Communications Security Establishment | Centre de la sécurité des télécommunications

Information Technology Security Guidance

IT Security Risk Management: A Lifecycle Approach

Information System Security Risk Management Activities

ITSG-33 – Annex 2

November 2012

Canada

Foreword

Annex 2 (*Information System 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 (CSE).

Suggestions for amendments should be forwarded through departmental communications security channels to your Information Technology (IT) Security Client Services Representative at CSE.

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

For further information, please contact CSE'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

This Annex is part of a series of guidelines on information technology (IT) security risk management that the Communications Security Establishment (CSE) 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 suggests an information system security implementation process (ISSIP). The goal of ISSIP is to help IT projects implement security solutions in information systems that satisfy the security objectives of confidentiality, integrity, and availability of the departmental business activities that information systems support. For the purposes of this Annex, an IT project is defined as a temporary endeavour undertaken to implement a new information system, or to implement significant changes to an existing information system. It implies that each IT project ends when the new information system has been implemented or has been altered and an IT operations organization has assumed operational responsibility.

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

Table of Contents

List of Figures

List of Tables

List of Abbreviations and Acronyms

BNS	Business Needs for Security
CM	Configuration Management
COMSEC	Communications Security
COTS	Commercial-off-the-Shelf
CSE	Communications Security Establishment
DDSM	Directive on Departmental Security Management
DS	Design Specifications
DSP	Departmental Security Plan
DT	Development Tools
FIPS	Federal Information Processing Standard
GC	Government of Canada
GOTS	Government-off-the-Shelf
IATF	Information Assurance Technical Framework
IEC	International Electrotechnical Commission
IPC	Information Protection Centre
ISO	International Organization for Standardization
ISSIP	Information System Security Implementation Process
IT	Information Technology
ITSG	Information Technology Security Guidance
MOU	Memorandum of Understanding
NATO	North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OpenSSL	Open Secure Sockets Layer
OSP	Operational Security Procedures
PGS	Policy on Government Security
PWGSC	Public Works and Government Services Canada
RAD	Rapid Application Development
RCMP	Royal Canadian Mounted Police
RFC	Request for Change
RFP	Request for Proposal
SAL	Security Assurance Level
SCS	Security Control Specification

SDLC	System Development Lifecycle
SDP	Secure Development Practices
SIP	Security Installation Procedures
SIV	Security Installation Verification
SLA	Service Level Agreement
SLC	System Lifecycle
SM	Security Measures
SPIN	Security Policy Implementation Notice
SQL	Structured Query Language
SRCL	Security Requirements Checklist
SRTM	Security Requirements Traceability Matrix
SSC	Shared Services Canada
SSE-CMM	System Security Engineering-Capability Maturity Model
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Testing
TA	Threat Assessment
TBD	To Be Determined
TBS	Treasury Board of Canada Secretariat
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TRA	Threat and Risk Assessment
URL	Uniform Resource Locator
VA	Vulnerability Assessment

1 Introduction

1.1 Purpose and Scope

This Annex provides guidelines to Government of Canada (GC) departments[1] on the efficient and cost-effective implementation of security in information systems in a manner consistent with policies, standards, and guidelines promulgated by Treasury Board of Canada Secretariat (TBS). This Annex addresses activities at the information system level of the information technology (IT) security risk management process that the ITSG-33 guidelines suggest to departments.

This Annex suggests an information system security implementation process (ISSIP) for GC IT projects. The goal of ISSIP is to help IT projects implement security solutions in information systems that satisfy the security objectives of confidentiality, integrity, and availability of the departmental business activities that information systems support. For the purposes of this Annex, an IT project is defined as a temporary endeavour undertaken to implement a new information system, or to implement significant changes to an existing information system. It implies that each IT project ends when the new information system has been implemented or has been altered and an IT operations organization has assumed operational responsibility.

While not the prime focus of this Annex, general guidance is also provided on additional information system security risk management activities that follow the implementation of information systems, which consists of the secure operations and maintenance of information systems, and the secure disposal of IT assets when information systems are retired.

1.2 Applicability

The guidelines in this publication apply to the implementation of security in information systems used to support departmental business activities in the unclassified, protected, and classified domains. Departments can use ISSIP:

- For the development of new departmental information systems and GC shared and common IT infrastructures;
- When making significant changes to existing information systems and GC shared and common IT infrastructures; and
- When acquiring external information system capabilities to be used either as standalone IT services or as capabilities to be integrated in GC information systems.

An IT project is acquiring an external capability when it plans to leverage a capability offered by another information system or IT infrastructure than the one being implemented by the project. The capability provider can be another organization within the sponsoring department, another department (e.g., Shared Services Canada (SSC) as the GC common service provider), or a commercial service provider.

For existing information systems and GC common and shared IT infrastructures, the definition of what constitutes a change is subject to interpretation. In most cases, changes within information systems require

[1] The term *departments* is used to mean GC departments, agencies, and other organizations subject to the *Policy on Government Security* [Reference 3].

authorization and some level of security assessment regardless of how significant they are. However, departmental authorities normally determine on a case-by-case basis whether the changes being proposed can be handled by their IT operations organization through established operational procedures (e.g., change management procedures addressing security concerns) or if they are significant enough to warrant the establishment of an IT project.

ISSIP is a comprehensive process and is described in detail in this publication. It is expected that departments with more mature IT project management and engineering capabilities can easily adapt and integrate the ISSIP process into their own SDLC process. IT projects with less mature capabilities will not be able to apply all facets of ISSIP immediately and more tailoring of the process will be required. These IT projects can use this publication as a reference to gradually improve their security engineering practices over time to deliver more dependable information systems.

1.3 Objectives and Expected Results

The objective of this Annex is to help departments implement and operate dependable, fit-for-purpose information systems in a manner that satisfies the objectives and requirements of TBS's *Policy on Government Security* (PGS) [Reference 3], *Directive on Departmental Security Management* (DDSM) [Reference 4], and *Standard on the Management of Information Technology Security* [Reference 5].

By following the guidelines in this Annex, IT projects can achieve the following results:

- Implement or acquire information systems or capabilities that satisfy the security needs of departmental business activities;
- Implement information systems robust enough to resist selected threats[2] in the operational environment at acceptable levels of risk; and
- Provide to stakeholders a realistic view of the risks that supported departmental business activities are exposed to as a result of their reliance on information systems.

1.4 Audience

This Annex is aimed at participants in the various phases of information system implementation projects. More specifically, it provides guidance to authorizers, project managers, security architects, security practitioners, security assessors, and members of IT operations groups.

[2] From all the potential threats, departments may specify a subset against which it wishes to protect its IT assets. 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 significantly a business activity's supporting functionality. Threat information, including decisions and justification for excluding specific threats, would normally be documented in departmental threat assessment reports. See Annex 1 of ITSG-33 [Reference 1] for information.

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 1 – *Departmental IT Security Risk Management Activities*
- ITSG-33, Annex 3 – *Security Control Catalogue*
- ITSG-33, Annex 4 – *Security Control Profiles*
- ITSG-33, Annex 5 – *Glossary*

1.7 Definitions

For definitions of key terms used in this Annex, refer to Annex 5 of ITSG-33 [Reference 11].

2 ISSIP Overview

2.1 General Approach

ISSIP is a comprehensive process consisting of a structured set of activities for implementing security in information systems. It incorporates activities to address information system security engineering[3], threat and risk assessment, security assessment, and authorization. Figure 1 on the following page shows an overview of ISSIP.

To apply ISSIP efficiently and cost-effectively, IT projects need to integrate ISSIP activities with system engineering, system testing, and other activities of their specific SDLC process. To assist projects with this integration, ISSIP maps the security-related activities to the phases of a reference SDLC process that follows a typical waterfall model. For example, ISSIP suggests integrating the security requirements analysis activity within the broader system requirements analysis activities. The same is recommended for design, testing, quality assurance, and any other pertinent activities. Note that ISSIP does not contain all the required activities of an IT project; only those pertaining to IT security are shown.

IT project managers can adapt ISSIP to other SDLC methodologies, which may use lightweight processes such as Agile and other rapid application development (RAD) methodologies. Guidance on adapting ISSIP activities to other SDLC methodologies such as these is beyond the scope of the ITSG-33 publications.

As shown in Figure 1, the reference SDLC model consists of the following phases:

- **Stakeholder engagement** – Identify and engage the stakeholders for the IT project;
- **Concept** – Define a concept for the information system;
- **Planning** – Plan the implementation of the information system;
- **Requirements analysis** – Define the requirements that the information system needs to implement in order to satisfy the business objectives;
- **High-level design** – Create a high-level system design that satisfies the information system's requirements;
- **Detailed design** – Specify a detailed design of the high-level system design;
- **Development** – Develop or procure and test the individual components of the information system;
- **Integration and testing** – Integrate the individual components into a complete system and conduct integration testing; and
- **Installation** – Install the information system in the production environment.

[3] ISSIP incorporates the applicable process areas of ISO/IEC's *System Security Engineering – Capability Maturity Model* (SSE-CMM) [Reference 6].

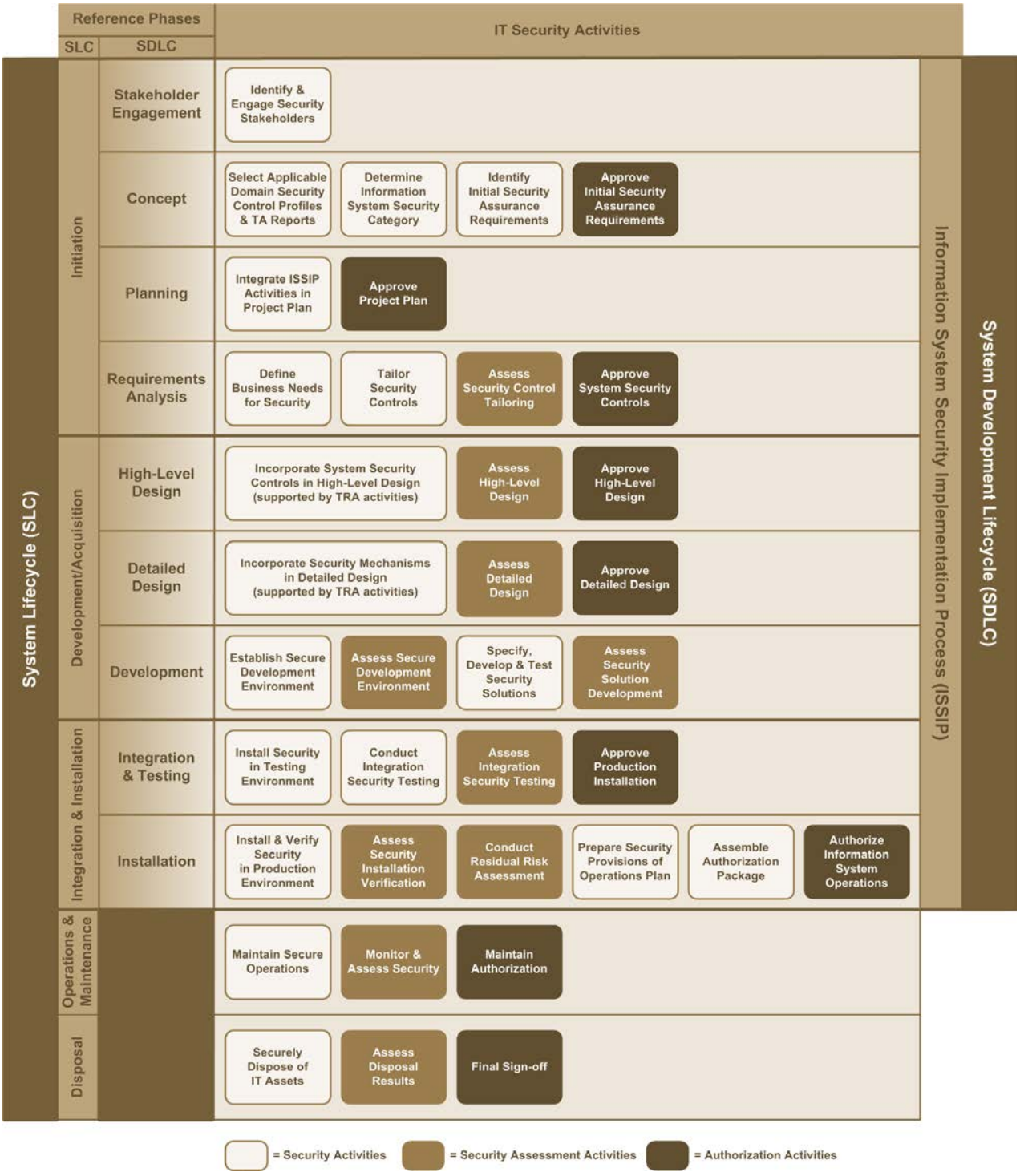


Figure 1: ISSIP Overview

Figure 1 includes two additional phases beyond those of the SDLC to show a complete system lifecycle (SLC):

- **Operations and maintenance** – An IT operations group operates and maintains the information system until its end of life; and
- **Disposal** – Upon retirement of the information system at the end of its life, the IT operations group disposes of or reassigns IT assets.

This description of the reference SDLC is generic and addresses all aspects of IT, such as performance, reliability, usability, and security. In a typical SDLC, these aspects are taken into account at each phase, in an integrated manner, such that requirements analysis takes into account requirements from all IT aspects, design activities seek to satisfy the requirements from all IT aspects, and so on. For efficiency purposes, the various IT aspects are not managed independently. The same is true of the security aspects of information systems. The activities that relate to security are integrated within the typical SDLC activities and performed in an integrated manner. This yields a more efficient process and provides greater assurance that the security aspects will be taken into account adequately.

The progression from security objectives to implemented security solutions in the information system consists of several stages of increasingly detailed security specifications that include business needs for security (e.g., ensure that information concerning business transactions is not disclosed to unauthorized parties), system security controls (e.g., transmission confidentiality), security mechanisms (e.g., Transport Layer Security (TLS) session encryption), and finally the security solutions within the information system (e.g., OpenSSL Version 3) that are then installed within the information system environment.

Note that the operations and maintenance phase and the disposal phase are not strictly part of the SDLC but are shown to highlight the important linkages between the secure implementation of information systems and their secure operations, maintenance, and disposal. Guidance is provided on these phases in sections 4 and 5.

2.2 Benefits of Using the ISSIP

By following the guidelines in this Annex, departments can:

- Comply with key IT security and IT security risk management instruments promulgated by TBS;
- Leverage a comprehensive approach to address IT security concerns with respect to the implementation and operation of information systems; and
- Consistently and cost-effectively deliver dependable information systems that meet departmental business objectives and security needs.

2.3 Authorization Conditions

Before starting an IT project, the project manager should get from the departmental security plan (DSP) the list of conditions required to be satisfied, as a minimum, to obtain the authorization to operate for an information system and maintain it during operations. If these conditions are not documented in the DSP, then the project manager should get them from the designated authorizer. The project manager should document the list of conditions in a project charter or the project plan. The charter or the plan should then

be signed by the authorizer, the IT project sponsor (if different), the IT project manager, and any other relevant stakeholders such as the information system operational authority.

Within the context of ISSIP, examples of authorization conditions could include:

- The IT project needs to use a specific departmental or domain security control profile;
- ISSIP activities need to be appropriately tailored and incorporated in the IT project plan;
- ISSIP outputs need to be provided to the security assessor and the authorizer for assessment and approval in accordance with the ISSIP assessment and approval activities;
- An agreed-upon authorization package needs to be assembled and delivered to the authorizer for authorization before commencing operations;
- An operations plan that includes security provisions needs to be produced and executed by the IT operations group; and
- The acceptable level of residual risk for the information system is low.

3 ISSIP Process Description

This chapter describes ISSIP activities corresponding to the nine phases of the reference SDLC. Each following subsection describes a phase of the reference SDLC and contains one or more subsections, each describing the ISSIP activities that are completed during that phase. Throughout this section, ISSIP outputs are identified using the appropriate subsection number (corresponding to the related activity that generates it) and letter identifiers.

ISSIP activities are described in a standard structure consisting of the following elements:

- **Objective** – The objective of the ISSIP activity;
- **Primary role** – The role that is responsible for completing the activity;
- **Supporting roles** – Roles supporting the primary roles to successfully complete the activity;
- **Inputs** – The activity's inputs;
- **Outputs** – The activity's outputs;
- **Security assurance requirements** – The identifiers and titles of the security assurance requirements that apply to the activity (Security assurance requirements are described in Section 8); and
- **Guidelines** – Guidelines on how to complete the activity.

Although ISSIP activities are described sequentially in this Annex, no process is completely linear and there may be several instances during an IT project where the team will have to go back to a previous activity and even a previous phase to complete or redo part of an analysis and refine definitions and specifications. Also note that ISSIP does not preclude the requirement for standard SDLC checkpoints and management approvals such as critical design reviews and quality gates.

Table 1 summarizes the process by listing all ISSIP activities and indicating their inputs and outputs. The outputs listed in the last column of Table 1 represent ISSIP work products and do not necessarily equate to individual deliverables or documents. To minimize documentation, IT projects should incorporate to the maximum extent possible ISSIP outputs in standard SDLC deliverables (e.g., security requirements in system requirements specifications, security designs in system design documents), as determined during the planning phase. To that end, Table 2 lists all ISSIP work products and suggests SDLC deliverables in which they could be integrated.

Table 3 provides suggestions for the assignment of ISSIP activities to primary and supporting roles. The responsibilities of these roles as they relate to ISSIP are described in Annex 1 of ITSG-33 [Reference 1].

Table 1: ISSIP Activities and Inputs and Outputs

Subsections	Activities	Inputs	Outputs
3.1	**Stakeholder Engagement Phase**		
3.1.1	Identify and engage security stakeholders	ITSG-33, Annex 2 – *Information System Security Risk Management Activities* [this publication] Available project documentation	(3.1.1-A) List of security stakeholders
3.2	**Concept Phase**		
3.2.1	Select applicable domain security control profiles and threat assessment reports	Available project documentation Available domain security control profiles Available domain threat assessment reports	(3.2.1-A) Applicable domain security control profile(s) (3.2.1-B) Applicable domain threat assessment report(s)
3.2.2	Determine information system security category	ITSG-33, Annex 1, Section 7 – *Security Categorization Process* [Reference 1] (3.2.1-A) Applicable domain security control profile	(3.2.2-A) Information system security categorization report
3.2.3	Identify initial security assurance requirements	ITSG-33, Annex 2, Section 8 – *Security Assurance Requirements* [this publication] (3.2.1-A) Applicable domain security control profile (3.2.1-B) Applicable domain threat assessment report (3.2.2-A) Information system security categorization report	(3.2.3-A) Initial security assurance requirements
3.2.4	Approve initial security assurance requirements	(3.2.3-A) Initial security assurance requirements	(3.2.4-A) Approved initial security assurance requirements
3.3	**Planning Phase**		
3.3.1	Integrate ISSIP activities in project plan	Project plan ITSG-33, Annex 2 – *Information System Security Risk Management Activities* [this publication] (3.1.1-A) List of security stakeholders (3.2.4-A) Approved initial security assurance requirements	(3.3.1-A) Project plan with ISSIP activities
3.3.2	Approve project plan	(3.3.1-A) Project plan with ISSIP activities	(3.3.2-A) Approved project plan with ISSIP activities

Subsections	Activities	Inputs	Outputs
3.4	**Requirements Analysis Phase**		
3.4.1	Define business needs for security	System documentation from the concept phase (3.2.1-A) Applicable domain security control profile (3.2.2-A) Information system security categorization report (3.2.4-A) Approved initial security assurance requirements	(3.4.1-A) Business needs for security
3.4.2	Tailor security controls	ITSG-33, Annex 3 – *Security Control Catalogue* [Reference 7] System documentation from the concept phase (3.2.1-A) Applicable domain security control profile (3.2.2-A) Information system security categorization report (3.2.4-A) Approved initial security assurance requirements (3.4.1-A) Business needs for security	(3.4.2-A) System security controls
3.4.3	Assess security control tailoring	(3.2.1-A) Applicable domain security control profile (3.2.4-A) Approved initial security assurance requirements (3.4.1-A) Business needs for security (3.4.2-A) System security controls	(3.4.3-A) Statement of assessment for security control tailoring
3.4.4	Approve system security controls	(3.4.2-A) System security controls (3.4.3-A) Statement of assessment for security control tailoring	(3.4.4-A) Approved system security controls

Subsections	Activities	Inputs	Outputs
3.5	**High-Level Design Phase**		
3.5.1	Incorporate system security controls in high-level design (supported by TRA activities)	ITSG-33, Annex 3 – *Security Control Catalogue* [Reference 7] ITSG-33, Annex 2, Section 7 – *Determining a Robustness Level* [this publication] ITSG security control design publications (3.2.1-B) Applicable domain threat assessment report (3.2.2-A) Information system security categorization report (3.2.4-A) Approved initial security assurance requirements (3.4.4-A) Approved system security controls	(3.5.1-A) High-level system design specifications with security controls (3.5.1-B) Revised system security controls (3.5.1-C) Results of TRA activities
3.5.2	Assess high-level design	(3.2.4-A) Approved initial security assurance requirements (3.5.1-A) High-level system design specifications with security controls (3.5.1-B) Revised system security controls (3.5.1-C) Results of TRA activities	(3.5.2-A) Statement of assessment for the high level system design
3.5.3	Approve high-level design	(3.5.1-A) High-level system design specifications with security controls (3.5.2-A) Statement of assessment for high-level system design	(3.5.3-A) Approved high-level system design specifications with security controls

