment changes, security controls are added or modified to meet evolving security needs. If it happens that even after changes to security controls are made during the operations and maintenance phase, it is found that the information system is no longer operating within acceptable levels

of residual risk, authorizers may need to consider revoking 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.

In the **disposal** phase of the system lifecycle, at the end of their useful life, information systems need to be decommissioned and IT operations groups need to securely **dispose** of sensitive IT assets in accordance with established policies, standards, and procedures.

3.3 Security Control Catalogue

Annex 3 of ITSG-33 [Reference 1] includes a catalogue of security controls that departments should leverage to meet their departmental and business security needs and priorities, as well as to comply with TBS policy instruments on IT security and IT security risk management. From a departmental perspective, security practitioners use this catalogue to define common security controls that should be part of the overall departmental security control profile. From an IT project perspective, these same security controls should be used to further refine the departmentally mandated ones to fit the information system's specific security needs.

The security controls in the catalogue are organized at the highest level into three classes and further subdivided into several families (or groupings) of related security controls. The three high level classes are defined as follows:

- ***Management*** class: Includes security controls that focus on the management of IT security and IT security risks;
- ***Technical*** class: Includes security controls that are implemented and executed by information systems primarily through security mechanisms contained in hardware, software, and firmware components; and
- ***Operational*** class: Includes information system security controls that are primarily implemented and executed by people and are typically supported by the use of technology, such as supporting software.

By leveraging these security controls, security practitioners can define security controls that align with their department's business security needs and ensure the adequate implementation of these security controls in departmental information systems.

3.4 Security Control Profiles

Annex 4 of ITSG-33 [Reference 7] includes a series of suggested security control profiles based on the security control catalogue for several different environments. These security control profiles are a suggested selection of security controls and control enhancements that departmental security authorities can use as a starting point to create department-specific security control profiles. These profiles, when properly implemented, must be suitable for protecting the confidentiality, integrity, and availability of departmental IT assets against threats that could cause injury to business activities. Given that, the suggested security control profiles constitute a starting point only and need to be tailored to meet the specific business, technical and threat contexts, as well as the risk tolerance of the department.

The selection of security controls, for each profile in Annex 4 of ITSG-33 [Reference 7], was based on industry and governmental security best practices, under certain threat assumptions, and derived from CSEC's analysis of the threat environment faced by information systems in the documented business context. They have been created as a tool to assist security practitioners in their efforts to protect information systems in compliance with applicable GC legislation and TBS policies, directives, and standards. Departmental security control profiles are used by the IT security function to implement and coordinate the deployment of common security controls across the 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 the project to protect the information system that they are implementing or updating.

4 Value to Departments

By adhering to the process defined within the set of ITSG-33 publications, departments will reap many benefits such as:

1. Consistently and cost-effectively managing IT security risks;
2. Consistently and cost-effectively delivering dependable information systems by increasing the maturity of IT projects in the implementation of security in information systems;
3. The ability to address all aspects of IT security in an efficient manner to satisfy department-wide business needs for security by applying a holistic approach across the organization in a consistent and reproducible way;
4. The ability to address stakeholder requirements by ensuring that the requirements of business owners (i.e., authorizers), and those of the security assessors that support them, are taken into account at the department level during the development of threat assessments and security control requirements, and during the implementation of information systems;
5. Improving communications among all security stakeholders by using standard terminology for IT security activities and security control requirements;
6. Improvement in transparency of security and risk management-related information by promoting the sharing of threat information and security control requirements among the departmental IT and IT security communities;
7. Improving the risk management decision making process when departments interconnect their information systems through the use of standardized, easily comparable departmental security control requirements and security assessment results; and
8. Compliance with the overall risk management strategy and objectives established by TBS through implementing key requirements of TBS policy instruments on IT security and IT security risk management.

5 References

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

[Reference 2] Communications Security Establishment Canada. *IT Security Risk Management: A Lifecycle Approach – Glossary*. ITSG-33, Annex 5. 1 November 2012.

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

[Reference 4] Treasury Board of Canada Secretariat. *Framework for the Management of Risk*. 19 August 2010.

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

[Reference 6] Communications Security Establishment Canada. *IT Security Risk Management: A Lifecycle Approach – Information System Security Risk Management Activities*. ITSG-33, Annex 2. 1 November 2012.

[Reference 7] Communications Security Establishment Canada. *IT Security Risk Management: A Lifecycle Approach – Security Control Profiles*. ITSG-33, Annex 4. 1 November 2012.

[Reference 8] Treasury Board of Canada Secretariat. *Directive on Departmental Security Management*. 1 July 2009.