Subsections	Activities	Inputs	Outputs
3.6	**Detailed Design Phase**		
3.6.1	Incorporate security mechanisms in detailed design (supported by TRA activities)	ITSG-33, Annex 3 – *Security Control Catalogue* [Reference 7] ITSG-33, Annex 2, Section 7 – *Determining a Robustness Level* [this publication] ITSG security control design publications Government and industry technical security standards and best practices (3.2.2-A) Information system security categorization report (3.2.4-A) Approved initial security assurance requirements (3.5.1-B) Revised system security controls (3.5.1-C) Results of TRA activities (3.5.3-A) Approved high-level system design specifications with security controls	(3.6.1-A) Detailed system design specifications with security mechanisms (3.6.1-B) Final system security controls (3.6.1-C) Updated security assurance requirements (3.6.1-D) Results of TRA activities
3.6.2	Assess detailed design	(3.6.1-A) Detailed system design specifications with security mechanisms (3.6.1-B) Final system security controls (3.6.1-C) Updated security assurance requirements (3.6.1-D) Results of TRA activities	(3.6.2-A) Statement of assessment for the detailed system design
3.6.3	Approve detailed design and development	(3.6.1-A) Detailed system design specifications with security mechanisms (3.6.2-A) Statement of assessment for detailed system design	(3.6.3-A) Approved detailed system design specifications with security mechanisms (3.6.3-B) Approval to proceed with development
3.7	**Development Phase**		
3.7.1	Establish secure development environment	(3.6.1-C) Updated security assurance requirements (3.6.3-A) Approved detailed system design specifications with security mechanisms (3.6.3-B) Approval to proceed with development	(3.7.1-A) Secure development environment (3.7.1-B) Development environment documentation

Subsections	Activities	Inputs	Outputs
3.7.2	Assess secure development environment	(3.6.1-C) Updated security assurance requirements (3.7.1-A) Secure development environment (3.7.1-B) Development environment documentation	(3.7.2-A) Statement of assessment for the secure development environment
3.7.3	Specify, develop, and test security solutions	Technology-specific security configuration standards and best practices (3.6.1-C) Updated security assurance requirements (3.6.3-A) Approved detailed system design specifications with security mechanisms (3.7.1-A) Secure development environment (3.7.1-B) Development environment documentation	(3.7.3-A) Information system implementation representation with security (3.7.3-B) Development security testing plans, test cases, and results (3.7.3-C) Operational security procedures (3.7.3-D) Security installation procedures
3.7.4	Assess security solution development	(3.6.1-C) Updated security assurance requirements (3.7.3-A) Information system implementation representation with security (3.7.3-B) Development security testing plans, test cases, and results (3.7.3-C) Operational security procedures (3.7.3-D) Security installation procedures	(3.7.4-A) Statement of assessment for security development
3.8	**Integration and Testing Phase**		
3.8.1	Install security in information system testing environment	(3.7.3-A) Information system implementation representation with security	(3.8.1-A) Information system testing environment with security
3.8.2	Conduct integration security testing	(3.6.1-C) Updated security assurance requirements (3.7.3-A) Information system implementation representation with security (3.8.1-A) Information system testing environment with security	(3.8.2-A) Integration security testing plans, test cases, and results

Subsections	Activities	Inputs	Outputs
3.8.3	Assess integration security testing	(3.6.1-C) Updated security assurance requirements (3.8.1-A) Information system testing environment with security (3.8.2-A) Integration security testing plans, test cases, and results	(3.8.3-A) Statement of assessment for integration security testing
3.8.4	Approve production installation	(3.7.2-A) Statement of assessment for the secure development environment (3.7.4-A)Statement of assessment for security development (3.8.3-A) Statement of assessment for integration security testing	(3.8.4-A) Approval to proceed with production installation
3.9	**Installation Phase**		
3.9.1	Install and verify security in information system production environment	(3.6.1-C) Updated security assurance requirements (3.7.3-A) Information system implementation representation with security (3.8.4-A) Approval to proceed with production installation	(3.9.1-A) Information system production environment with security (3.9.1-B) Security installation verification results
3.9.2	Assess security installation verification	(3.6.1-C) Updated security assurance requirements (3.7.3-A) Information system implementation representation with security (3.9.1-A) Information system production environment with security (3.9.1-B) Security installation verification results	(3.9.2-A) Statement of assessment for security installation verification
3.9.3	Conduct residual risk assessment	All previous ISSIP outputs	(3.9.3-A) Residual risk assessment results
3.9.4	Prepare security provisions for operations plan	All previous ISSIP outputs	(3.9.4-A) Security provisions for operations plan
3.9.5	Assemble authorization package	All previous ISSIP outputs	(3.9.5-A) Authorization package
3.9.6	Authorize information system operations	(3.9.5-A) Authorization package	(3.9.6-A) Authorization to operate

Table 2: Suggested Integration of ISSIP Outputs in IT Project Deliverables

ISSIP Output IDs	ISSIP Outputs	Suggested IT Project Deliverables
3.1.1-A	List of security stakeholders	Project charter
3.2.1-A	Applicable domain security control profile(s)	Not applicable as this is a deliverable from departmental IT security risk management activities
3.2.1-B	Applicable domain threat assessment report(s)	Not applicable as this is a deliverable from departmental IT security risk management activities
3.2.2-A	Information system security categorization report	Not applicable as this is a standalone document
3.2.3-A	Initial security assurance requirements	• Quality assurance plan • Project schedule
3.2.4-A	Approved initial security assurance requirements	
3.6.1-C	Updated security assurance requirements	
3.3.1-A	Project plan with ISSIP activities	Project plan
3.3.2-A	Approved project plan with ISSIP activities	
3.4.1-A	Validated business needs for security	• System requirements definition • Requirements traceability matrix
3.4.2-A	System security controls	
3.4.4-A	Approved system security controls	
3.5.1-B	Revised system security controls	
3.6.1-B	Final system security controls	
3.4.3-A	Statement of assessment for security control tailoring	Requirements analysis gate review report
3.5.1-A	High-level system design specifications with security controls	High level system design specifications
3.5.3-A	Approved high-level system design specifications with security controls	
3.5.1-C	Results of TRA activities (from high level design phase)	• High level system design specifications • TRA report (if required)
3.5.2-A	Statement of assessment for the high level system design	High-level design gate review report
3.6.1-A	Detailed system design specifications with security mechanisms	Detailed system design specifications
3.6.3-A	Approved detailed system design specifications with security mechanisms	
3.6.1-D	Results of TRA activities (from detailed design phase)	• Detailed system design specifications • TRA report (if required)

ISSIP Output IDs	ISSIP Outputs	Suggested IT Project Deliverables
3.6.2-A	Statement of assessment for detailed design	Detailed design gate review report
3.6.3-B	Approval to proceed with development	
3.7.1-A	Secure development environment	Not applicable
3.7.1-B	Development environment documentation	Development environment documentation
3.7.3-A	Information system implementation representation with security	Information system implementation representation
3.7.3-B	Development security testing plans, test cases, and results	System testing documentation
3.8.2-A	Integration security testing plans, test cases, and results	
3.7.3-C	Operational security procedures	Operational procedures
3.7.3-D	Security installation procedures	System installation procedures
3.7.2-A	Statement of assessment for the secure development environment	System development gate review report
3.7.4-A	Statement of assessment for security development	
3.8.1-A	Information system testing environment with security	Not applicable
3.8.3-A	Statement of assessment for integration security testing	System testing gate review report
3.8.4-A	Approval to proceed with production installation	
3.9.1-A	Information system production environment with security	Not applicable
3.9.1-B	Security installation verification results	Quality assurance final review report
3.9.3-A	Residual risk assessment results	• Residual risk assessment report • TRA report (if required)
3.9.4-A	Security provisions for operations plan	Operations plan
3.9.5-A	Authorization package	Authorization package
3.9.2-A	Statement of assessment for security installation verification	Final gate review report
3.9.6-A	Authorization to operate	

Table 3: Suggested Assignment of ISSIP Activities to Roles

Sub-sections	ISSIP Activities	Roles (P=Primary role, S=Supporting role)													
		Authorizer	Project Manager	Business Analyst	(Departmental) Security Architect	System Designer	System Developer	Departmental Security Officer	System Integrator	System Tester	IT Security Coordinator	Security Practitioner	(External) Security Assessor	System Administrator	IT Operations Personnel
3.1	**Stakeholder Engagement Phase**														
3.1.1	Identify and engage security stakeholders	S	P												
3.2	**Concept Phase**														
3.2.1	Select applicable domain security control profiles and TA reports	S	S	S								P			
3.2.2	Determine information system security category			S								P			
3.2.3	Identify initial security assurance requirements											P			
3.2.4	Approve initial security assurance requirements	P	S		S							S			
3.3	**Planning Phase**														
3.3.1	Integrate ISSIP activities in project plan		P									S			
3.3.2	Approve project plan	P	S					S			S				
3.4	**Requirements Analysis Phase**														
3.4.1	Define business needs for security			S	S							P			
3.4.2	Tailor security controls											P			
3.4.3	Assess security control tailoring											S	P		
3.4.4	Approve system security controls	P											S		
3.5	**High-Level Design Phase**														
3.5.1	Incorporate system security controls in high-level design (supported by TRA activities)					P			S			S			
3.5.2	Assess high-level design											S	P		
3.5.3	Approve high-level design	P											S		

Sub-sections	ISSIP Activities	Roles (P=Primary role, S=Supporting role)													
		Authorizer	Project Manager	Business Analyst	(Departmental) Security Architect	System Designer	System Developer	Departmental Security Officer	System Integrator	System Tester	IT Security Coordinator	Security Practitioner	(External) Security Assessor	System Administrator	IT Operations Personnel
3.6	**Detailed Design Phase**														
3.6.1	Incorporate security mechanisms in detailed design (supported by TRA activities)					**P**			**S**			**S**			
3.6.2	Assess detailed design											**S**	**P**		
3.6.3	Approve detailed design and development	**P**											**S**		
3.7	**Development Phase**														
3.7.1	Establish secure development environment						**P**					**S**			
3.7.2	Assess secure development environment											**S**	**P**		
3.7.3	Specify, develop, and test security solutions						**P**		**S**	**S**		**S**			
3.7.4	Assess security solution development											**S**	**P**		
3.8	**Integration and testing Phase**														
3.8.1	Install security in information system testing environment								**P**			**S**			
3.8.2	Conduct integration security testing								**S**	**P**		**S**			
3.8.3	Assess integration security testing											**S**	**P**		
3.8.4	Approve production installation	**P**											**S**		
3.9	**Installation Phase**														
3.9.1	Install and verify security in information system production environment											**S**		**P**	
3.9.2	Assess security installation verification											**S**	**P**	**S**	
3.9.3	Conduct residual risk assessment											**S**	**P**		
3.9.4	Prepare security provisions of operations plan											**P**	**S**		**S**
3.9.5	Assemble authorization package											**P**	**S**		
3.9.6	Authorize information system operations	**P**	**S**										**S**		

3.1 Stakeholder Engagement Phase

This subsection describes the ISSIP activity of the stakeholder engagement phase of the SDLC, which are part of the initiation phase of the SLC.

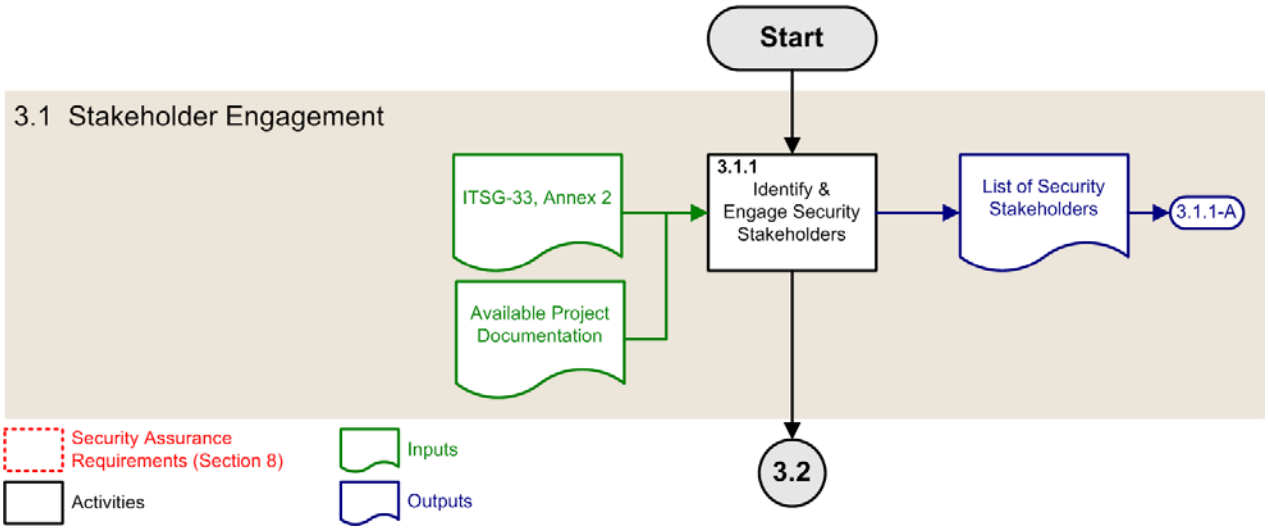


Figure 2: ISSIP Activity of the Stakeholder Engagement Phase

3.1.1 Identify and Engage Security Stakeholders

Objectives:	Identify and engage the security stakeholders of the IT project
Primary role:	Project manager
Supporting roles:	Authorizer
Inputs:	ITSG-33, Annex 2 – *Information System Security Risk Management Activities* [this publication] Available project documentation
Outputs:	(3.1.1-A) List of security stakeholders
Security assurance requirements:	No specific requirements

Guidelines:

ISSIP relies on the participation of senior departmental officials to obtain appropriate funding and resources at the beginning of the process, review and approve key ISSIP outputs during the process, and authorize information system operations at the end of the process. ISSIP therefore begins at the initiation

phase of an IT project to ensure that security stakeholders are identified and made aware of ISSIP requirements from the onset.

The key security stakeholder is the program and service delivery manager who will be relying on the information system for their program or service delivery. This program and service delivery manager may be the authorizer[4] (or someone higher-up the chain of command, refer to Annex 1 of ITSG-33, Section 5.13 [Reference 1]). The authorizer's role is to authorize the use of the information system to support organizational objectives. By means of this authorization, the authorizer assumes responsibility for relying on the information system and therefore accepts the risks associated with doing so.

Another security stakeholder to consider is the departmental enterprise security architect, whose role is to develop security architectures and standards and promulgate their adoption within the organization. Some departments may have an enterprise security architect on staff. The function may also be the responsibility of a senior manager, such as a chief information officer or a chief technology officer, or an organizational unit.

In addition to the authorizer and the enterprise security architect, IT projects may require an external security assessor such as a certification authority to participate in ISSIP activities. Some departments have appointed a certification authority to conduct security assessment activities in support of authorization. When this is the case, the IT project should obtain the certification authority's commitment at this phase, and determine exactly which of the security assessment activities they intend to conduct. Finally, IT projects require support from the IT operational authority to ensure that the information system is appropriately integrated within existing departmental IT operations.

[4] The authorizer is sometimes called the *accreditation authority* in the context of an IT project.

3.2 Concept Phase

This subsection describes the ISSIP activities of the concept phase of the SDLC, which is part of the initiation phase of the SLC.

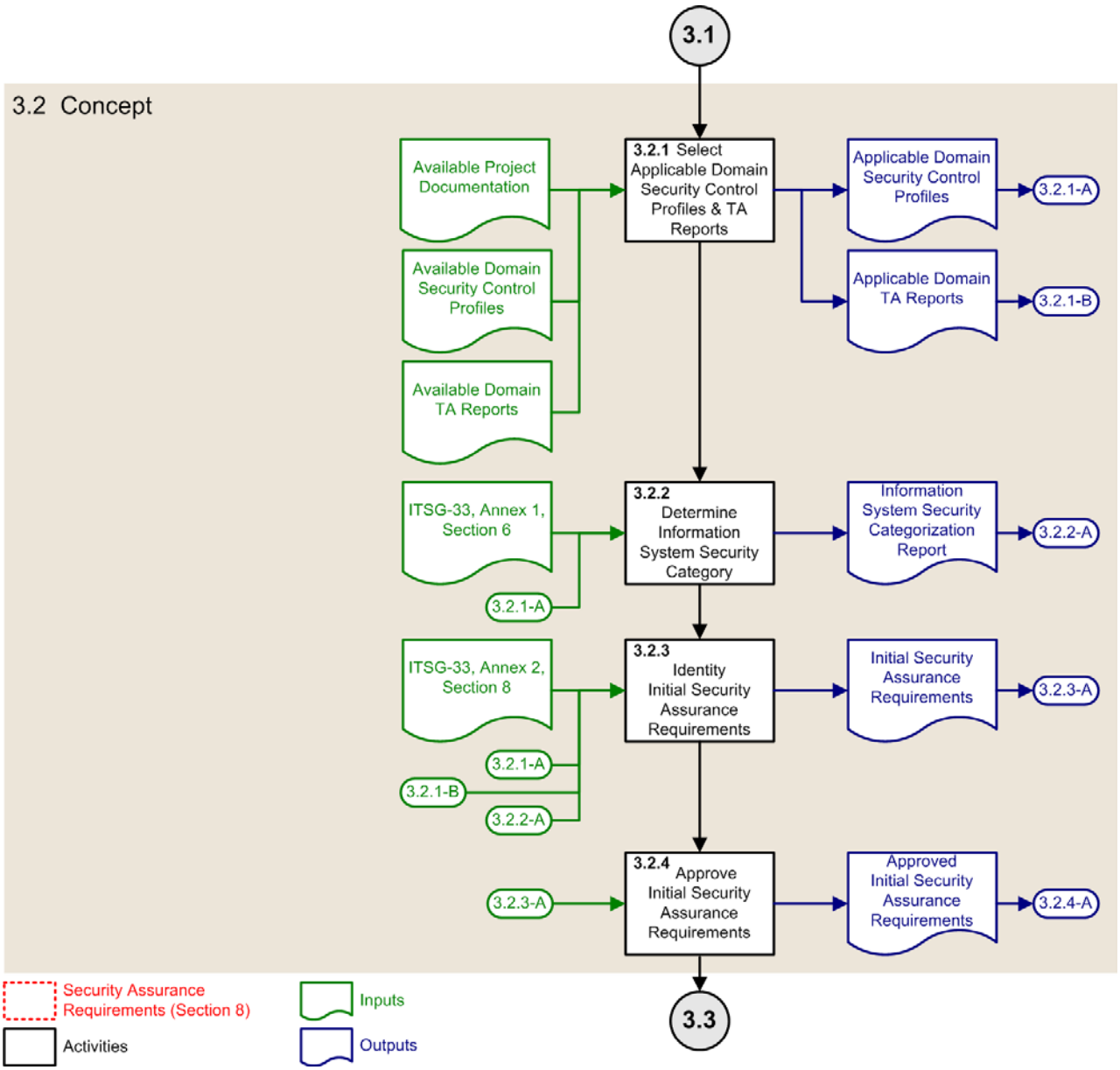


Figure 3: ISSIP Activities of the Concept Phase

Early on in the implementation process, IT projects select domain security control profiles (or a departmental security control profile if no domain profiles exist) that applies to the business activities that the information system will support, and determine a suitable security category for the information system. The results of these key activities allow for the specification, commensurate with the sensitivity and criticality of business activities and the significance of the threats against them, of an initial set of security assurance requirements, which gives IT project authorities the ability to adequately plan for the IT security aspects of their project.

3.2.1 Select Applicable Domain Security Control Profiles and TA Reports

Objectives:	Select the domain security control profiles (or departmental security control profiles if no domain profiles exist) that applies to the business activities that the information system will support, and the threat assessment reports that relates to those domains and profiles.
Primary role:	Security practitioner
Supporting roles:	Business analyst, authorizer, IT project manager
Inputs:	Available project documentation Available domain security control profiles Available domain threat assessment reports
Outputs:	(3.2.1-A) Applicable domain security control profiles (3.2.1-B) Applicable domain threat assessment reports
Security assurance requirements:	No specific requirements

Guidelines:

Domain security control profiles recommend the implementation of a set of security controls to protect defined business activities against selected threats. It is therefore important for security practitioners to select the correct domain security control profiles and related threat assessment reports to establish a suitable basis for tailoring and implementing security controls for their information system. The consolidation of applicable security controls is done as part of the security control tailoring process (as described in Section 3.4.2).

Depending on the nature of their programs and services, departments may have a single departmental security control profile or several domain security control profiles. The term domain security control profile is used in this publication.

Departmental security authorities or the authorizer may mandate the use of one or more specific domain security control profiles for the IT project. Otherwise, security practitioners have to either select applicable profiles from available ones, or develop one specifically for the business activities that their information system will support if none is available or applicable. The guidelines for developing domain security control profiles are provided in Annex 1 of ITSG-33 [Reference 1].

When profiles are mandated or selected, security practitioners have to validate that the profiles apply to the business activities that the information system will support, and to the technical and threat contexts of the IT project.

In the case where only one domain security control profile is selected by an IT project, it is still necessary to validate the business, technical and threat assumptions documented in the profile to ensure that it apply to the context of the IT project.

Note: To simplify the text in the reminder of this publication, the case of one applicable domain security control profile for an IT project will be used.

When selecting security control profiles, security practitioners perform the following tasks:

- Validate the applicability of the business context;
- Validate the applicability of the technical context;
- Validate the applicability of the threat context; and
- Validate the applicability of IT security approaches.

3.2.1.1 Validate the Applicability of the Business Context

Near the beginning of the IT project, it is useful for security practitioners to understand the context of the project and the business activities that the information system will support, and validate those with the business context of the selected domain security control profile. To perform that validation, there are several IT project deliverables that, although outside the scope of ISSIP, are helpful in this regard.

For example, a project charter is a good source of information that can help security practitioners validate the business context as it typically identifies the essential components of a project, in particular its purpose, goals, scope, business objectives, project risks, and assumptions.

Security practitioners can also leverage project documentation defining project-specific requirements (e.g., business, legal, privacy, etc.).

The following example serves to illustrate the business context validation process:

> A security practitioner is considering the use of a domain security control profile that was developed for a business context where there are financial activities involving Protected B information. From the IT project's perspective, the goal is to implement an additional user interface to a legacy financial system that processes Protected B information. Because the project's information system will support business activities that fall within the scope of the profile's business context, the security practitioner concludes that the business context of the profile under consideration is applicable.

3.2.1.2 Validate the Applicability of the Technical Context

The second step in validating a domain security control profile is to validate that the technical context and assumptions identified in the profile apply to the technical context of the IT project.

> Continuing with the example in Section 3.2.1.1, the security practitioner determines that the profile's technical context is applicable to financial systems used by a small number of internal employees working in the same building. From the IT project's perspective, the technical objective is to expand user access to a large number of employees working across Canada, and to some preferred partners in the banking industry. Because the profile under consideration was developed for a different technical context, the security practitioner concludes that, to be suitable, the profile under consideration would require tailoring.

3.2.1.3 Validate the Applicability of the Threat Context

The third step in validating a domain security control profile is to validate that the threats identified in the threat context section of the profile, and further defined in the domain threat assessment report associated with the profile (if one exists), applies to the business activities that the information system will support.

> Continuing with the example in Section 3.2.1.1, the security practitioner determines that the profile was developed to address unsophisticated threats because the technical context assumed that any supporting information systems would not be directly connected to external networks, which meant that the domain's business activities would not be exposed to sophisticated external adversaries. From the IT project's perspective, one of the objectives is to link the legacy financial system to a site in a foreign country for a temporary special event, which means that the profile under consideration was developed for a different threat context. The security practitioner therefore concludes that, to be suitable, the profile under consideration would require significant tailoring.

3.2.1.4 Validate the Applicability of IT Security Approaches

The fourth step in validating a domain security control profile is to validate that the IT security approaches documented in the profile are compatible with the IT project's objectives.

> Continuing with the example in Section 3.2.1.1, the security practitioner determines that the profile's IT security approaches include the establishment of a strong network perimeter around information system components to lessen the need for internal security controls, thus reducing complexity and limiting costs. From the IT project's perspective, one of the objectives is to link a large number of clients to the financial system through the new centralized interface, thus allowing the use of a strong perimeter approach. Because the project will apply IT security approaches that fall within the scope of the profile's IT security approaches, the security practitioner concludes that the IT security approaches of the profile under consideration is applicable.

3.2.2 Determine Information System Security Category

Objectives:	Determine the security category of the information system based on the business activities (i.e., business processes and related information) that it will support
Primary role:	Security practitioner
Supporting roles:	Business analyst
Inputs:	ITSG-33, Annex 1, Section 6 – *Security Categorization Process* [Reference 1] (3.2.1-A) Applicable domain security control profile
Outputs:	(3.2.2-A) Information system security categorization report
Security assurance requirements:	No specific requirements

Guidelines:

In the previous activity (Section 3.2.1), domain security control profiles have been validated as applicable to the IT project. These profiles have been developed to be applicable to specific types of business activities (including related information assets). The security category of these business activities[5] are documented in the profiles and usually included in the name of the profile (e.g., *Profile for Business Reporting Activities of Security Category Protected A, Low Integrity, Low Availability*).

In this activity, the IT project needs to specify a security category for the information system to be implemented. This security category means that the information system is being implemented and operated to satisfy security objectives.

It is recommended that an information system inherits the security category of the business activities that it supports as documented in the validated profiles. This simply means that the information system is being implemented and operated to meet the security needs of the business activities.

In the case of one applicable profile, the security category of the information system should be the same as the security category of the business activities documented in the profile. If several domain security control profiles apply, it is recommended that the security category of the information system reflect the highest category of all applicable profiles (i.e., high-water mark) to ensure that the information system will be able to satisfy the security objectives of all supported business activities.

[5] As described in Annex 1 of ITSG-33 [Reference 1], the security category of a business activity is established by determining the level of injuries that could reasonably be expected if the confidentiality, integrity, and availability of supporting IT assets are compromised. For example, if the compromise of the availability of an information system supporting a business activity servicing citizens is expected to cause medium level injuries to these citizens, then that business activity's security category is medium for availability. The same process applies to confidentiality and integrity.

For example:

Business Activity	**Business Activity Security Category**		
	Confidentiality	**Integrity**	**Availability**
Sensor Data Analysis	Unclassified	**Medium**	Low
Business Reporting	**Protected A**	Low	Low
Information System Category	**Protected A**	**Medium**	**Low**

If the IT project decides to select a different security category for the information system using a different method than suggested above (e.g., to reduce cost), the authorizer must approve that decision and accept the risks.

See Annex 1 of ITSG-33 [Reference 1] for more information on domain security control profiles and the security categorization of business activities.

3.2.3 Identify Initial Security Assurance Requirements

Objectives:	Identify the initial security assurance requirements prescribed for the information system
Primary role:	Security practitioner
Supporting roles:	None
Inputs:	ITSG-33, Annex 2, Section 8 – *Security Assurance Requirements* [this publication] (3.2.1-A) Applicable domain security control profile (3.2.1-B) Applicable domain threat assessment report (3.2.2-A) Information system security categorization report
Outputs:	(3.2.3-A) Initial security assurance requirements
Security assurance requirements:	No specific requirements

Guidelines:

Security assurance requirements specify security-related tasks that IT projects are to complete throughout the ISSIP to increase confidence in the adequacy of their security work. Generally speaking, each security assurance requirement is composed of engineering tasks (i.e., the engineering work and documentation to complete), documentation content requirements (i.e., the content and evidence to include in engineering task outputs), and assessment tasks (i.e., the evaluation work required to assess the engineering tasks and their outputs).

The guidelines in this Annex indicate where in ISSIP activities security assurance requirements come into play. The actual security assurance requirements (engineering tasks, documentation content requirements, and assessment tasks) are defined in Section 8.

In normal circumstances, the applicable security control profile will specify appropriate security assurance requirements that can serve as the initial set for the IT project. Otherwise, security practitioners can follow the process below:

1) Using the information system's security category, which is documented in the information system security categorization report (Section 3.2.2), identify the highest level of injury of all three objectives of confidentiality, integrity, and availability. For example, if the information system's security category is (Protected B, Medium integrity, High availability), then the highest injury level is high. If the security category is (Protected B, Low integrity, Low availability), then the highest injury level is medium.

2) Using the threat information contained in the applicable domain security control profile and the associated domain threat assessment report (if one is available) or departmental threat assessment report, determine the highest category of threat agent capabilities (deliberate threats) and magnitude of event (accidental and natural threats) by following the process described in Section 7.4.2.

3) Using Table 7 and the guidelines in Section 7.4.3 as a guide, identify the robustness level corresponding to the highest injury level determined in Step 1, and the highest threat category determined in Step 2. The corresponding level represents the maximum overall system robustness level[6]. This is the robustness level with the view of the system as a black box, and generally represents the level required in the implementation of critical security controls. This does not mean that all security controls within the system will be implemented at this level. The determination of security control-specific robustness level is done during the design analysis phases.

4) Using Table 4 in Section 7.3, identify the security assurance level (SAL) corresponding to the initial robustness level.

5) Using Table 9 in Section 8.3, identify the initial set of security assurance requirements.

Note that this process will yield the most stringent security assurance level required by the project. This level will be adjusted later in the design phases to ensure the right balance between security assurance and cost effectiveness. IT projects need to have some knowledge of security assurance requirements at this early stage in order to support project planning. These security assurance requirements are adjusted later, during the design phases, in response to more specific, security control-related robustness requirements.

[6] Refer to Section 7 for more details on robustness.

3.2.4 Approve Initial Security Assurance Requirements

Objectives:	Obtain the approval to proceed with the project planning phase on basis of the initial security assurance requirements
Primary role:	Authorizer
Supporting roles:	Departmental architect or departmental security architect, project manager, security practitioner
Inputs:	(3.2.3-A) Initial security assurance requirements
Outputs:	(3.2.4-A) Approved initial security assurance requirements
Security assurance requirements:	No specific requirements

Guidelines:

Before proceeding with the planning phase, IT projects should review with the authorizer the ISSIP outputs from the concept phase and obtain the authorizer's approval of the initial security assurance requirements. Concept phase ISSIP outputs establish the level of effort for system security engineering and security assessment activities for the entire project and are therefore important factors in determining project costs and timeline.

IT projects should schedule this activity as part of the project gating activities for the concept phase of their SDLC.

When reviewing ISSIP outputs from the concept phase, authorizers should consider:

- Reviewing with departmental security officials and a departmental architect or departmental security architect (for departments that have one) the security approaches defined in the applicable domain security control profile to understand their impact on project complexity and team member requirements in terms of knowledge, skills, and experience;
- Reviewing with the security practitioner the selected information system security category to ensure that the business activities have been correctly identified and that appropriate security category levels have been selected for the information system's confidentiality, integrity, and availability; and
- Reviewing with the project manager and the security practitioner the selection of the initial security assurance requirements to understand their impact on project costs, resources, and timeline.

3.3 Planning Phase

This subsection describes the ISSIP activities of the planning phase of the SDLC, which are part of the initiation phase of the SLC.

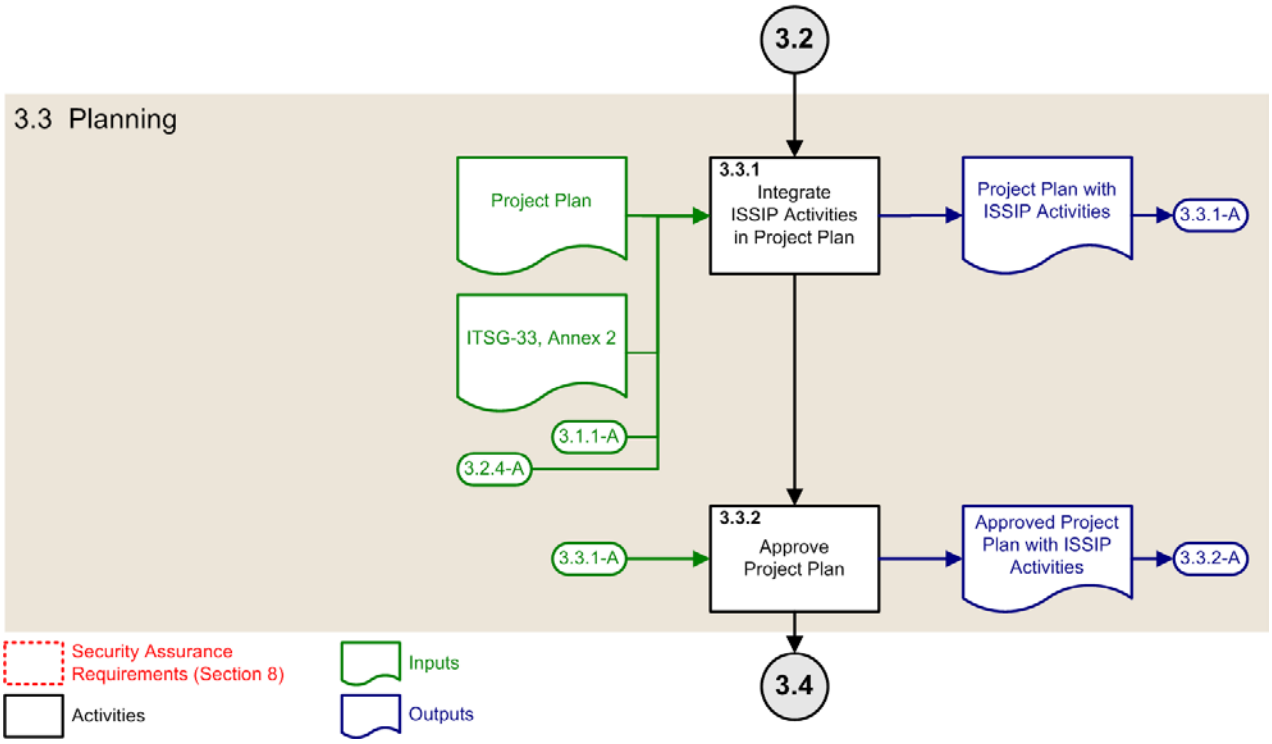


Figure 4: ISSIP Activities of the Planning Phase

3.3.1 Integrate ISSIP Activities in Project Plan

Objectives:	Plan the security aspects of the project
Primary role:	Project manager
Supporting roles:	Security practitioner
Inputs:	Project plan ITSG-33, Annex 2 – *Information System Security Risk Management Activities* [this publication] (3.1.1-A) List of security stakeholders (which determines, in part, project tasking) (3.2.4.-A) Approved initial security assurance requirements
Outputs:	(3.3.1-A) Project plan with ISSIP activities
Security assurance requirements:	No specific requirements

Guidelines:

For best results, IT projects should integrate ISSIP activities in the project plan instead of using a separate plan.

In a typical IT project, the project manager, with the assistance of security practitioners and the participation of the authorizer, would tailor the ISSIP to fit the project's goal (e.g., implement new system versus implement changes or enhancements) and complexity (e.g., implementing a web site, deploying technical infrastructure, building a custom financial or military application). IT projects would also adapt ISSIP based on the availability of deliverables issued from departmental processes (e.g., domain security control profiles). In projects where there is no applicable domain security control profile available, IT projects will have to include additional activities to develop one. If such is the case, project authorities should seek the participation of their IT security coordinator and the appropriate business community.

IT projects need to assess security-related costs as part of the overall project costing to establish sufficient funding. There are several aspects of information system security implementation for IT projects to consider when assessing project costs:

- The nature of the business activities that will be supported by the information system (e.g., simple public web site versus military command and control) and the information system's security category (e.g., Protected B versus classified system);
- The nature of the technical environment and the type and complexity of the overall security strategy as defined by the security approaches described in the applicable domain security control profile (e.g., single-purpose, closed information system not connected to any external networks versus highly distributed information system servicing various types of user communities with a focus on distributed application security);

- The security assurance requirements and their impact on the level of effort for system security engineering, security assessment, documentation, and the establishment and management of the development environment; and
- The availability of an applicable domain security control profile and domain threat assessment report. IT projects that fail to locate an applicable domain security control profile and domain threat assessment report may have to rely on a departmental security control profile and a departmental threat assessment report, and in some cases develop a domain security control profile. This may increase the level of effort to define and tailor security controls and conduct threat and risk assessment (TRA) activities.

It is important to note that security under-funding will most likely result in the implementation of less-secure information systems and leave authorizers in a situation where they have to accept greater residual risks.

See Table 3 for recommended assignment of ISSIP activities to roles and Annex 1 of ITSG-33 [Reference 1] for guidelines on roles and responsibilities.

3.3.2 Approve Project Plan

Objectives:	Obtain the approval to proceed with the project according to the project plan
Primary role:	Authorizer
Supporting roles:	Project manager, departmental security officer, IT security coordinator
Inputs:	(3.3.1-A) Project plan with ISSIP activities
Outputs:	(3.3.2-A) Approved project plan with ISSIP activities
Security assurance requirements:	No specific requirements

Guidelines:

The main purpose of this activity is to obtain the approval of the authorizer to proceed with the IT project as per the project plan. From this point onward, any changes to the planned security activities may increase project costs, impact timeline, reduce assurance in the information system's security posture, and lead to higher levels of residual risks.

3.4 Requirements Analysis Phase

This subsection describes the ISSIP activities of the requirements analysis phase of the SDLC, which are part of the initiation phase of the SLC.

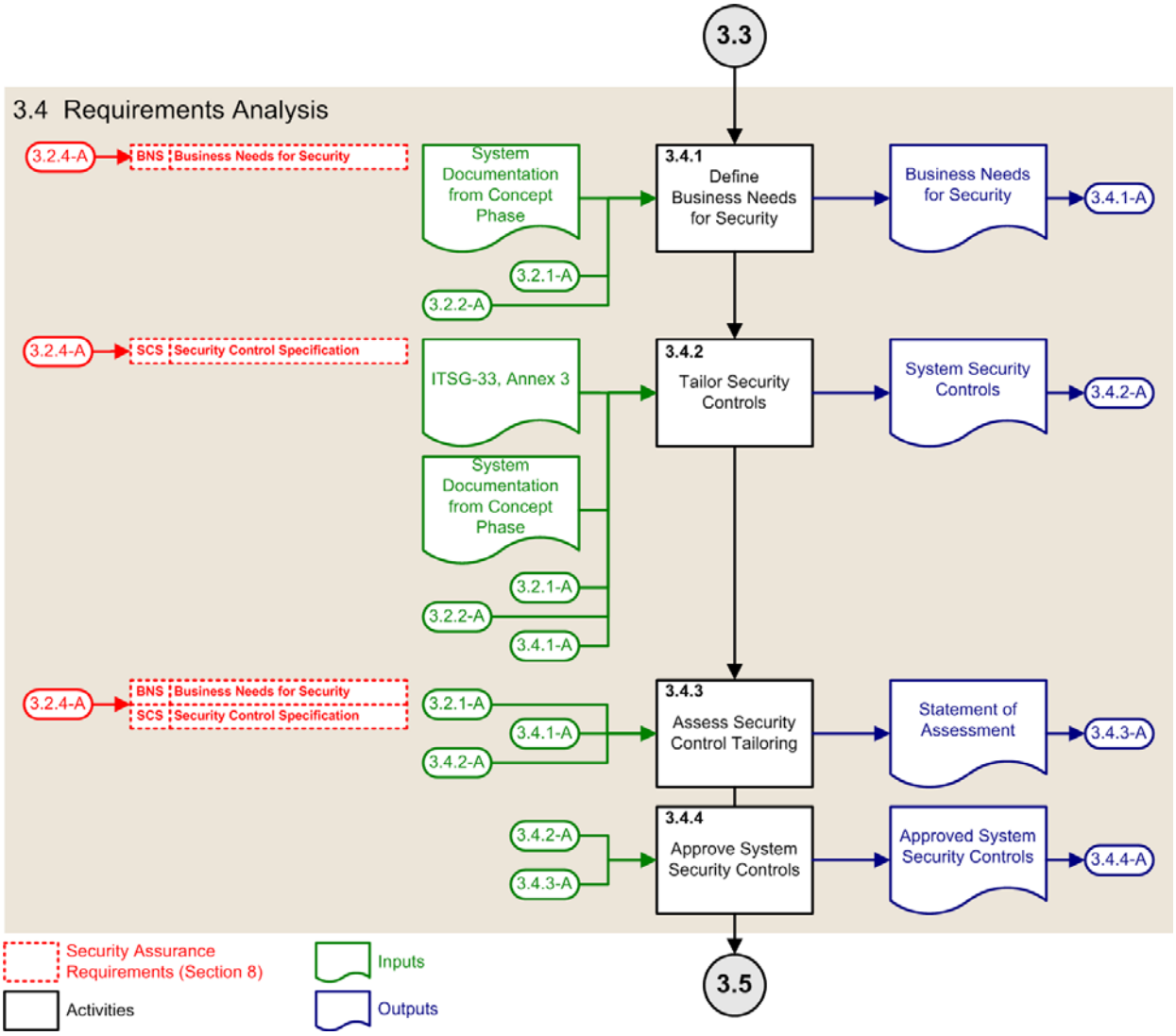


Figure 5: ISSIP Activities of the Requirements Analysis Phase

3.4.1 Define Business Needs for Security

Objectives:	Define the business needs for security that the information system needs to satisfy
Primary role:	Security practitioner
Supporting roles:	Business analyst, departmental architect or departmental security architect
Inputs:	System documentation from concept phase (e.g., concept of operations) (3.2.1-A) Applicable domain security control profile (3.2.2-A) Information system security categorization report
Outputs:	(3.4.1-A) Business needs for security
Security assurance requirements:	(3.2.4.-A) Security assurance engineering tasks and documentation content requirements for business needs for security (Section 8, BNS-E and BNS-D)

Guidelines:

The business needs for security represent the authorizer's, business owner's, and other stakeholder's security requirements. As such, they define in business terms what each business activity's business processes and related information require in terms of protection to satisfy the business-related security objectives of confidentiality, integrity, and availability. They are derived from laws, regulations, policies, directives, standards, contractual obligations, and objectives that govern business activities. When supporting business activities, information systems need to satisfy the confidentiality, integrity, and availability needs of business activities through the implementation of appropriate IT security controls.

Business needs for security should be defined in whole or in part in the applicable domain security control profile. Security practitioners extract these already defined business needs for security, compare them against project documentation to confirm their applicability to the IT project, and to identify and define any additional needs that are not documented in the profile.

IT projects should define business needs for security with the assistance of a knowledgeable business analyst. IT projects should also seek the collaboration of a departmental architect or departmental security architect (person or group, if one exists), who should be in tune with business security needs and equipped to help bridge the gap between those requirements and the information system that the IT project will eventually develop or update.

Refer to Annex 1 of ITSG-33 [Reference 1] for more information on business needs for security and domain security control profiles.

3.4.2 Tailor Security Controls

Objectives:	Tailor the security controls to satisfy the system-specific requirements, as defined by the applicable domain security control profile, the information system security category, and the business needs for security. Refine the description of system-specific security controls to ensure that they are written in an unambiguous manner that will clearly inform system designers and security practitioners doing the future design work, and to ensure that precise security requirements are included in any required request for proposal (RFP) when outsourcing some aspects of the implementation work.
Primary role:	Security practitioner
Supporting roles:	None
Inputs:	ITSG-33, Annex 3 – *Security Control Catalogue* [Reference 7] System documentation from concept phase (e.g., concept of operations) (3.2.1-A) Applicable domain security control profile (3.2.2-A) Information system security categorization report (3.4.1-A) Business needs for security
Outputs:	(3.4.2-A) System security controls
Security assurance requirements:	(3.2.4-A) Security assurance engineering tasks and documentation content requirements for security control specification (Section 8, SCS-E and SCS-D)

Guidelines:

The main input of this activity is a domain security control profile. This profile documents the set of departmentally mandated security controls applicable to the IT project. Security controls are defined in Annex 3 of ITSG-33 [Reference 7]. Each security control is composed of basic functional security requirements and any number of enhancements that increase the protection afforded by the basic function.

The security control tailoring process can be summarized as follows:

1) Select from the applicable security control profile the security controls and enhancements that apply to the information system. As described in Annex 1 of ITSG-33 [Reference 1], the profile should provide guidance on the appropriate owners for the implementation and operations of security controls.

2) If required, tailor the security controls and enhancements to satisfy the information system's business needs for security.

3) Rationalize the security controls and enhancements to optimize the tailoring. Document the justification for additions and removals of security controls and enhancements for the security assessor and authorizer.

4) Refine the security control definitions to ensure that they are written in an unambiguous manner that will clearly inform the security practitioners doing the future design work.

Through tailoring, security practitioners specify undefined security control parameters, select additional security controls and control enhancements, and remove unnecessary or non-applicable security controls and control enhancements. Security practitioners should document their justification for all additions and removals to inform the security assessor and authorizer of the rationale for doing so.

When tailoring security controls for a specific information system, security practitioners should review the applicable domain security control profile and reference material to ensure that there are no new or additional requirements that have not been captured in the profile. When doing so, security practitioners should consider the following:

- Organizational policies, standards, and procedures that relate to the business activities;
- The regulatory instruments, contractual requirements, and departmental security requirements applicable specifically to the IT project;
- Departmental IT and IT security standards such as those defined in enterprise architecture artefacts, which may contain technology-related requirements and constraints; and
- The threat environment defined in the domain threat assessment report.

Security practitioners can also tailor security controls based on risk-related information that may be available at this stage (e.g., a significant threat that has recently resulted in a compromise of an existing departmental information system, a known vulnerability that equally affects all departmental systems).

The output of the tailoring process at this point is a set of system-specific security controls, which will be subjected to further tailoring and refinement later in the ISSIP, as part of the system and security design process and supporting TRA activities.

3.4.2.1 Security Requirements Traceability Matrix (SRTM)

One way for IT projects to meet many of the security assurance requirements is to use a security requirements traceability matrix or SRTM. The SRTM is a suitable tool when security assurance requirements call for tracing the correspondence between an information system's requirements and design specifications.

Through the SRTM, the IT project can satisfy the security assurance objective of ensuring that a security control specification forms a clear, unambiguous, and well-defined description of applicable security controls.

Within the ISSIP, IT projects can use the SRTM as follows:

- During the business needs for security validation process (Section 3.4.1), to document business needs for security and trace their correspondence with the departmental objectives that they satisfy (Section 8.4.1);
- During the security control tailoring process (Section 3.4.2), to document system security controls and trace their correspondence to the business needs for security and other applicable high-level requirements that they satisfy (Section 8.4.2);
- During the high-level design process (Section 3.5.1), to trace design specifications to their corresponding system security controls (Section 8.4.3), and to trace system security controls to the threats that they counter (Section 8.4.4);

- During the detailed design process (Section 3.6.1), to trace security mechanisms to their corresponding system security controls (Section 8.4.3), and to trace system security mechanisms to the threats that they counter (Section 8.4.4); and
- When developing test cases during the information system development process (Section 3.7.3), to trace test cases to security mechanisms (Section 8.4.9).

The SRTM can be integrated in the project's broader requirements traceability matrix if deemed appropriate.

3.4.3 Assess Security Control Tailoring

Objectives:	Confirm that the security control tailoring process was completed in conformance with the security assurance requirements
Primary role:	Security assessor
Supporting roles:	Security practitioner
Inputs:	(3.2.1-A) Applicable domain security control profile (3.4.1-A) Business needs for security (3.4.2-A) System security controls
Outputs:	(3.4.3-A) Statement of assessment for security control tailoring
Security assurance requirements:	(3.2.4-A) Security assurance assessment tasks for business needs for security and security control specification (Section 8, BNS-A and SCS-A)

Guidelines:

With assistance from the security practitioner, the security assessor should perform the following tasks:

- Confirm that the business needs for security definition satisfies the engineering tasks and the documentation content requirements;
- Confirm that the security control tailoring work satisfies the engineering tasks and documentation content requirements; and
- Prepare a statement of assessment for approval.

The term *statement of assessment* is used to mean any recognition or acknowledgement that the assessment process has been completed with acceptable results. It can be as simple as a record of decision appearing in the minutes of an engineering or project meeting or as formal as an assessment certificate signed by a security assessor.

Important note about assessment and approval activities:

While the ISSIP's security assessment and approval activities are shown as being performed at the end of their respective phase, in practice security assessors should actively participate in the execution of ISSIP activities, review ISSIP outputs as they are produced, and immediately advise authorizers of security issues and how they affect security objectives and risk. By doing so, security assessors can ensure that IT projects resolve security issues as they are identified by requesting corrections to ISSIP outputs, additional work from the project team (e.g., redo part of the security testing), or any other corrective activities, instead of waiting at the end of a phase to do so and face schedule delays, additional project costs, and unacceptable risks.

However, there may be situations where a specific security issue cannot be resolved. When such is the case, security assessors should immediately inform their authorizer, advise them of the potential impact on security objectives and risk, and obtain approval to proceed with the project with or without implementing compensating measures. Finally, security assessors should document unresolved security issues with justification and risk assessment results in statements of assessment.

3.4.4 Approve System Security Controls

Objectives:	Obtain the approval to proceed with the high-level design of the information system using the tailored set of system security controls
Primary role:	Authorizer
Supporting roles:	Security assessor
Inputs:	(3.4.2-A) System security controls (3.4.3-A) Statement of assessment for security control tailoring
Outputs:	(3.4.4-A) Approved system security controls
Security assurance requirements:	No specific requirements

Guidelines:

The main purpose of this activity is to obtain the approval of the authorizer to proceed with the high-level design phase of the IT project using the defined system security controls. IT projects should schedule this activity as part of the project gating activities for the requirements analysis phase of their SDLC.

3.5 High-Level Design Phase

This subsection describes the ISSIP activities of the high-level design phase of the SDLC, which are part of the development/acquisition phase of the SLC.

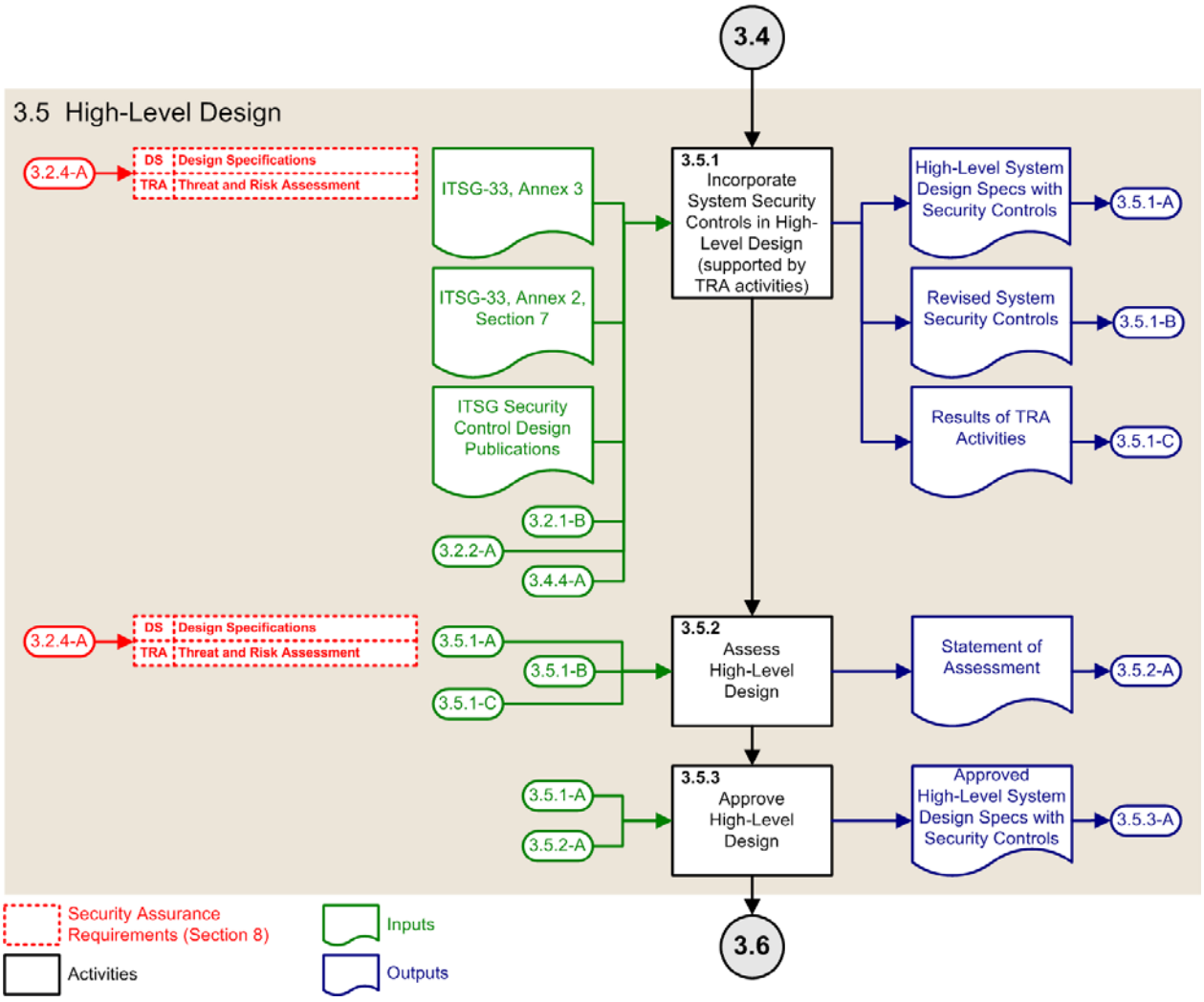


Figure 6: ISSIP Activities of the High-Level Design Phase

3.5.1 Incorporate System Security Controls in High-Level Design

Objectives:	Incorporate the system security controls in the information system's high-level design
Primary role:	System designer
Supporting roles:	Security practitioner, system integrator
Inputs:	ITSG-33, Annex 3 – *Security Control Catalogue* [Reference 7] ITSG-33, Annex 2, Section 7 – *Determining a Robustness Level* [this publication] ITSG security control design publications (e.g., ITSG-31 – *User Authentication Guidance for IT Systems* [Reference 8]) (3.2.1-B) Applicable domain threat assessment report (3.2.2-A) Information system security categorization report (in support of IT asset sensitivity assessment, part of TRA activities) (3.4.4-A) Approved system security controls
Outputs:	(3.5.1-A) High-level system design specifications with security controls (3.5.1-B) Revised system security controls (3.5.1-C) Results of TRA activities
Security assurance requirements:	(3.2.4-A) Security assurance engineering tasks and documentation content requirements for design specifications (Section 8, DS-E and DS-D) (3.2.4-A) Security assurance engineering tasks and documentation content requirements for TRA (Section 8, TRA-E and TRA-D)

Guidelines:

During the high-level design phase (sometimes called architecture design, system design, or logical design), IT projects allocate the information system's technical, operational, and management security controls to high-level system design elements. The allocation process is not specific to security and would normally follow the standard system engineering process for allocating requirements to high-level system design elements. In addition to this allocation, IT projects specify an adequate robustness level for each security control (or set of security controls with a similar robustness requirement) to guide the follow-on detailed design work and ensure the most appropriate IT security mechanisms and solutions are selected. See Section 7 for guidance on robustness.

During the high-level design process, the system designer and the security practitioner may tailor the system security controls further as they consider various approaches to security design and assess threats and risks. Section 3.5.1.1 provides further guidance on tailoring based on security design approaches and TRA activities. The security control tailoring procedures are described in Section 9.

3.5.1.1 Conduct TRA Activities

The high-level design process is supported by TRA activities, which builds on the results of the relevant domain threat assessment (if one exists) or departmental threat assessment. Part of the purpose of these TRA activities is to provide a basis for adding or removing security controls (using Annex 3 of ITSG-33 [Reference 7]) and specifying security control robustness levels to address the threat environment in a cost-effective manner.

Within ISSIP, the TRA activities are an essential component of information system security engineering. To an IT project, the TRA process is a tool that supports system design activities. System designers and security practitioners apply the TRA process to:

- Consider IT asset sensitivity and threats when identifying system components and their interactions, and when selecting security mechanisms;
- Assess the adequacy of security controls and security mechanisms at mitigating threats;
- Consider security costs and benefits;
- Adjust design specifications based on assessment results;
- Document risk scenarios; and
- Assess and report residual risks to security stakeholders.

When building information systems, the TRA activities are best performed as an iterative process. Figure 7 illustrates this approach. Performing the TRA activities in this manner is an effective way to ensure that threats, vulnerabilities, and impacts are taken into consideration when making design decisions.

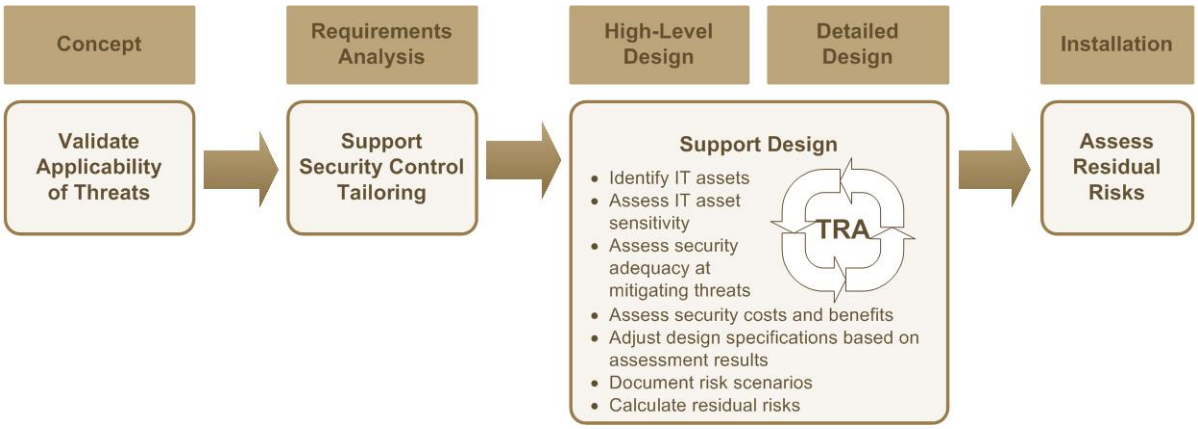


Figure 7: TRA Activities as part of ISSIP

It is recommended that system designers and security practitioners document TRA activity results in standard IT project deliverables as they progress through high-level design, detailed design, and integration and testing. The production of a standalone TRA report is neither recommended nor required. However, if there is a requirement to consolidate TRA activity results in a report, then it is recommended to do so as part the residual risk assessment (Section 3.9.3).

During the high-level design phase, the purpose of the TRA activities is to help system designers and security practitioners design an information system that will adequately protect IT assets from selected threats with the current set of system security controls, and any additional security control tailoring that may be required. The security controls need to be of sufficient robustness and allocated at the right place within the system design to adequately protect IT assets from the threats they will face in the information system's operational environment.

When tailoring system security controls at this stage, IT projects should consider the security approaches described in the applicable domain security control profile, as system-specific security controls require rationalization to account for their interrelationships.

> To illustrate this point, consider end users who need to interact with an information system that processes protected information using both desktop computers at work and notebook computers while offsite.
>
> The applicable domain security control profile for this information system prescribes the protection of information at rest (e.g., hard drive encryption) to protect the sensitive data and physical access control (e.g., an *operations zone*) to control access to desktop computers. In this scenario, the protection of information at rest could be allocated to the mobile device (e.g., notebook computers) to reduce the impact of a stolen device. In the case of fixed devices (e.g., desktop computers), the protection provided by the *operations zone* would significantly reduce the exposure of any protected data stored locally on the device.
>
> In this example, the security control requirement for data protection at rest would be unnecessary for the desktop computers to obtain an acceptable residual risk. By rationalizing security controls in this manner, IT projects can optimize security, reduce development and operational costs, and increase usability.

As documented in Annex 1 of ITSG-33 [Reference 1], departments conduct a departmental threat assessment or business-specific domain threat assessments to support IT projects. Such an approach greatly improves the quality of threat data and reduces the effort that IT projects invest in TRA activities as part of the SDLC.

IT projects should ask their departmental IT security coordinator for the TRA process that they need to follow.

3.5.1.2 Determine Security Control Robustness Levels

During TRA activities, system designers and security practitioners analyze threats and the sensitivity of the information system's IT assets, and allocate security controls to high-level design elements to adequately protect these IT assets. IT asset sensitivity is equivalent to the security category (and therefore the levels of injury) of the business activities that each IT asset supports. For example, an application server that supports a business activity with a security category of (Protected B, Medium integrity, Medium availability) will inherit a sensitivity of Protected B, medium integrity, medium availability. Security practitioners also specify the security control robustness levels that will guide detailed-level designers in the selection of appropriate security mechanisms. While not strictly required, this step provides valuable guidance to the detailed designer and is, therefore, recommended.

Robustness is used within the ISSIP for specifying the strength of and assurance required of implemented security controls to adequately protect against selected threats that can compromise the confidentiality,

integrity, and availability of IT assets. Security controls that protect more sensitive IT assets (i.e., IT assets that support business activities with higher levels of expected injuries) or that are exposed to more significant threats (i.e., threat agents with more sophisticated capabilities) need to be stronger and require more assurance in their implementation and therefore require higher levels of robustness. The robustness model is described in Section 7.

Based on the previous analysis of the information system's security category, the threat context and security approaches described in the applicable security control profile, and additional threat information documented in the associated departmental threat assessment report or domain threat assessment report (if one exists), it is possible to determine cost-effective security control robustness levels to satisfy the business needs for security.

The security approaches described in the applicable domain security control profile can also influence the specification of robustness levels, due to the protection afforded by interdependent security controls.

> For example, an information system protected by strong boundary security controls (e.g., strong transmission confidentiality, strong source authentication), strong physical security (e.g., gates, guards), and personnel security (e.g., security clearance) may allow for less robust internal security controls (e.g., standard audit and accountability controls). However, this places more emphasis on a few important controls, which therefore need to be monitored more closely to ensure that they indeed reduce the internal threat to an acceptable level. For example, if past experience (e.g., internal fraud) shows that the internal threat is higher than initially estimated, more robust internal controls should be considered (e.g., strong authentication and strong audit and accountability controls).

In turn, robustness levels influence the security assurance requirements applicable to IT projects. Higher levels of robustness specified for a set of security controls usually require more stringent security assurance requirements to be applied during the design, development, testing, and operations of these security controls.

> Because the selection of a robustness level affects costs, IT projects may have to consider other factors when selecting a security control robustness level. For example, it may not be cost-effective for a department to protect a specific business activity against sophisticated threats (e.g., highly motivated foreign intelligence services performing targeted attacks, organized crime compromising employees) because it is determined that the interest of the threat agents mostly lie elsewhere within the department. In this example, departmental officials may decide to aim for a lower robustness level (i.e., one that will not necessarily protect the information system against sophisticated threats) and accept the risk of doing so. Acceptance of the risk is thus made explicit at an early phase of the information system's development. In any event, the selection of a different robustness level than the one recommended in Section 7 should be justified and sufficiently documented.

The robustness level of security controls and the related security assurance requirements may be adjusted later during the detailed-design phase of the ISSIP in response to refined threat analyses and design choices.

Refer to Section 7 for guidance on the determination of appropriate security control robustness levels based on IT assets sensitivity and threat category.

3.5.2 Assess High-Level Design

Objectives:	Confirm that the allocation of security controls in the high-level design was completed in conformance with the security assurance requirements
Primary role:	Security assessor
Supporting roles:	Security practitioner
Inputs:	(3.5.1-A) High-level system design specifications with security controls (3.5.1-B) Revised system security controls (3.5.1-C) Results of TRA activities
Outputs:	(3.5.2-A) Statement of assessment for the high level system design.
Security assurance requirements:	(3.2.4-A) Security assurance assessment tasks for design specification (Section 8, DS-A) (3.2.4-A) Security assurance assessment tasks for TRA (Section 8, TRA-A)

Guidelines:

With assistance from the security practitioner, the security assessor should perform the following tasks:

- Confirm that the high-level design specification work satisfies the engineering tasks and the documentation content requirements;
- Confirm that the TRA work satisfies the engineering tasks and documentation content requirements; and
- Prepare a statement of assessment for approval.

3.5.3 Approve High-Level Design

Objectives:	Obtain the approval to proceed with the detailed design of the information system based on the high-level design specifications
Primary role:	Authorizer
Supporting roles:	Security assessor
Inputs:	(3.5.1-A) High-level system design specifications with security controls (3.5.2-A) Statement of assessment for the high-level system design
Outputs:	(3.5.3-A) Approved high-level system design specifications with security controls
Security assurance requirements:	No specific requirements

Guidelines:

This activity is recommended for large IT projects and when implementing information systems to support more critical business activities, and may be omitted for smaller IT projects and less critical information systems.

IT projects should schedule this activity as part of the project gating activities for the high-level design phase of their SDLC.

The main purpose of this activity is to obtain the approval of the authorizer to proceed with the detailed design phase of the IT project using the high-level design specifications. It also gives the authorizer and other security stakeholders the opportunity to review and approve the other ISSIP outputs from the high-level design phase before allowing the IT project to proceed. IT projects should consider:

- Reviewing with the authorizer and departmental security officials the results of the TRA activities from the high-level design phase, particularly the decisions and supporting arguments for reducing or augmenting security controls; and
- Reviewing with departmental security officials the revised system security controls.

3.6 Detailed Design Phase

This subsection describes the ISSIP activities of the detailed design phase of the SDLC, which are part of the development/acquisition phase of the SLC.

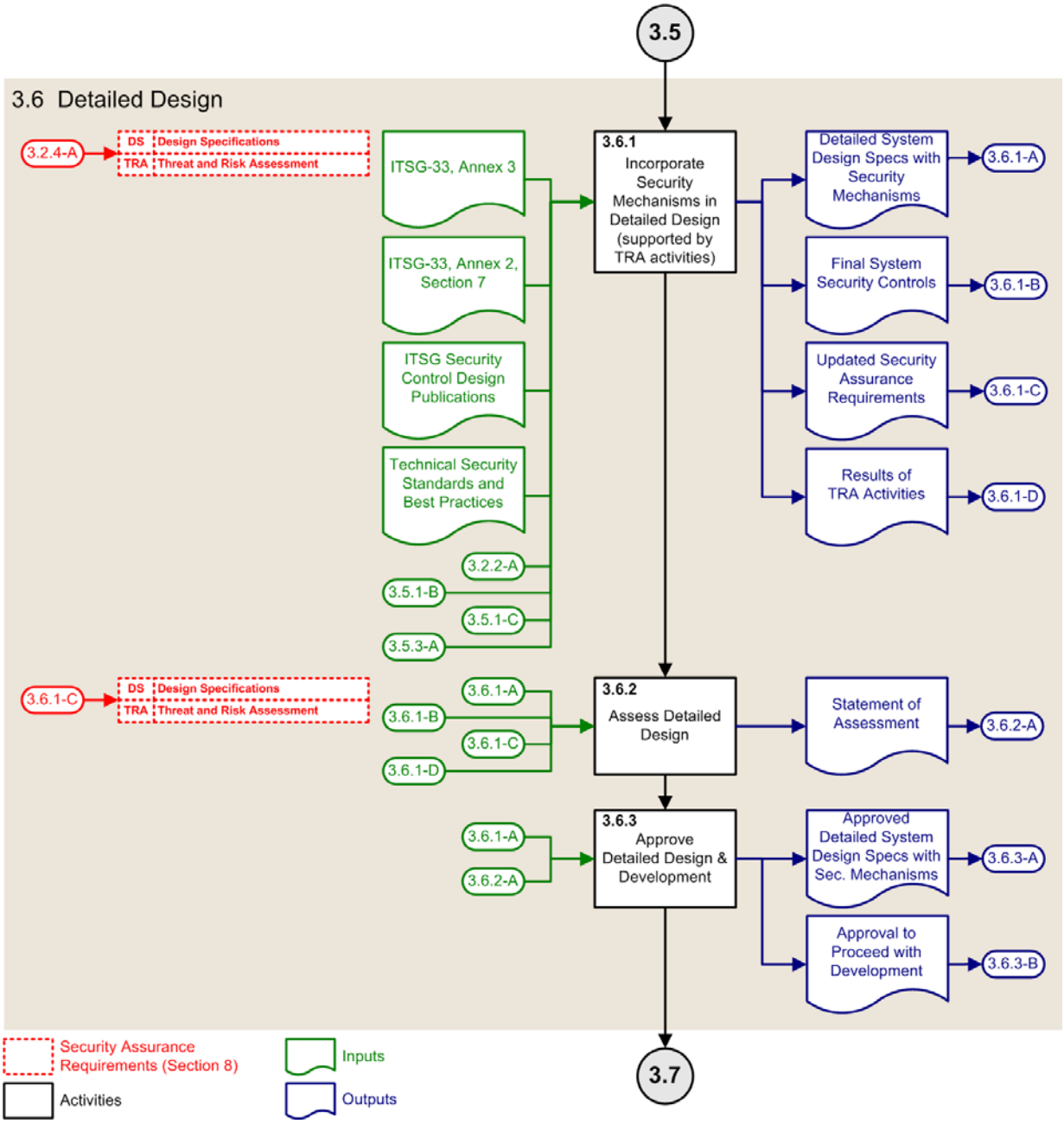


Figure 8: ISSIP Activities of the Detailed Design Phase

3.6.1 Incorporate Security Mechanisms in Detailed Design

Objectives:	Satisfy security control requirements in the information system's detailed design by assigning suitable security mechanisms to detailed design elements
Primary role:	System designer, system integrator
Supporting roles:	Security practitioner
Inputs:	ITSG-33, Annex 3 – *Security Control Catalogue* [Reference 7] ITSG-33, Annex 2, Section 7 – *Determining a Robustness Level* [this publication] ITSG security control design publications (e.g., ITSG-31 – *User Authentication Guidance for IT Systems* [Reference 8]) Governmental and industry technical security standards and best practices (3.2.2-A) Information system security categorization report (in support of IT asset sensitivity assessment, part of the TRA activities) (3.5.1-B) Revised system security controls (3.5.1-C) Results of TRA activities (from previous phase) (3.5.3-A) Approved high-level system design specifications with security controls
Outputs:	(3.6.1-A) Detailed system design specifications with security mechanisms (3.6.1-B) Final system security controls (3.6.1-C) Updated security assurance requirements (3.6.1-D) Results of TRA activities
Security assurance requirements:	(3.2.4-A) Security assurance engineering tasks and documentation content requirements for design specifications (Section 8, DS-E and DS-D) (3.2.4-A) Security assurance engineering tasks and documentation content requirements for TRA (Section 8, TRA-E and TRA-D)

Guidelines:

During the detailed design phase, IT projects allocate security mechanisms to the detailed design elements to satisfy the security controls specified in the high-level system design specifications. The detailed design process is not specific to security and should follow the standard system engineering process for transforming high-level design specifications into detailed design specifications.

3.6.1.1 Conduct TRA Activities

During the detailed design phase, the TRA activities provide risk-based rationale for specifying security mechanisms of sufficient strength to protect information system components from threats. The high-level design specifies the required robustness levels of security controls. Note that ITSG publications such as ITSG-31 – *User Authentication Guidance for IT Systems* [Reference 8] contain guidelines on the selection of security mechanisms for security controls such as authentication based on robustness levels.

The security mechanisms need to be of sufficient strength and allocated at the right place within the detailed design to adequately protect IT assets from the threats that they will face in the information system's operational environment. The TRA activities could lead to changes in the selection of security controls to address security issues specific to the detailed design. If changes are effected, then the system security controls output must be updated accordingly.

It is recommended that system designers and security practitioners document TRA activity results in standard IT project deliverables as they progress through high-level design, detailed design, and integration and testing.

Changes in the specified robustness levels at this stage may result in changes to security assurance requirements. IT projects need to consider such changes carefully as they may result in additional costs and delays if the requirements analysis phase or high-level design phase of the SDLC need to be repeated, in whole or in part, to address new security assurance requirements. If changes are effected, then the security assurance requirements output must be updated accordingly.

See Section 9 for security control tailoring procedures.

3.6.2 Assess Detailed Design

Objectives:	Confirm that the specification of security mechanisms in the detailed design was completed in conformance with the security assurance requirements
Primary role:	Security assessor
Supporting roles:	Security practitioner
Inputs:	(3.6.1-A) Detailed system design specifications with security mechanisms (3.6.1-B) Final system security controls (3.6.1-C) Updated security assurance requirements (3.6.1-D) Results of TRA activities
Outputs:	(3.6.2-A) Statement of assessment for detailed system design
Security assurance requirements:	(3.6.1-C) Security assurance assessment tasks for design specifications (Section 8, DS-A) (3.6.1-C) Security assurance assessment tasks for TRA (Section 8, TRA-A)

Guidelines:

With assistance from the security practitioner, the security assessor should perform the following tasks:

- Confirm that the detailed design specification work satisfies the engineering tasks and the documentation content requirements;
- Confirm that the TRA work satisfies the engineering tasks and documentation content requirements; and
- Prepare a statement of assessment for approval.

3.6.3 Approve Detailed Design and Development

Objectives:	Obtain the approval to proceed with the development of the information system based on the detailed design specifications
Primary role:	Authorizer
Supporting roles:	Security assessor
Inputs:	(3.6.1-A) Detailed system design specifications with security mechanisms (3.6.2-A) Statement of assessment for detailed system design
Outputs:	(3.6.3-A) Approved detailed design specifications with security mechanisms (3.6.3-B) Approval to proceed with development
Security assurance requirements:	No specific requirements

Guidelines:

The main purpose of this activity is to obtain the authorizer's approval to proceed with the development of the information system based on the detailed design specifications. If required, IT projects should obtain this approval before establishing the development environment and engaging the development team, which can represent significant project costs. It also gives the authorizer and other security stakeholders the opportunity to review and approve the other ISSIP outputs from the detailed design phase before allowing the IT project to proceed. IT projects should consider:

- Reviewing with the authorizer and departmental security officials the results of the TRA activities from the detailed design phase, particularly the decisions and supporting arguments for reducing or augmenting security controls and for selecting the security mechanisms;
- Reviewing with departmental security officials the final system-specific security controls; and
- Reviewing with the authorizer and departmental security officials, all changes to the security assurance requirements for the remainder of the security activities.

IT projects should schedule this activity as part of the project gating activities for the detailed design phase of their SDLC.

The approval to proceed with the development of the information system can be as simple as a record of decision appearing in the minutes of an engineering or project meeting, or as formal as a letter of approval signed by the authorizer.

3.7 Development Phase

This subsection describes the ISSIP activities of the development phase of the SDLC, which are part of the development/acquisition phase of the SLC.

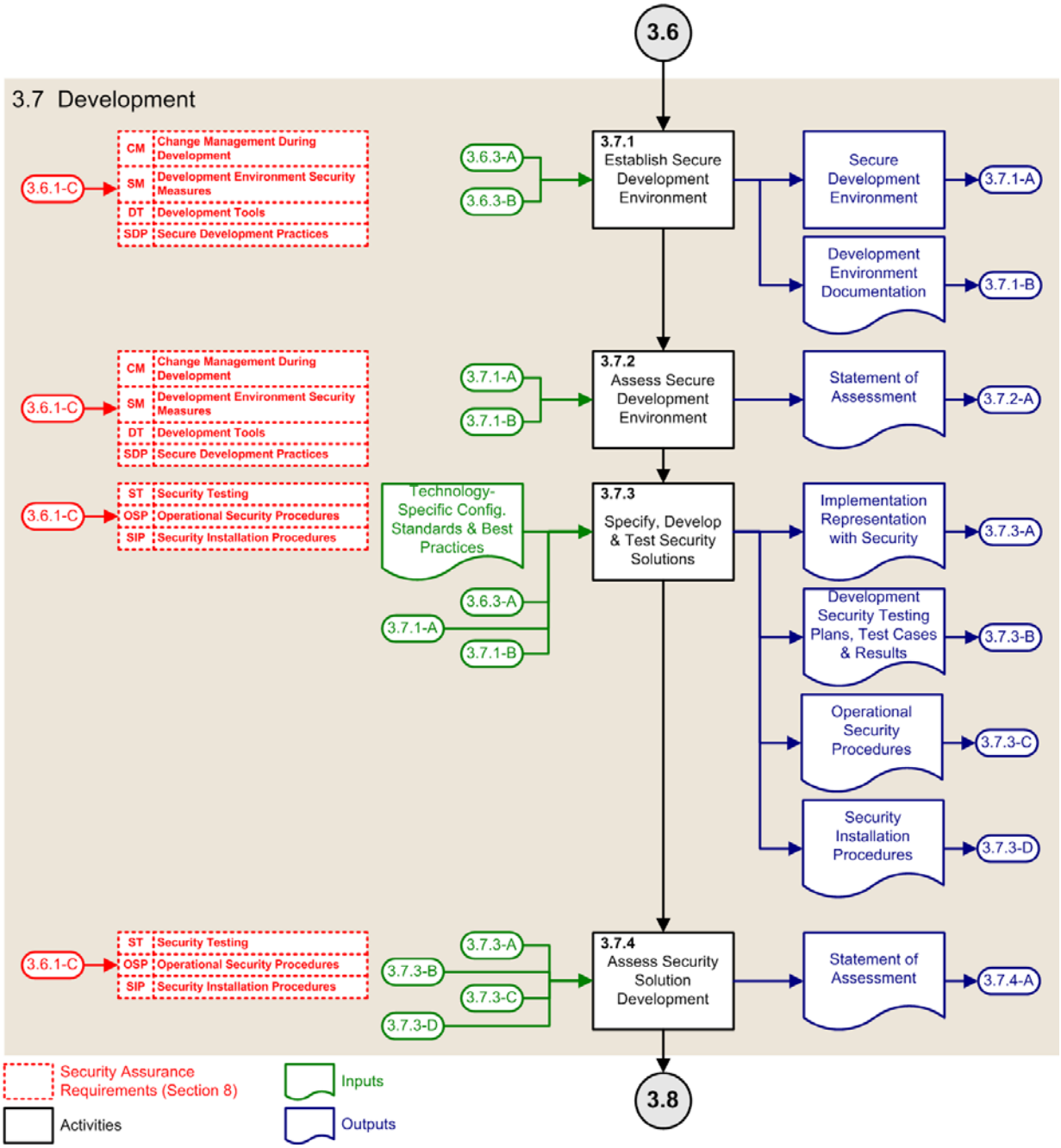


Figure 9: ISSIP Activities of the Development Phase

3.7.1 Establish Secure Development Environment

Objectives:	Establish a secure system development environment to support the development of the information system and its security
Primary role:	System developer
Supporting roles:	Security practitioner
Inputs:	(3.6.3-A) Approved detailed system design specifications with security mechanisms (3.6.3-B) Approval to proceed with development
Outputs:	(3.7.1-A) Secure development environment (3.7.1-B) Development environment documentation
Security assurance requirements:	(3.6.1-C) Security assurance engineering tasks and documentation content requirements for change management during development (Section 8, CM-E and CM-D) (3.6.1-C) Security assurance engineering tasks and documentation content requirements for development environment security measures (Section 8, SM-E and SM-D) (3.6.1-C) Security assurance engineering tasks and documentation content requirements for development tools (Section 8, DT-E and DT-D) (3.6.1-C) Security assurance engineering tasks and documentation content requirements for secure development practices (Section 8, SDP-E and SDP-D)

Guidelines:

Security assurance requirements largely dictate the work that the IT project needs to invest to establish a suitably secure development environment and practices. To avoid security vulnerabilities and weaknesses in information systems, security assurance requirements prescribe the use of sound development and procurement practices, not just for security solutions but for all aspects of the information system. Efforts that are invested in establishing quality, reliability, and resiliency of software and hardware all contribute to the development of dependable information systems regardless of whether or not these efforts are directed at security.

Development and procurement practices that support the implementation of dependable information systems include, but are not limited to, the following:

- Security engineering principles and methodologies;
- Secure coding practices;
- Use of safe language standards;
- Use of source code analysis tools and techniques;
- Use of binary analysis tools and techniques;

- Source code review;
- Code signing;
- Use of commercial or open-source automated test tools;
- Selection of commercial products that have been validated against security criteria (e.g., FIPS for cryptographic modules, Common Criteria for products); and
- Use of trusted software and hardware suppliers.

3.7.2 Assess Secure Development Environment

Objectives:	Confirm that the secure development environment was established in conformance with the security assurance requirements
Primary role:	Security assessor
Supporting roles:	Security practitioner
Inputs:	(3.7.1-A) Secure development environment (3.7.1-B) Development environment documentation
Outputs:	(3.7.2-A) Statement of assessment for the secure development environment
Security assurance requirements:	(3.6.1-C) Security assurance assessment tasks for change management during development (Section 8, CM-A) (3.6.1-C) Security assurance assessment tasks for development environment security measures (Section 8, SM-A) (3.6.1-C) Security assurance assessment tasks for development tools (Section 8, DT-A) (3.6.1-C) Security assurance assessment tasks for secure development practices (Section 8, SDP-A)

Guidelines:

With assistance from the security practitioner, the security assessor should perform the following tasks:

- Confirm that the work to establish the development environment satisfies the engineering tasks and the documentation content requirements; and
- Prepare a statement of assessment for approval.

3.7.3 Specify, Develop, and Test Security Solutions

Objectives:	Specify the security solutions that will implement the security mechanisms as specified in detailed design specifications, develop custom security components, and acquire those that are commercially available. Apply secure practices to all aspects of the information system development activities.
Primary role:	System developer
Supporting roles:	Security practitioner, system integrator, system tester
Inputs:	Technology-specific security configuration standards and best practices (3.6.3-A) Approved detailed system design specifications with security mechanisms (3.7.1-A) Secure development environment (3.7.1-B) Development environment documentation
Outputs:	(3.7.3-A) Information system implementation representation with security (including bill of materials and security configuration parameters) (3.7.3-B) Development security testing plans, test cases, and results (3.7.3-C) Operational security procedures (3.7.3-D) Security installation procedures
Security assurance requirements:	(3.6.1-C) Security assurance engineering tasks and documentation content requirements for security testing (Section 8, ST-E and ST-D) (3.6.1-C) Security assurance engineering tasks and documentation content requirements for operational security procedures (Section 8, OSP-E and OSP-D) (3.6.1-C) Security assurance engineering tasks and documentation content requirements for security installation procedures (Section 8, SIP-E and SIP-D)

Guidelines:

The development activities follow the secure development practices that are implemented for the secure development environment in response to security assurance requirements. The prescribed practices apply not just to the development of security solutions but to the entire information system (e.g., secure coding practices apply to all software components of the information system, and are not limited to the security components). Security mechanisms can be implemented in several ways:

- By acquiring and installing commercial security products;
- By using the security mechanisms of commercial (non-security) products;
- By securely configuring commercial products;
- By coding a security control as a discrete software program;

- By inserting a security control as code within other software code;
- By acquiring an external capability (i.e., a capability from an external provider);
- By specifying an operational security procedure (see Section 3.7.3.1); and
- By specifying a security installation procedure (see Section 3.7.3.3).

As the development work progresses, system developers, with the help of security practitioners, need to identify and address, within the physical implementation, system configuration parameters that apply to their choices of technology. For example, if a system developer opts for OpenSSL to implement a session encryption security mechanism, the system developer specifies the security configuration parameters that satisfy applicable configuration standards or best practices. System developers need to identify all such parameters and include corresponding specifications in the information system's implementation representation. The implementation of system security parameters can then be assessed during the installation phase of the SDLC.

Any testing that can be conducted as part of the development effort and that contributes to the establishment of security assurance is part of this activity. This includes functional testing of custom security solutions (e.g., functional unit testing), but may also include other forms of testing such as negative functional testing of non-security functions (e.g., fuzz testing of URL against a web application). It may also include the testing of operational procedures to determine usability and maintainability.

System developers must produce development security testing plans, test cases, and results for security assurance purposes.

Security in contracting guidelines may influence the procurement of commercial solutions in many ways. For example, practices may require the use of trusted sources for software acquisition.

The information system implementation representation with security is the main output of the development phase. It is the least abstract representation of the information system. It consists of source code, hardware and software products, physical network diagrams, configuration documentation such as build books, and so on. Collectively, these elements allow for the construction of the information system without having to make any further design or implementation decisions.

3.7.3.1 Functional Security Testing

Security testing in this phase of the SDLC includes functional security testing. The purpose of functional security testing is to validate the functionality of security mechanisms as implemented by security solutions.

When the test cases are prepared, system developers should ensure that the functionality of each security mechanism will be appropriately tested, and that each test clearly establishes its correspondence with the security mechanism that it validates. As indicated in Section 3.4.2.1, system developers can use an SRTM to establish this correspondence. If an SRTM is used, system testers can update it with the actual results as security testing progresses. Doing so will result in an SRTM that provides full backward traceability from test cases to design elements to business needs for security.

3.7.3.2 Operational Security Procedures

In support of operations, system developers and security practitioners should produce a set of operational security procedures that ensure the secure operation, administration, and maintenance of the information

system during its operational period. Operational security procedures form part of the security provisions that IT operations groups should include in their operations plan.

Subject to departmental policies and standards, operational security procedures should address the following topics:

- Information system security policies and procedures;
- Security aspects of change management (which includes patch management);
- Security aspects of configuration management;
- Security aspects of release management;
- Incident management;
- Contingency planning;
- Periodic information system security assessments such as vulnerability assessments;
- Security maintenance requirements such as cryptographic key updates;
- Review of threats, vulnerabilities, and risks;
- Security compliance reviews and audits;
- Risk management reporting; and
- Security aspects of an information system disposal plan.

Typically, these topics will be covered by operational security procedures that have already been implemented as common security controls. IT projects should consult with their IT security coordinator to determine if operational security procedures inherited as common security controls satisfy the system-specific security controls, and identify those that have to be developed as part of the project.

3.7.3.3 Security Installation Procedures

System developers should produce security installation procedures for the information system. Security installation procedures describe the steps required to correctly install and configure security solutions and set security configuration parameters, including hardening procedures, during the installation process and as part of disaster recovery.

3.7.4 Assess Security Solution Development

Objectives:	Confirm that the development of security solutions and the information system as a whole was completed in conformance with the security assurance requirements
Primary role:	Security assessor
Supporting roles:	Security practitioner
Inputs:	(3.7.3-A) Information system implementation representation with security (3.7.3-B) Development security testing plans, test cases, and results. (3.7.3-C) Operational security procedures (3.7.3-D) Security installation procedures
Outputs:	(3.7.4-A) Statement of assessment for security development
Security assurance requirements:	(3.6.1-C) Security assurance assessment tasks for security testing (Section 8, ST-A) (3.6.1-C) Security assurance assessment tasks for operational security procedures (Section 8, OSP-A) (3.6.1-C) Security assurance assessment tasks for security installation procedures (Section 8, SIP-A)

Guidelines:

With assistance from the security practitioner, the security assessor should perform the following tasks:

- Confirm that the security testing work performed as part of development satisfies the engineering tasks and the documentation content requirements;
- Confirm that the operational security procedures satisfy the documentation content requirements;
- Confirm that the security installation procedures satisfy the documentation content requirements; and
- Prepare a statement of assessment for approval.

3.8 Integration and Testing Phase

This subsection describes the ISSIP activities of the integration and testing phase of the SDLC, which are part of the integration and installation phase of the SLC.

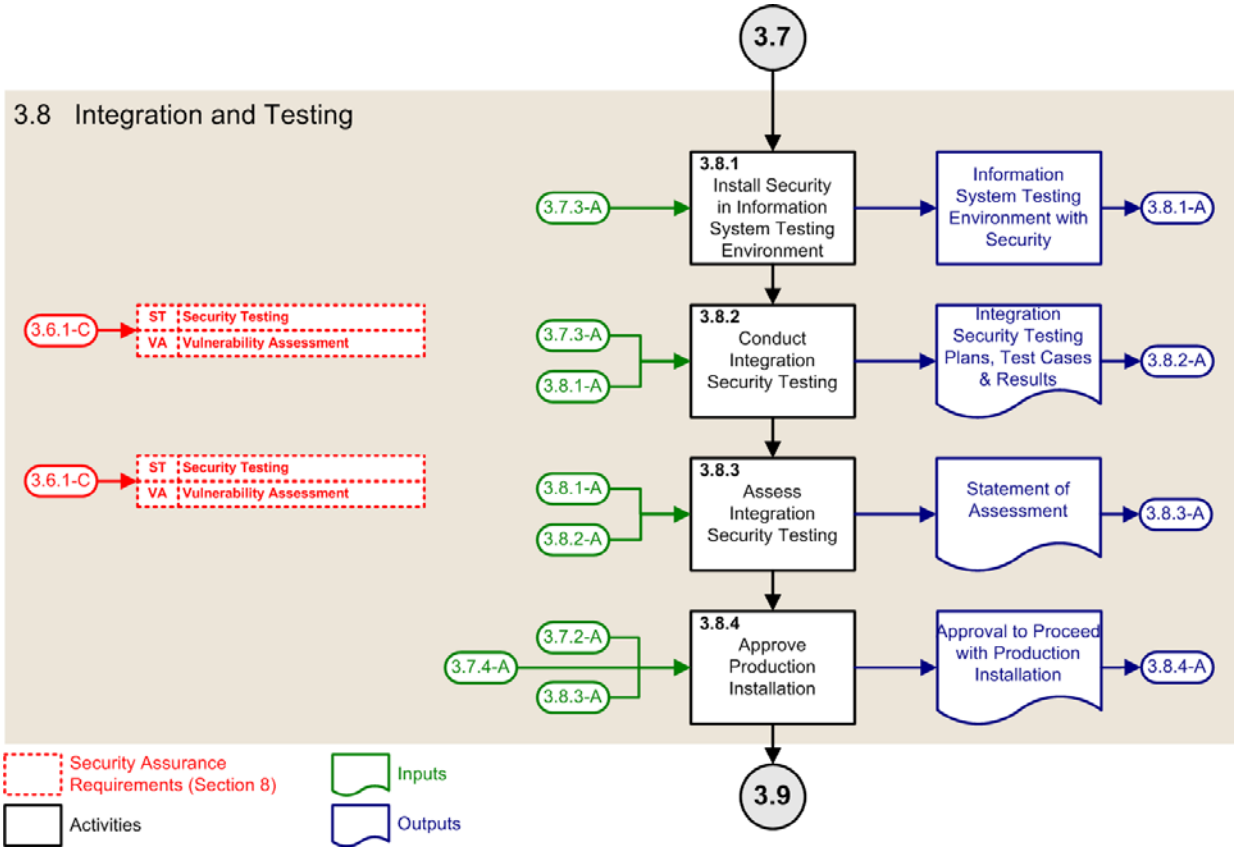


Figure 10: ISSIP Activities of the Integration and Testing Phase

3.8.1 Install Security in Information System Testing Environment

Objectives:	Install security in the information system's testing environment in accordance with the information system implementation representation
Primary role:	System integrator
Supporting roles:	Security practitioner
Inputs:	(3.7.3-A) Information system implementation representation with security
Outputs:	(3.8.1-A) Information system testing environment with security
Security assurance requirements:	No specific requirements

Guidelines:

To prepare for security testing, IT projects install security components and apply security configuration within one or more testing environments. The testing environments need to provide suitable platforms to conduct all of the prescribed security tests.

Note that IT projects may go through several stages of testing; integration and then quality assurance, or integration and then user acceptance, for example. When such is the case, the IT project installs security capabilities at every testing stage.

3.8.2 Conduct Integration Security Testing

Objectives:	Test the security aspects of the information system in accordance with security testing plans
Primary role:	System tester
Supporting roles:	Security practitioner
Inputs:	(3.7.3-A) Information system implementation representation with security (3.8.1-A) Information system testing environment with security
Outputs:	(3.8.2-A) Integration security testing plans, test cases, and results
Security assurance requirements:	(3.6.1-C) Security assurance engineering tasks and documentation content requirements for security testing (Section 8, ST-E and ST-D) (3.6.1-C) Security assurance engineering tasks and documentation content requirements for vulnerability assessment (Section 8, VA-E and VA-D)

Guidelines:

Integration security testing at this phase should cover all of the security solutions that are part of the information system, both technical and procedural, including operational security procedures and security

installation procedures. Integration security testing includes functional security testing and may also include vulnerability assessments and penetration testing, depending on the security assurance requirements. Test failures should be investigated and, to the extent possible, corrected and retested as part of the security test cycle. The implementation representation, operational security procedures, and security installation procedures should be updated to reflect all corrective changes.

System integrators must produce as part of this activity integration security test plans and test cases along with their associated results.

Note: Regression testing should be conducted by IT projects, and the results reported, along with integration security testing results, in order to increase the confidence that changes and updates to the information system have not inadvertently introduced weaknesses with security implications.

3.8.2.1 Vulnerability Assessment and Penetration Testing

Depending on the security assurance requirements, system testers may conduct vulnerability assessments as part of security integration testing. The objectives of vulnerability assessment activities at this stage are to:

- Ensure that the installed IT products are free of known vulnerabilities or that known vulnerabilities are documented and have been mitigated to an acceptable level; and
- Ensure that security hardening (e.g., disabling of unused TCP ports and services) has been implemented in accordance with departmental or industry standards and best practices.

The system tester may also have to conduct penetration testing to validate certain aspects of the information system's security, for example, by testing the resilience of a web application interface to certain attacks (e.g., SQL injection), or testing the resilience of network perimeter security by exercising firewall rules or router hardening configuration.

3.8.3 Assess Integration Security Testing

Objectives:	Confirm that security testing was completed in conformance with the security assurance requirements
Primary role:	Security assessor
Supporting roles:	Security practitioner
Inputs:	(3.8.1-A) Information system testing environment with security (3.8.2-A) Integration security testing plans, test cases, and results
Outputs:	(3.8.3-A) Statement of assessment for integration security testing
Security assurance requirements:	(3.6.1-C) Security assurance assessment tasks for security testing (Section 8, ST-A) (3.6.1-C) Security assurance assessment tasks for vulnerability assessment (Section 8, VA-A)

Guidelines:

With assistance from the security practitioner, the security assessor should perform the following tasks:

- Confirm that the security testing work performed as part of integration satisfies the engineering tasks and the documentation content requirements;
- Confirm that the vulnerability assessment work satisfies the engineering tasks and the documentation content requirements; and
- Prepare a statement of assessment for approval.

3.8.4 Approve Production Installation

Objectives:	Obtain the approval to proceed with the installation of the information system in the production environment in accordance with the information system implementation representation
Primary role:	Authorizer
Supporting roles:	Security assessor
Inputs:	(3.7.2-A) Statement of assessment for the secure development environment (3.7.4-A) Statement of assessment for security development (3.8.3-A) Statement of assessment for integration security testing
Outputs:	(3.8.4-A) Approval to proceed with production installation
Security assurance requirements:	No specific requirements

Guidelines:

This activity is recommended for large IT projects, or when implementing information systems to support more critical GC programs or business processes.

The main purpose of this activity is to obtain the authorizer's approval to proceed with the installation of the information system in the production environment in accordance with the implementation representation. The approval can be as simple as a record of decision appearing in the minutes of an engineering or project meeting, or as formal as a letter of approval signed by the authorizer.

3.9 Installation Phase

This subsection describes the ISSIP activities for the installation phase of the SDLC, which are part of the integration and installation phase of the SLC.

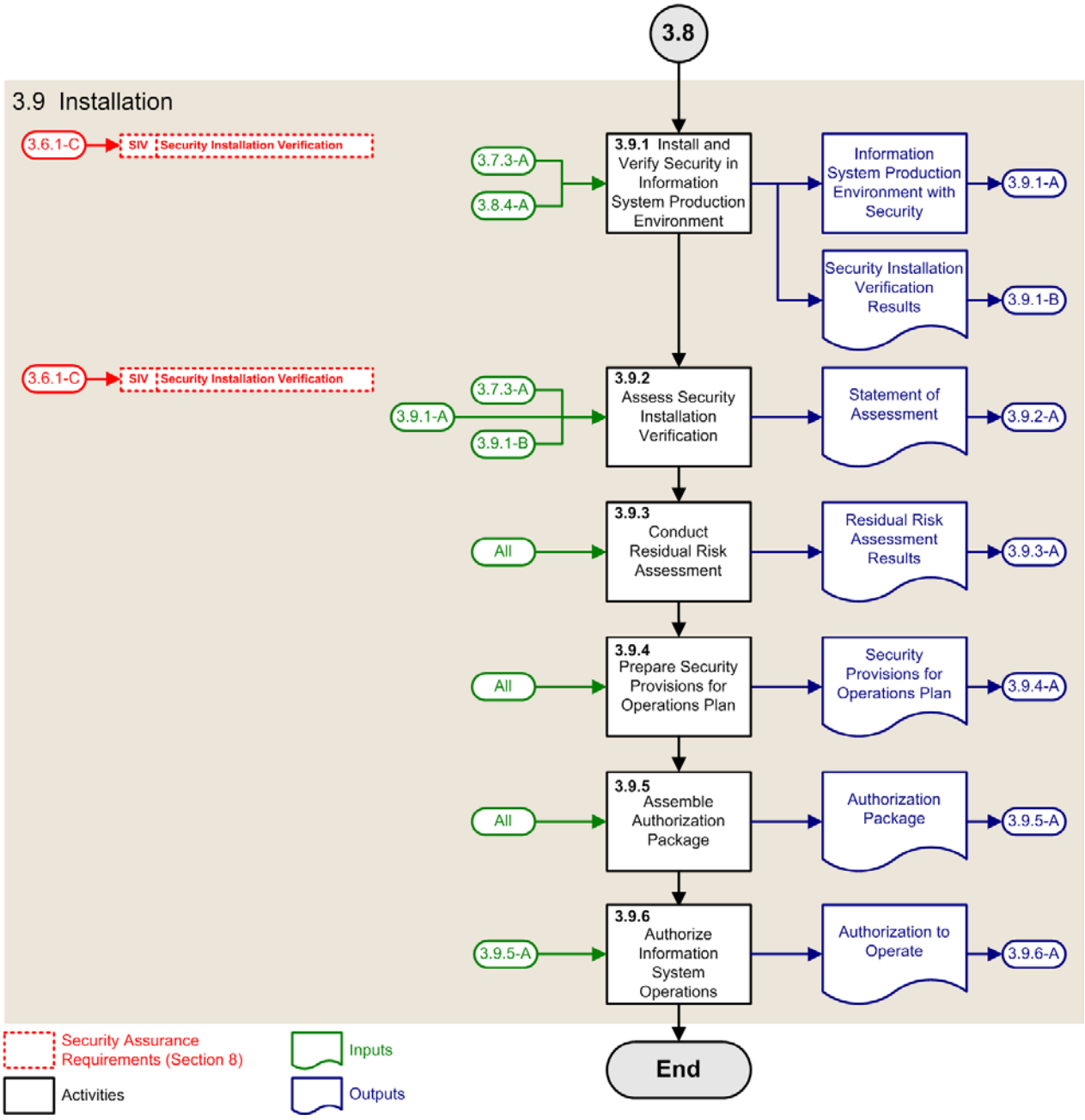


Figure 11: ISSIP Activities of the Installation Phase

3.9.1 Install and Verify Security in Information System Production Environment

Objectives:	Install security in the information system's production environment and confirm that the installation and configuration complies with the implementation representation
Primary role:	System administrator
Supporting roles:	Security practitioner
Inputs:	(3.7.3-A) Information system implementation representation with security (3.8.4-A) Approval to proceed with production installation
Outputs:	(3.9.1-A) Information system production environment with security (3.9.1-B) Security installation verification results
Security assurance requirements:	(3.6.1-C) Security assurance engineering tasks and documentation content requirements for security installation verification (Section 8, SIV-E and SIV-D)

Guidelines:

This activity is completed in conjunction with the information system installation activities. As part of the installation process, the security practitioner verifies the security installation as prescribed by the security assurance requirements. This verification is completed by reviewing and inspecting the security solutions that are implemented in the production environment to confirm that everything is installed and configured as per the implementation representation. Deficiencies in installation and configuration are corrected as part of this activity.

3.9.2 Assess Security Installation Verification

Objectives:	Confirm that the security installation verification was completed in conformance with the security assurance requirements
Primary role:	Security assessor
Supporting roles:	Security practitioner, system administrator
Inputs:	(3.7.3-A) Information system implementation representation with security (3.9.1-A) Information system production environment with security (3.9.1-B) Security installation verification results
Outputs:	(3.9.2-A) Statement of assessment for security installation verification
Security assurance requirements:	(3.6.1-C) Security assurance assessment tasks for security installation verification (Section 8, SIV-A)

Guidelines:

With assistance from the security practitioner and the system administrator, the security assessor should perform the following tasks:

- Confirm that the security installation verification work satisfies the engineering tasks and the documentation content requirements; and
- Prepare a statement of assessment for approval.

3.9.3 Conduct Residual Risk Assessment

Objectives:	Determine and document the residual levels of risk under which the information system will be operating
Primary role:	Security assessor
Supporting roles:	Security practitioner
Inputs:	All previous ISSIP outputs
Outputs:	(3.9.3-A) Residual risk assessment results
Security assurance requirements:	No specific requirements

Guidelines:

To complete the residual risk assessment, the security assessor, with the help of the security practitioner, should consider performing the following tasks:

- Summarize risk scenarios and risk decisions (i.e., mitigate, avoid, accept) that have been documented during the high-level and detailed design phases through the TRA activities;
- Summarize security deficiencies identified during the development, integration and testing, and installation phases of the SDLC that have not been corrected or mitigated;
- Adjust risk levels to determine the risk profile under which the information system will be operating; and
- Document the results in a residual risk assessment report.

There are several reasons why there may be outstanding security deficiencies at this late stage in the process. For example, the IT project may have decided to delay until the maintenance phase the correction of a minor bug in a software module discovered during integration security testing to avoid delaying the entire project. As another example, a vulnerability in a software product was discovered when conducting a vulnerability assessment during integration security testing for which there is no patch or workaround available from the vendor. The residual risk assessment activity includes an assessment of the impact that outstanding security deficiencies such as these may have on vulnerabilities and risks.

The security assessor should ensure that request for change (RFC) records have been created in the change management system for each outstanding security deficiency. The use of other mechanisms such as the use of a safeguard implementation plan is not recommended.

In addition to assessing and documenting residual risks, this activity may also include the preparation of a TRA report, if one is required. Security practitioners can prepare a TRA report by consolidating the results of the TRA activities, which were documented during the high-level design phase (Section 3.5.1.1) and detailed design phase (Section 3.6.1.1), with the results of the residual risk assessment. In general, the size and complexity of a TRA report should reflect the size and complexity of the IT project.

3.9.4 Prepare Security Provisions for Operations Plan

Objectives:	Prepare the security provisions for the information system's operations plan
Primary role:	Security practitioner
Supporting roles:	Security assessor, IT operations personnel
Inputs:	All previous ISSIP outputs
Outputs:	(3.9.4-A) Security provisions for operations plan
Security assurance requirements:	No specific requirements

Guidelines:

The security provisions for an operations plan specify a schedule of actions and procedures that the operational group performs during the operations and maintenance phase to ensure that the information system's security posture is maintained, and that risks are appropriately managed.

Security provisions for the operations plan consist of the following:

- The operational security procedures developed during the development phase (Section 3.7.3); and
- A list of outstanding security deficiencies and their mitigation plans and schedules.

3.9.5 Assemble Authorization Package

Objectives:	Prepare an authorization package, which provides the necessary evidence to support the authorization of information system operations
Primary role:	Security practitioner
Supporting roles:	Security assessor
Inputs:	All previous ISSIP outputs
Outputs:	(3.9.5-A) Authorization package
Security assurance requirements:	No specific requirements

Guidelines:

The authorization package is what is submitted to the authorizer for authorization. The authorizer and the project manager should agree at the beginning of the IT project as to the exact composition of the authorization package. At a minimum, the authorization package should include the statements of assessment, the residual risk assessment results or TRA report, and the operations plan (which includes the security provisions).

3.9.6 Authorize Information System Operations

Objectives:	Authorize information system operations
Primary role:	Authorizer
Supporting roles:	Security assessor, project manager
Inputs:	(3.9.5-A) Authorization package
Outputs:	(3.9.6-A) Authorization to operate
Security assurance requirements:	No specific requirements

Guidelines:

The authorizer is responsible for authorizing information system operations. The decision whether or not to authorize operations is made on the basis of the content of the authorization package. The authorizer may issue an authorization to operate, with or without conditions, or issue a denial of authorization to operate. The decision will be based on several factors, most importantly the acceptability of the residual risks and the nature of outstanding security deficiencies.

Authorization is a state that an information system is in during the operations and maintenance phase of the SLC. It is not a condition that expires after a period of time and that needs to be renewed. Once in operation, an information system is subjected to continuous security monitoring and assessment by the

responsible IT security group, as well as by the IT security function following the guidelines in Annex 1 of ITSG-33 [Reference 1]. In the case of a major security event, the authorization to operate may be revoked. This would essentially remove the information system from its operational state. In the case of other less severe security events, or in light of security assessment results, the authorizer may request security updates to maintain the information system's authorization to operate.

An authorization to operate can be conveyed to the individual or the organization with the information system's operational responsibility, as well as the stakeholders by issuing a formal statement of authorization. The statement should include the date that the operations commenced, as well as any conditions under which authority was granted. A denial of operations should lead back to some point in the SDLC where the root cause of the denial can be addressed to the satisfaction of the authorizer.

3.9.6.1 System Security Plan

By completing the ISSIP activities, IT projects will produce the information elements that are normally found in a system security plan (not to be confused with the departmental security plan, which is discussed in Annex 1 of ITSG-33 [Reference 1]). Although ISSIP promotes the minimization of standalone security documentation through the integration of ISSIP outputs into standard project deliverables, it does not proscribe the use of system security plans. Where departments have established the requirement for system security plans in their departmental security control profile or domain security control profiles, IT projects can easily prepare one for their information system by assembling information elements from various ISSIP outputs. Refer to security control PL-2 in Annex 3 of ITSG-33 [Reference 7] for more information.

4 Secure Operations and Maintenance Phase

This section provides general guidelines to departments on the security activities that help maintain the security posture of information systems during their in-service period.

While the ISSIP is strictly an SDLC methodology, there are security activities that operations groups perform as part of a larger SLC process to maintain the security posture of information systems as delivered by IT projects. These activities address security during the operations and maintenance phase of a typical SLC process.

4.1 Maintain Secure Operations

Objectives:	Maintain the security posture of the information system during the operations and maintenance phase of the SLC by administering and maintaining the implemented security solutions.
Primary role:	IT operations personnel, system administrator
Supporting roles:	System designer, system developer, system integrator, IT security coordinator, security practitioner, (external) security assessor
Inputs:	(3.7.3-A) Information system implementation representation with security (3.9.4-A) Security provisions for operations plan
Outputs:	(4.1-A) Outputs produced during the secure operations of the information system e.g., change and problem management records, incident reports, security configuration updates, consolidated system logs (consisting of system event records, security event records, audit records, application event records, intrusion detection records, etc.), and security solution performance metrics. (4.1-B) Updated information system implementation representation
Security assurance requirements:	Various requirements depending on the activity (e.g., a design change would require engineering, documentation, and testing activities to implement)

Guidelines:

IT operations groups administer and maintain the information system's security during the operations and maintenance phase of the SLC according to the security provisions of the operations plan (as defined in Section 3.9.4). The administration and maintenance process ensures that security solutions remain properly configured and are properly used.

To effectively maintain and administer the security of information systems, departments:

- Establish and assign operational security roles and responsibilities;
- Provide security awareness and training to operational staff and users;
- Perform periodic security maintenance and administrative tasks on security solutions;

- Analyse, specify, and implement changes to security solutions in response to new requirements, evolving threats, security incidents, and newly discovered vulnerabilities;
- Implement security patches and updates; and
- Manage security configurations.

During the operational phase, IT operations groups maintain the security posture of information systems through change and configuration management processes and procedures that address security concerns as documented in change and configuration management plans. Changes during that period may require changes to security solutions or may otherwise have an impact on the information system's security posture. Any request for changes should describe the impact that the changes will or may have on security. Where changes are expected to increase residual risks, IT operations groups should determine through TRA activities if additional security controls and solutions, or additional changes beyond those that are planned, are required to maintain residual risks at acceptable levels. For important changes, IT operations groups should, under advice of authorizers, request the assistance of security assessors to perform impact assessments. The authorizer, with the assistance of the IT operations group, security practitioners, and security assessors, may decide that some changes are so significant that they require the initiation of a new IT project. Such an IT project should follow the departmental mandated ISSIP process.

To manage changes in a secure manner, departments should consider the following guidelines:

For routine upgrades or changes to information systems:

- Include impact assessments in a formal change request process; and
- Require that change requests be approved by operational authorities.

For major changes to information systems:

- Include impact assessments in a formal change request process;
- Require that change requests be approved by operational authorities and authorizers; and
- Optionally, require that an analysis be conducted by a security assessor.

In support of authorization maintenance (see Section 5.5 of Annex 1 of ITSG-33 [Reference 1]), departments should also require, at a minimum, that the following security activities be conducted when implementing upgrades and changes:

- Conduct security testing and report results where deploying new system components;
- Conduct a vulnerability assessment to ensure that the information system security posture remains unchanged; and
- Update the information system's residual risk assessments or TRA reports to capture the results of impact assessments.

4.2 Monitor and Assess Security

Objectives:	Continuously monitor and assess the performance of implemented security solutions during the operations and maintenance phase of the SLC to ensure that the information system consistently satisfies its security objectives.
Primary role:	For monitoring: IT operations personnel, security practitioners (if an information protection centre (IPC) function exists) For assessment: Security practitioner, (external) security assessor
Supporting roles:	IT security coordinator
Inputs:	Reports from GC lead agencies Threat and vulnerability assessment reports from open sources (4.1-A) Outputs produced during secure operations (4.1-B) Updated information system implementation representation
Outputs:	(4.2-A) Outputs from security monitoring and assessment E.g.: IT security risk management dashboard, security incident reports, TRA reports, vulnerability assessment reports, penetration testing reports, security performance reports, IPC reports.
Security assurance requirements:	As specified in Section 3 for the activities being performed (e.g., VA-E and VA-D in Section 8.4.12 would apply to a vulnerability assessment).

Guidelines:

IT operations groups need to monitor and assess on an ongoing basis the security posture of their information systems in collaboration with the IT security function and a departmental IPC[7], if one exists. Ongoing security monitoring and security assessment are essential processes that help departments detect and respond in a timely manner to attacks, security breaches, and other potentially compromising events and changes within and around the information system's environment. Ongoing security monitoring and security assessment inform the IT security function, as well as incident management, change management, and other operational processes to initiate corrective changes.

To effectively monitor the security posture of their information systems, IT operations groups, in collaboration with security practitioners in the IT security function or an IPC, should perform the following activities:

- Monitor and analyze changes in threats, vulnerabilities, impacts, and risks, and identify the need for changes;
- Monitor the performance and functional effectiveness of security mechanisms and solutions;
- Analyze event records to determine the cause of security events;

[7] The responsibility for the ongoing security monitoring and assessment may be shared between a departmental operations group and an IPC, or assume entirely by the departmental IPC.

- Identify, report, and respond to security incidents; and
- Adequately protect logs, reports, and other security monitoring artefacts.

IT operational groups, in collaboration with the departmental IT security function, need to properly identify security incidents and orchestrate appropriate responses, recovery, and reporting processes and procedures to avoid or limit impacts, recover operations, and inform departmental officials. In some cases, security incident response and recovery may require the coordinated effort of other groups within and outside of the department.

To support departmental IT security risk management activities, ongoing security monitoring and security assessment activities should inform departmental senior officials of the overall performance of the departmental IT security posture. Such links provide the basis for identifying improvement opportunities and implementing IT security function-level changes. See Annex 1 of ITSG-33 [Reference 1] for more information on departmental IT security monitoring and assessment activities.

4.3 Maintain Authorization

Objectives:	Maintain the authorization of the information system during the operations and maintenance phase of the SLC.
Primary role:	Authorizer
Supporting roles:	(External) security assessor, security practitioners
Inputs:	(4.1-A) Outputs produced during the secure operations (4.1-B) Updated information system implementation representation (4.2-A) Outputs from security monitoring and assessment
Outputs:	Authorizer instructions and recommendations
Security assurance requirements:	No specific requirements.

Guidelines:

This activity is performed hand-in-hand with the authorization maintenance activity at the department level. See Annex 1 of ITSG-33 [Reference 1] for detail on this and other departmental IT security risk management activities. It is important for the IT operations groups to keep detailed written records of their security maintenance, administration, monitoring, and security assessment activities, and sufficiently document security-related changes in the information system's environment, security incidents, and all remedial actions. Good operational security documentation simplifies authorization maintenance.

5 Disposal Phase

This section provides guidelines to departments on the secure disposal of IT assets when an information system reaches its end of life.

5.1 Securely Dispose of IT Assets

Objectives:	Securely dispose of IT assets
Primary role:	Security practitioner, system administrator
Supporting roles:	Security assessor
Inputs:	Formal information system disposal request with disposal plan Configuration and asset management records for the information system (3.9.4-A) Security provisions for operations plan
Outputs:	(5.1-A) Disposal report
Security assurance requirements:	No specific requirements

Guidelines:

When an information system reaches its end-of-life and is to be removed from operation, the IT operations group should dispose of sensitive IT assets in accordance with the secure disposal procedures of the operations plan (see Section 3.9.4). Processes and procedures that support this function include:

- Media sanitization;
- Secure media disposal;
- Configuration and asset management; and
- Special security procedures such as the disposal of controlled cryptographic items or TEMPEST equipment.

IT operations groups should produce a disposal report that clearly identifies the IT assets that have been disposed, and the method and authority by which they were disposed. This is especially important for IT media, controlled cryptographic items, and TEMPEST equipment. The disposal report should also identify the data files that were purged, moved, and archived.

5.2 Assess Disposal Results

Objectives:	Confirm that the disposal activities were completed in conformance with the requirements of Section 5.1
Primary role:	(External) Security assessor
Supporting roles:	Security practitioner, system administrator
Inputs:	(5.1-A) Disposal report
Outputs:	(5.2-A) Statement of assessment on disposal activities
Security assurance requirements:	No specific requirements

Guidelines:

Security assessors should review the information system disposal report to confirm that sensitive IT assets have been fully and securely disposed of in accordance with the provisions of the operations plan and any other applicable policies and standards, and submit a statement of assessment to the information system's authorizer. Security assessors should ensure that any deficiencies in the disposal activities are promptly corrected to the satisfaction of the authorizer before issuing the statement of assessment.

5.3 Final signoff

Objectives:	Document the authorizer approval of the disposal activities and the retirement of the information system
Primary role:	Authorizer
Supporting roles:	(External) Security Assessor
Inputs:	(5.2-A) Statement of assessment on disposal activities
Outputs:	(5.3-A) Final sign-off
Security assurance requirements:	No specific requirements

Guidelines:

After reviewing the statement of assessment on disposal activities, authorizers should signify their approval of the information system's retirement. The final sign-off should be forwarded to the IT security function for archiving. Authorizers should also inform owners of the business activities that were relying on the information system by, for example, forwarding to them a copy of the final sign-off.

6 External Capabilities

An IT project is integrating an external capability when it plans to leverage a capability provided by an information system other than the one being implemented by the project. The capability provider in this case can be another organization within the sponsoring department, another department, or a commercial service provider. The decision to use an external capability may be enforced by TBS or the sponsoring department, or may come as a result of requirements or design analysis. Regardless of the reason, IT projects need to determine the set of security requirements that the capability and its provider need to satisfy, and use that set as the basis for acquiring the capability.

An IT project that is integrating an external capability follows the ISSIP described in the previous sections but includes an additional activity: the specification of the security requirements that apply to the external capability. The applicable security requirements will depend on several factors, including: the security assurance requirements, the business needs for security and system-specific security controls that the external capability relates to, and how much influence the IT project or the sponsoring department has on the security posture of the information system of the capability provider. Security requirements may relate to security functionality (e.g., strong end-user authentication), the security of the providers' information systems (e.g., strong incident management internal capability), or the trust that can be placed in the provider's ability to securely deliver the external capability.

Figure 12 shows, in the context of the SDLC, the ISSIP activity for specifying security requirements for an external capability. Inputs to this activity may include:

- Security assurance requirements from the concept phase;
- Business needs for security and system-specific security controls from the requirements analysis phase;
- Other security requirements that may be required for policy or risk management purposes; and
- Security design specifications from the high-level design phase.

Once defined, applicable security requirements serve as input to the procurement process to acquire the external capability from the provider. The type of procurement process is dependent upon whether the provider is internal to the department (e.g., negotiate a memorandum of understanding (MOU)), is another department (e.g., negotiate a formal service level agreement (SLA)), or is a commercial service provider (e.g., issue an RFP). In all cases, the procurement process includes an assessment to ascertain that the external capability satisfies all of the applicable security requirements.

The exact set of ISSIP activities will vary depending on how the external capability will be used. If the external capability is to be integrated in an existing information system, detailed design, development, and integration and testing efforts will be limited to any new components or interfaces that are required in order to make use of the external capability. If the external capability is to be used as a standalone service, the process will likely end at the conclusion of the procurement process.

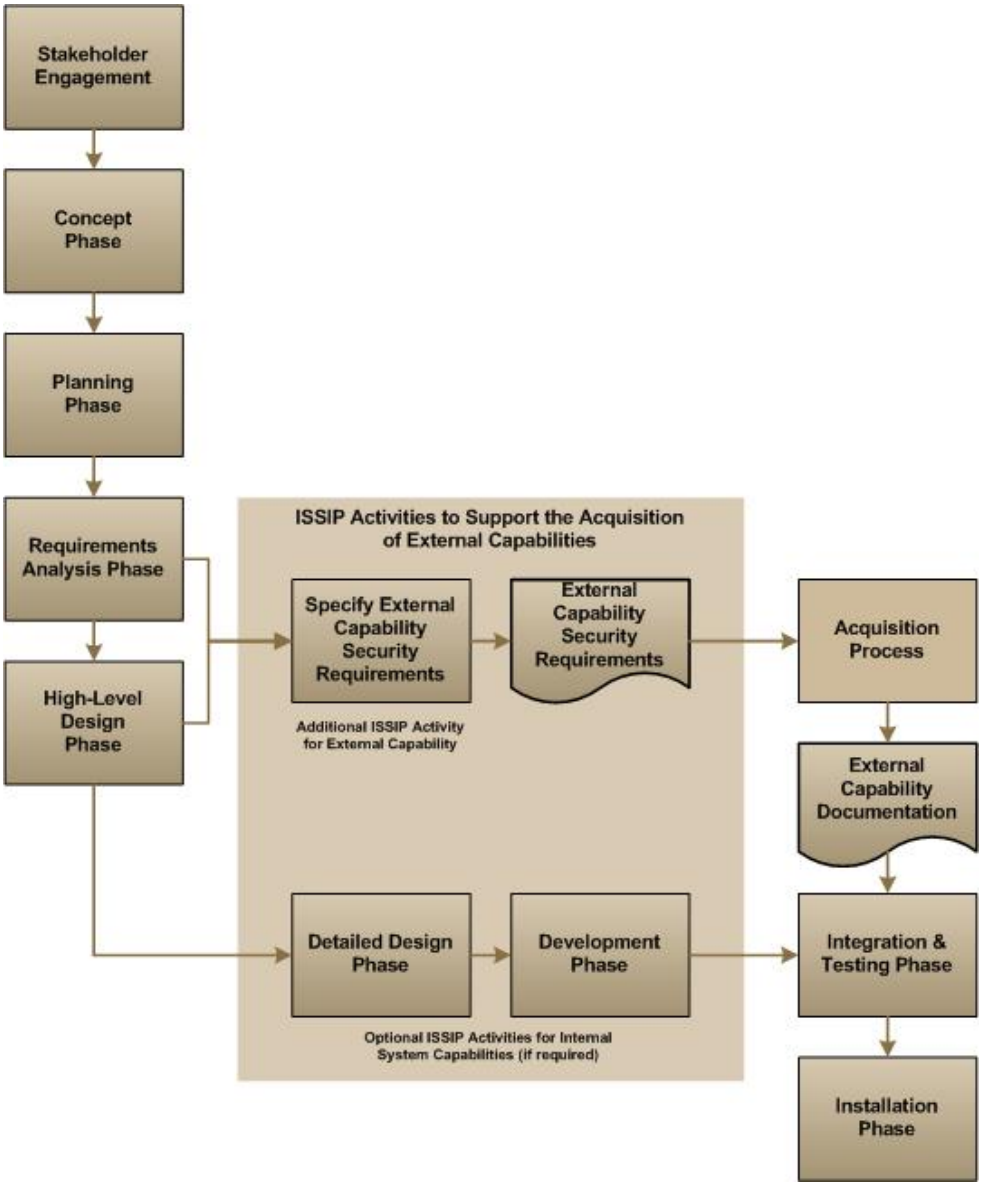


Figure 12: ISSIP Process with External Capability

Departments could also consider using an ISO 27001 [Reference 9] certification as a way to assess the IT security maturity of commercial service providers when procuring external capabilities. However, an ISO 27001 certification alone does not guarantee that the claimed security posture of a commercial service provider's external capability will be fit for purpose. Departments should therefore assess a provider's certification claim along with compliance with other security requirements as part of the bid evaluation process.

6.1 Use of Mandated IT Services

Departments that must use a mandated IT service have to apply a slightly different approach than the one described previously. Departments need to assess the security posture of the service provider's IT service in supporting their specific business activities, in order to either (1) identify additional security controls to be implemented in their environment, or (2) understand the risks they will be accepting.

To successfully carry out such an assessment, departments need to have in place a security risk management program with the following elements:

- An established IT security risk management function meeting the requirements of the PGS [Reference 3] and DDSM [Reference 4] (e.g., a function based on ITSG-33 Annex 1 [Reference 1], ISO 27001 [Reference 9], or NIST 800-39 [Reference 13]) and operating at a level of maturity consistent with the sensitivity and criticality of their programs;
- An established information system security implementation process (i.e., a secure SDLC or a system security engineering process) adequate for the needs of the organization;
- A departmental threat assessment documenting the threats that have been deemed in-scope, and providing a rationale for the threats that have been deemed out of scope or not applicable;
- One or more departmental security control profiles that document the baseline security controls for the information systems supporting departmental business activities. Each profile needs to document the assumptions related to the business, threat, and technological contexts, and applicable security approaches. Each profile should also contain the acceptable residual risk level at which information systems subject to the profile can operate; and
- A continuous monitoring capability capable of analyzing the security posture of information systems, be they internal or external (e.g., those of other GC departments or commercial IT service providers). This capability should include key security performance indicators and metrics to measure success or failure. Security posture analysis includes, for example, results of:
    - Periodic security assessments (e.g., assessment of backup infrastructure and related practices, verification of the configuration of a malware detection service, vulnerability analysis of a common authentication service);
    - Periodic reviews of incident reports (e.g., a server was compromised and data exfiltrated, the server was sanitized and rebuilt from a secure baseline, the vulnerability has been patched, and additional monitoring has been put in place);
    - Periodic reviews of security-related events (e.g., log data show an unusual amount of failed login attempts to a database); and
    - Periodic assessments of operational staff security-related activities (e.g., administrators using their privileged accounts for administrative tasks exclusively and not for surfing the web).

Having these key elements in place, departments should be able to assess a mandated IT service, assuming access to the following information:

- A detailed description of the provider's risk management function. For example:
    - The service provider does not have a documented function;

  - The service provider does have a documented function, however it is not executed consistently; or
  - The service provider does have a documented process and it is certified by an external auditor (e.g., ISO 27001 certification).

- A detailed description of the provider's information system security implementation process. For example:
  - The service provider does not have a documented process;
  - The service provider does have a documented process, however it is not applied consistently; or
  - The service provider does have a documented process and is able to prove that it has applied the process rigorously during the implementation of the mandated IT service.
- A detailed threat assessment. For example:
  - The service provider does not have a documented threat assessment;
  - The service provider has a documented threat assessment, however it was not leveraged substantially during the establishment of the risk management function and during the implementation of the mandated IT service; or
  - The service provider has a documented threat assessment and is able to prove that it was leveraged significantly during the establishment of the risk management function and during the implementation of the mandated IT service.
- One or more security control profiles. For example:
  - The service provider does not have a documented security control profile (or equivalent security requirements specification);
  - The service provider has a documented security control profile, however it was only partially implemented during the establishment of the risk management function and during the implementation of the mandated IT service; or
  - The service provider has a documented security control profile and is able to prove that it was substantially implemented during the establishment of the risk management function and during the implementation of the mandated IT service. All security controls not currently implemented are documented, a rationale for the reason is provided, and a plan for implementation, if required, is provided.
- Detailed security-related information required to perform a security posture analysis of the mandated IT service. For example:
  - Assessment reports of the mandated IT service's security controls are available on a periodic basis and when required (e.g., after an incident);
  - Reports are provided promptly for all related incidents;
  - Reports are provided promptly for all related security-related events; or

- Assessment reports of operational staff security-related activities are available on a periodic basis and when required (e.g., after an incident or a major change in the provider's infrastructure).

Departments can assess the adequacy of the security posture of an IT service by comparing key elements of its departmental IT security risk management function (i.e., risk management process, information system security implementation process, threat assessment, security controls profiles, monitoring and analytical capability, which includes key security performance indicators and metrics) with the security-related information provided above.

If the key elements and the provided security-related information align and compare favourably, departments may conclude that the IT service's security posture is adequate to support the department's business activities at the documented level of acceptable residual risk.

If the departmental IT security function has not produced these key elements, or produced them only partially, the evaluation cannot be performed conclusively. The same is true if the service provider cannot provide the required information, or if the information is inadequate. In this case, no definitive conclusion can be drawn on the adequacy of the IT service's security posture to support the department's business activities.

7 Determining a Robustness Level

7.1 Introduction

Throughout the ISSIP process, the security practitioner is required to identify required robustness level for various security controls. This section defines the concept of robustness, describes a robustness model[8], and provides a methodology for determining an appropriate robustness level for a security control (or a set of security controls). This methodology equips security practitioners with a consistent way of designing and implementing appropriate security solutions to protect information systems.

7.2 Robustness

Robustness is a characterization of the security *strength* and *assurance* of a security control. The security strength is related to the control's potential ability to protect the confidentiality, integrity, or availability of IT assets. The security assurance of a control is related to confidence that the control is designed and implemented correctly, and is operating as intended. Together, these two aspects define the requirements that must be met in the implementation of a control to satisfy its security objective. For example, a security control that is conceptually strong (e.g. an encryption algorithm using the Advanced Encryption Standard) but comes with no assurance (e.g. there is no evidence to show that the algorithm is coded correctly) will have a lower effective robustness than a similar control that does have higher assurance (e.g. the software has been validated).

Security controls that protect more sensitive or critical IT assets or that are exposed to more significant threats will generally require stronger security solutions and require more assurance in their implementation and therefore require higher levels of robustness. The robustness model defines a hierarchy of robustness levels that are based on expected injury levels and the capabilities or magnitude of the threats.

7.3 Components of Robustness Model

Table 4 defines a robustness model in terms of five robustness levels (R1 to R5) and the associated strength and assurance requirements for each level. These five robustness levels have been tailored to counter a defined set of threat categories (presented in Section 7.4.2).

Although five levels of robustness are defined in this model, not all robustness levels are necessarily applicable to each security control (i.e., some controls such as backup or auditing may not have an implementation at a Level 4 or 5). The requirements for the security strength component are specific to each individual security control. The requirements for the security assurance component are generally the same across security controls of the same robustness level.

[8] The CSEC robustness model is based upon an approach developed by the National Security Agency (NSA), documented in Section 4 (Technical Security Countermeasures) of the *Information Assurance Technical Framework* (IATF) [Reference 10].

Table 4: Robustness Level Definitions

Robustness		Security Strength	Security Assurance	
			Level	Description
Low	**R1**	Basic strength. For deliberate threats, resistant to unsophisticated threats (comparable to Td1 to Td3 categories), but it is expected that more sophisticated attacks will succeed in compromising the protected IT assets.	SAL 1	Low level of assured security is required.
	R2	For accidental and natural hazard threats, resistant to threat events of categories Ta1 and Ta2, but it is expected that threat events of higher magnitude will compromise the protected IT assets.	SAL 2	Moderate level of assured security is required.
Medium	**R3**	Medium strength. For deliberate threats, resistant to sophisticated threats (comparable to Td4 and Td5 categories), but it is expected that some sophisticated attacks will succeed in compromising the protected IT assets. These controls would typically counter a threat from an organized effort (e.g., an organized group of hackers). For accidental and natural hazard threats, resistant to threat events of categories Ta3 and Ta4, but it is expected that threat events of high magnitude will compromise the protected IT assets.	SAL 3	Best commercial level of assured security is required, and developers or users are prepared to incur additional security-specific design costs.
High	**R4**	High strength or high grade. For deliberate threats, resistant to the most sophisticated threats (comparable to Td6 and Td7 categories), and there should not be any reasonable way for attacks to succeed in compromising the IT assets. They are resistant to the national laboratory or nation-state threats.	SAL 4	*Currently out of scope*
	R5	For accidental and natural hazard threats, resistant to threats events of category Ta5, and only vulnerable to threat events of catastrophic proportions.	SAL 5	*Currently out of scope*

Each robustness level in Table 4 is associated with one of three main categories. These include Low, Medium, and High Robustness. Additionally, each individual robustness level, R1 to R5, is composed of a security strength component and a security assurance component:

- **Security strength** – The characterization of an implemented security control's potential[9] to protect the confidentiality, integrity and availability of IT assets against threat agent capabilities, natural hazards or accidental events. As the strength increases, the effort (cost) or magnitude required by the threat agent to defeat the implemented control also increases.

[9] Note that the protective potential of a security control can be fulfilled only when it is implemented with adequate security assurance.

- **Security assurance** – Confidence-building tasks that aim to ensure that a security control is designed and implemented correctly, and is operating as intended. In addition, security assurance includes tasks that aim to ensure the ability of all security controls in an information system's security design, implementation and operations to satisfy the business needs for security.

Each of these aspects of robustness is described in detail in the following subsections.

7.3.1 Security Strength Level

The security strength of a control at a certain robustness level is a function of the specific design criteria and mechanisms implementing the control. As shown in Table 4, the security strength can range in level from basic strength to high grade, and each aims to counter one or more categories of threat capability. These capabilities (T1 to T7) are defined in Section 7.4.2 and include deliberate and accidental threats.

A security control (e.g., authentication, authorization) is implemented using one or more security mechanisms (e.g., one-time password, access control lists). The strength of a control, and the mechanism(s) implementing it, is a function of the design criteria applied to counter the identified threat agent capabilities and their associated attack methods, or to the identified natural hazards or accidental events. Note that strength is a relative measure of the effort (cost) or magnitude required to defeat or compromise the security control and is not related to the cost of implementing it.

It is the intent of the robustness model to ensure that security controls at the same strength level provide comparable protection, in that they counter equivalent threats. However, selecting the same strength level for all security controls does not ensure that the whole system and its security will operate at that level. An overall system security engineering analysis is required to assess the actual strength of the complete solution.

The design criteria required to implement a security control at a certain level of strength are specified in security control guidance publications such as ITSG-31 – *User Authentication Guidance for IT Systems* [Reference 8]. Refer to CSE's web site (www.cse-cst.gc.ca/its-sti/publications/index-eng.html) for a list of current guidance publications.

7.3.2 Security Assurance Level

The security assurance of a control (or set of controls) at a certain robustness level is defined by a set of tasks to be performed during implementation, providing the assurance that security controls meet the expected objectives.

Each robustness level has a security assurance component, identified by a specific security assurance level (SAL), which can range from low security assurance (SAL1) to very high security assurance (SAL5). The security assurance levels defined in this publication are as follows:

- **SAL1** – A low level of assured security is required;
- **SAL2** – A moderate level of assured security is required; and
- **SAL3** – The best commercial level of assured security in conventional products is required; developers or users are prepared to incur additional security-specific design costs.

SAL4 and SAL5 are currently out of scope of this publication[10]. Security assurance levels are further defined in Section 8 of this publication.

Security assurance is provided through tasks completed by information system developers, implementers, and security assessors. Assurance is increased through the additional effort in one or more of the following areas:

- **Better design practices** – Use of modular design, clear interfaces definition, loose coupling of functions, and other design practices which improve the quality of the design. Higher levels of development process maturity provide for the use of better design practices[11];
- **Better documentation** – Complete, accurate, and well-managed design documentation which improves the quality of information system implementation, and decreases the likelihood of errors and omissions;
- **Scope** – The design and assessment efforts are broader in scope (e.g., including details of subsystems rather than simple interfaces increases assurance for the overall system);
- **Depth** – The design and assessment efforts are greater because they are performed to a finer level of detail; and
- **Rigour** – The design and assessment efforts are greater because they are performed in a more structured, formal manner.

These assurance tasks can ensure, for example, that business needs for security are justified; that the set of selected security controls satisfies business needs for security; and that the security controls are designed and implemented correctly and are operating as intended. The goal is to apply the effort required to provide the necessary level of security assurance.

7.3.2.1 Trust in Supplier/Developer

In addition to the previous elements of security assurance, suppliers providing security designs, products, and solutions should be trusted. As the injury level and the category of threat agent capabilities and magnitude of event increase (and accordingly, the required level of robustness), the trust required in the supplier also increases.

Departments can establish trust in suppliers in part through the GC contract bidding process by completing a Security Requirements Checklist (SRCL) form, which is issued with bid solicitation documents. By using a SRCL, departments can establish as a mandatory requirement that a supplier comply with the Industrial Security Program requirements. This program is managed by PWGSC.

Through this program, PWGSC can either issue a designated organization screening at the Protected A, Protected B, or Protected C level, or a facility security clearance at the Confidential, Secret, Top Secret, NATO Confidential, or NATO Secret level. Depending on the level sought, the process may include an assessment to establish that the company is not under adverse foreign influence, the formal appointment and security screening of a company security officer, the security screening of key senior officials, the security screening of employees and subcontractors, a physical security assessment, etc. This program

[10] Contact CSEC IT Security Client Services for guidance regarding assurance levels SAL4 and SAL5.

[11] For example, see Software *Engineering Institute - Capability Maturity Model Integration*, www.sei.cmu.edu and *System Security Engineering – Capability Maturity Model*, www.sse-cmm.org.

establishes assurance in the loyalty and the integrity of a company and its workforce in serving the Government of Canada and is therefore an important element of trust.

For assurance levels SAL1 to SAL3, the supplier should hold, as a minimum, a designated organization screening. For assurance levels SAL4 and SAL5, the supplier should hold a facility security clearance. The level of screening or clearance should be determined by a TRA, and should take into account the specified role of the supplier and the knowledge that they will gain concerning the information system. It is recommended that departments set a departmental standard in this regard to ensure consistency. In general, development work requiring higher levels of assurance (SAL4 and above) should have suppliers with at least a Secret facility security clearance.

7.4 Determine a Cost-effective Robustness Level

7.4.1 Determine Injury Levels

The first step in determining a cost-effective robustness level for a security control is to determine the injury levels associated with the IT assets that the security control will be protecting. As explained in Section 3.5.1.2, injury levels for the security objectives of confidentiality, integrity, and availability are linked to the security category of the business activities that the IT assets will support.

However, many security controls protect IT assets against a compromise of two or three of these security objectives simultaneously (e.g., access control). In most cases, it is recommended to take the high watermark of the three injury levels to determine robustness. For example, an IT asset that will support a business activity with injury levels of (Protected B, High Integrity, Low Availability) would yield a high watermark injury level of high.

For the purpose of selecting a robustness level, injury levels are identified as I1 to I5, which correspond to the levels of very low to very high.

7.4.2 Determine Category of Threat Agent Capabilities and Magnitude of Event

The second step in determining a cost-effective robustness level is to select a relevant deliberate threat category using Table 5, and the relevant magnitude of events for accidental or natural threats using Table 6. The input to this process is the threat assessment report, which should normally be validated at the beginning of the concept phase of the SDLC (see Section 3.2.1).

The threat categories defined in these tables represent an increasing level of threat agent capabilities and magnitude of accidental threats and natural hazards. Note that as threat agent capabilities evolve over time, the examples provided in this table will be updated. As this table contains only examples, departmental threat assessments should document current information on threat agent capabilities relevant to the organization.

Table 5: Deliberate Threat Category Descriptions and Examples

Threat Category	Threat Agent	Examples of Increasing Threat Agent Capabilities
Td1	Non-malicious adversary (e.g., non-malicious unauthorized browsing, modification, or destruction of information due to lack of training, concern, or attentiveness)	• Basic end user capabilities to access information systems and contents
Td2	Passive, casual adversary with minimal resources who is willing to take little risk (e.g., listening, *script kiddie*)	• Execution of a publicly available vulnerability scanner • Execution of scripts to attack servers • Attempts to randomly delete system files • Modification of configuration file settings
Td3	Adversary with minimal resources who is willing to take significant risk (e.g., unsophisticated hackers)	• Use of publicly available hacker tools to run various exploits • Insiders installing trojans and key loggers on unprotected systems • Use of simple phishing attacks to compromise targets with malware • Execution of programs to crash computers and applications
Td4	Sophisticated adversary with moderate resources who is willing to take little risk (e.g., organized crime, sophisticated hackers, international corporations)	• Sophisticated use of publicly available hacker tools, including 0-day exploits • Ability to create own attack tools in software • Basic social engineering attacks • Ability to assemble hardware using commercial-off-the-shelf (COTS) components to facilitate attacks • Phishing attacks to gain access to credit card or personal data
Td5	Sophisticated adversary with moderate resources who is willing to take significant risk (e.g., organized crime, international terrorists)	• Bribery of insiders to get information • Modification or fraudulent use of commercial products to support financial gain (e.g., tampered or bogus ATM cash machines) • Physical destruction of infrastructure • Side-channel attacks (e.g. power analysis attacks on smart cards)
Td6	Extremely sophisticated adversary with abundant resources who is willing to take little risk (e.g., well-funded national laboratory, nation-state, international corporation)	• TEMPEST attacks • Supply chain attacks, such as tampering of or fraudulent commercial products to support espionage (e.g., tampered network routers or firewalls) • Hard to detect implant technologies in hardware or software • Exploitation of non-public vulnerabilities
Td7	Extremely sophisticated adversary with abundant resources who is willing to take extreme risk (e.g., nation-states in time of crisis)	• Blackmail or intimidation of insiders to compromise system security • Penetration of secure facilities to enable attacks

Table 6: Accidental Threat and Natural Hazard Category Descriptions

Threat Category	Magnitude of Event
Ta1	• Minor accidental events (e.g., trip over a power cord, enter wrong information)
Ta2	• Moderate accidental events (e.g., render server inoperable, database corruption, release information to wrong individual or organization) • Minor hardware or software failures (e.g., hard disk failure) • Minor mechanical failures (e.g., power failure within a section of a facility) • Minor natural hazards (e.g., localized flooding, earthquake compromising part of a facility)
Ta3	• Serious inadvertent or accidental events (e.g., cut facility telecommunications or power cables, fire in a facility, large scale database corruption) • Moderate mechanical failures (e.g., long term facility power failure) • Moderate natural hazards (e.g., localized flooding or earthquake compromising a facility)
Ta4	• Serious mechanical failures (e.g., long term, city-wide power failure) • Serious natural hazards (e.g., earthquake with city-wide devastation)
Ta5	• Very serious mechanical failures (e.g., long term, regional power failure) • Very serious natural hazard (e.g., earthquake with regional or national devastation)

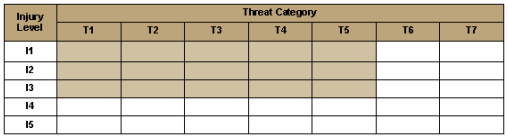
7.4.3 Determine Robustness Level

To determine a cost-effective robustness level for a security control (or set of security controls with similar requirements), security practitioners select from Table 7 the level of robustness corresponding to the assessed injury level (I1 – I5) and threat category (T1 - T7) related to the security control(s). The recommended robustness levels aim to mitigate the specified threat agent capabilities (deliberate threat agents) and magnitude of events (accidental and natural hazards) to achieve ***low*** residual risks for the security objectives of confidentiality, integrity and availability.

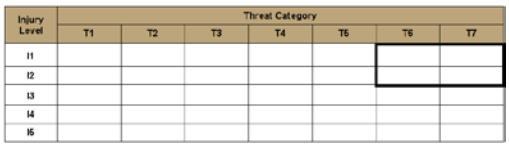
Table 7: Recommended Cost-effective Robustness Level to Achieve Low Residual Risks

Injury Level	Threat Category						
	T1	**T2**	**T3**	**T4**	**T5**	**T6**	**T7**
I1	R1	R1	R1	R2	R2	*R4*	*R4*
I2	R1	R1	R1	R2	R2	*R4*	*R4*
I3	R1	R1	R2	R3	R3	R4	R4
I4	*R1*	*R2*	*R3*	*R3*	*R3*	R4	R5
I5	*R1*	*R2*	*R3*	*R3*	R4	R5	R5

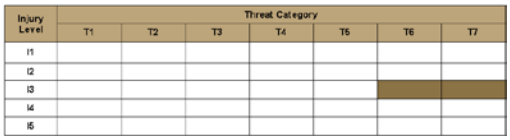
7.4.3.1 Table Description and Rationale



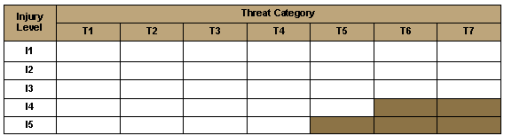
The light brown shaded cells in Table 7 (I1-T1 to I3-T5) represent typical scenarios where the IT assets being protected are supporting business activities of a security category of very low to medium injury levels (i.e., Confidential, Protected B, and lower; medium to low integrity or availability), where the threat category is assessed at a low to high level. The recommended robustness levels range from R1 to R3, which are typically associated with low-end to high-end COTS security solutions.



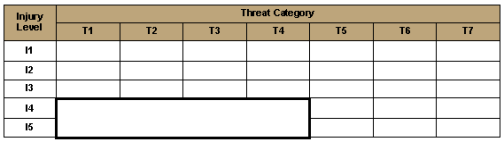
The white cells in italic text (I1-T6 to I2-T7) represent scenarios where IT assets being protected are supporting business activities of a security category of very low to low injury levels (i.e., Unclassified and Protected A information, very low to low integrity and availability), where the threat category is assessed at a very high level. The minimum robustness level required to mitigate extremely sophisticated threats (e.g., nation-state foreign intelligence services) is R4, which is typically associated with government-off-the-shelf (GOTS) medium to high grade security solutions. However, in this case, the cost is usually considered prohibitive given the low sensitivity of the IT assets to be protected, and as such a lower level of robustness (e.g., R2) is typically selected. By doing so, extremely sophisticated threats will not be countered, and the resulting risk is formally accepted.



The dark shaded cells (I3-T6 and I3-T7) represent scenarios where the IT assets being protected are supporting business activities of a security category of medium injury level typically related to the processing of Confidential information, where the threat category is assessed at a very high level. The recommended robustness level is R4, which is typically associated with government-off-the-shelf (GOTS) medium to high grade security solutions. In the case of Confidential information, R4 is recommended to align with foreign partners and NATO alliance agreements. It is recommended that any systems processing classified information, implemented for military or NATO use, should be built to mitigate the T7 threat category.



The dark shaded cells (I4-T6, I4-T7, I5-T5 to I5-T7) represent typical scenarios where the IT assets being protected are supporting business activities of a security category of high to very high injury levels (i.e., Protected C, Secret, and Top Secret; high to very high integrity or availability), and where the threat category is assessed at a high to very high level. The recommended robustness levels range from R4 to R5, which are typically associated with GOTS high grade security solutions, including Type 1 crypto solutions. For these high injury levels and threat categories, risk mitigation using only lower robustness controls is not recommended. Note that CSE COMSEC policies apply when protecting classified information.



The white cells with italic text (I4-T1 to I5-T4) represent typical scenarios where the IT assets being protected are supporting business activities of a security category of high injury level (i.e., Protected C, Secret, and Top Secret; high to very high integrity or availability), and where the threat category is assessed at a low to medium level. An example of such scenarios is the assessed internal threat

of a physically segregated, dedicated system-high environment[12] with appropriately cleared users not connected to systems of lower classification (including the Internet), and protected with adequate physical security. It is important when selecting these robustness levels for internal security controls to be careful that the assessed threat category is really of low to medium level (e.g., basic to sophisticated threat capabilities, explicitly excluding extremely sophisticated capabilities). Known insider threats, unusual operational environments (e.g., Canadian embassy located in a hostile country) or a porous perimeter (e.g., uncontrolled USB ports) will greatly influence the assessed threat category.

Injury Level	Threat Category						
	T1	T2	T3	T4	T5	T6	T7
I1							
I2							
I3							
I4							
I5							

The cell (I4-T5) represents a scenario where the IT assets being protected are supporting business activities of a security category of high injury level (i.e., Protected C, Secret, high integrity or availability), and where the threat category is assessed at a sophisticated level. This scenario could include law enforcement or counter-terrorism information systems processing information requiring protection from organized crime threats, for example. Nation-state extremely sophisticated threats would have been deemed out of scope because this information is already shared with many international organizations, for example. In this case, the use of high-end COTS or low grade GOTS security solutions could be considered.

Table 8 provides examples of typical information systems and an assessment of the required robustness level of key security controls for these systems (some security controls' robustness level might be lower, depending on the security design. Refer to the explanatory text of cells (I4-T1 to I5-T4) in Table 7 above for such an example). Since the examples in Table 8 are for illustrative purposes, only deliberate threats are considered.

[12] A dedicated system-high environment is an IT system where all users are cleared to the highest classification stored or processed by the system, have formal access approval and a need-to-know for all data.

Table 8: Simple Examples of Security Control Robustness Level Determination (Considering only Deliberate Threats)

Example Information System	Description	Key Security Controls Robustness Level	
		Determination	Level
Unclassified Wiki server in a departmental restricted zone	• Server serves unclassified wiki pages with low integrity and availability requirements. • Server is not connected or accessible to any external or public networks, including the Internet.	The expected injury level is assessed as very low (I1). The threat environment is assessed as very low (Td1).	R1
GC departmental network	• GC departmental network containing low sensitivity business office and collaboration applications and a few custom applications. • Public servants have access to the Internet.	The expected injury level is assessed as low (I2). The threat environment is assessed as medium (Td4).	R2
Transaction-based web application (non-critical)	Web application serves a large community of users and delivers on-line GC services (e.g., a job bank where potential candidates can submit and update their resumes).	The expected injury level is assesses as low (I2). The threat environment is assessed as medium (Td4).	
Transaction-based web application (mission critical)	Web application serves a large community of users and delivers on-line GC services (e.g., financial- or health- related transactions).	The expected injury level is assessed as medium (I3). The threat environment is assessed as medium (Td4 to Td5).	R3
Collaboration application for sharing Secret information among law enforcement agencies	• Collaboration application (email, white-boarding, instant messaging, etc.) used by law enforcement personnel to exchange Secret information. • The collaboration application is running within a protected enclave.	The expected injury level is assessed as high (I4). The threat environment is assessed as medium (Td5).	
Nuclear power-plant control system	• The system controls all aspects of the power-plant generation process. • The control system is not directly connected to outside networks; however, users have access to internet-connected computers in the control room.	The expected injury level is assessed as very high (I5). The threat environment is assessed as medium (Td5).	R4
Information transfer between Top Secret and Protected domains	A cross-domain solution is used to transfer data between a Top Secret and a Protected domain.	The expected injury level is assessed as very high (I5). The threat environment is assessed as high (Td6).	R5
Information transfer of military Top Secret information	Top Secret military information is transferred between a base located in hostile territory and Ottawa HQ over a satellite link.	The expected injury level is assessed as very high (I5). The threat environment is assessed as high (Td7).	

7.5 Failure to Satisfy Robustness Requirements

When implementing a security control, it is possible that an IT project will elect for a lower robustness level than what is required, or not to implement some of the recommended robustness requirements. This will decrease the effectiveness of the implemented security control in mitigating selected threats. The reasons may include, but are not limited to, prohibitive cost, lack of a commercially available solution with the appropriate features, or operational urgency. The rationale for such a decision should be documented as part of the TRA activities, and to permit re-examination of the robustness selection if circumstances change in the future.

8 Security Assurance Requirements

8.1 Introduction

This section defines security assurance requirements for IT projects. They are grouped under 13 topics based on their objectives. A security assurance level (SAL) consists of a pre-selected set of security assurance requirements that yields an incremental degree of confidence in the adequacy of the security engineering and documentation work performed by the project team, and ultimately that the implemented security controls perform as intended and satisfy the business needs for security. This section currently defines security assurance levels 1 to 3. Definitions of security assurance levels 4 and 5 are currently out of scope[13].

Each security assurance requirement consists of engineering tasks, documentation content requirements, and assessment tasks to be completed as part of the IT project. Within the context of security assurance, an engineering task is an action that relates to an engineering aspect of security (e.g., selecting and documenting system security controls in security control specifications). A documentation content requirement specifies the structure and contents of an engineering task output or outputs (e.g., the amount of detail in describing security controls in a security control specification). An assessment task is an action for determining if an engineering task and its outputs meet the security assurance requirements (e.g., verifying that security controls are in fact described in sufficient detail in a security control specification).

An assessment task includes all steps that the security assessor takes to ensure that the IT project corrects any deficiency in the execution of engineering tasks and their documentation outputs, as well as the steps to confirm that these corrective actions have been completed. This essentially makes the process of correcting engineering and documentation deficiencies an integral part of each assessment task. By following these practices, IT projects can resolve security assurance issues as they are discovered by the security assessor, and thus ensure that security assurance targets are met at the conclusion of each phase.

There is always the possibility for project authorities to decide not to implement a security assessor's recommendation. For example, the authorizer may find a security assessor's recommendation to implement an additional security control to better mitigate a specific threat to be cost-prohibitive and may decide to accept the risk instead. Security assessors should ensure that statements of assessment reflect such decisions and any impact that they may have on residual risks.

Security assurance requirements vary in rigour as the security assurance level increases. The rigour of a security assurance requirement relates to the effort invested in carrying out the task. For example, there may be a requirement to formally document security controls, and an additional requirement to include in the specification the reason why each security control satisfies its corresponding business needs for security (i.e., produce a security control rationale), a more rigorous engineering task.

[13] Contact CSEC IT Security Client Services for guidance regarding assurance levels SAL4 and SAL5.

The 13 security assurance requirement topics and their objectives are as follows:

- **Business needs for security** – Establish that the business needs for security for the information system have been correctly defined;
- **Security control specification** – Establish that security controls have been correctly defined and that they satisfy their business needs for security;
- **Design specifications** – Establish that the security design of the information system design satisfies all security controls;
- **Threat and risk assessment** – Establish that the security design of the information system adequately mitigates threats;
- **Change management during development** – Establish that the management of information system elements (e.g., application source code) during development is performed adequately;
- **Development environment security measures** – Establish that the security of the development environment is adequate (e.g., protecting against unauthorized changes to source code);
- **Development tools** – Establish that the selection and use of appropriate development tools is adequate (e.g., COTS versus open source development tools, ensuring that only authorized tools are used);
- **Secure development practices** – Establish that the information system was developed following secure practices (e.g., use of source code analysis tools and techniques, source code review, robust programming practices);
- **Security testing** – Establish that the security solutions satisfy design requirements, have been implemented correctly, and are operating as expected;
- **Operational security procedures** – Establish that the secure use, administration, and maintenance of the information system during its operational period will be performed adequately;
- **Security installation procedures** – Establish that the information system can be installed in a secure manner in the production environment;
- **Vulnerability assessment** – Establish that the information system is free of vulnerabilities or that vulnerabilities have otherwise been mitigated to an acceptable level of residual risk; and
- **Security installation verification** – Establish that information system security has been installed and configured correctly in the production environment.

8.2 Usage

Table 9 provides the set of security assurance requirements suggested to be used during an IT project, depending on the analysis performed during the concept phase of the IT project. This set of security assurance requirements can be refined during the high-level and detailed design phases to address specific security design requirements.

8.3 Definitions of Security Assurance Levels

During the concept phase of the ISSIP, IT project managers and security practitioners specify the appropriate level of effort required (linked to the robustness required from the security controls) to ensure the secure design, development, installation, and operations of information systems (Section 3.2.3). To help specify that level of effort, Table 9 defines security assurance levels 1 to 3 by allocating security assurance requirements to each of the security assurance levels. These levels are pre-packaged, suggested assurance requirements appropriate for IT projects requiring rudimentary to high assurance in the implementation of security controls. The security assurance requirements are defined in the next section.

Note that domain security control profiles should suggest a security assurance level for the implementation of security controls to help IT projects specify the appropriate security assurance requirements.

Table 9: Definitions of Security Assurance Levels 1 to 3

ID	Security Assurance Topic	Security Assurance Levels			
		Task Type	SAL1	SAL2	SAL3
BNS	Business Needs for Security	Engineering	BNS-E-1	BNS-E-1	BNS-E-1 BNS-E-2
		Documentation Content	BNS-D-1 BNS-D-2	BNS-D-1 BNS-D-2	BNS-D-1 BNS-D-2
		Assessment	BNS-A-1	BNS-A-1	BNS-A-1
SCS	Security Control Specification	Engineering	SCS-E-1	SCS-E-1	SCS-E-1 SCS-E-2
		Documentation Content	SCS-D-1 SCS-D-2	SCS-D-1 SCS-D-2	SCS-D-1 SCS-D-2 SCS-D-3 SCS-D-4
		Assessment	SCS-A-1	SCS-A-1	SCS-A-1
DS	Design Specifications	Engineering	DS-E-1	DS-E-1	DS-E-1
		Documentation Content	DS-D-1 DS-D-2	DS-D-1 DS-D-2	DS-D-1 DS-D-2
		Assessment	DS-A-1 DS-A-2	DS-A-1 DS-A-2	DS-A-1 DS-A-2
TRA	Threat and Risk Assessment	Engineering	TRA-E-1	TRA-E-1	TRA-E-1 TRA-E-2
		Documentation Content	TRA-D-1 TRA-D-2	TRA-D-1 TRA-D-2 TRA-D-3	TRA-D-1 TRA-D-2 TRA-D-3
		Assessment	TRA-A-1	TRA-A-1	TRA-A-1
CM	Change Management During Development	Engineering		CM-E-1 CM-E-2 CM-E-3 CM-E-4	CM-E-1 CM-E-2 CM-E-3 CM-E-5

ID	Security Assurance Topic	Security Assurance Levels			
		Task Type	**SAL1**	**SAL2**	**SAL3**
		Documentation Content		CM-D-1 CM-D-2	CM-D-1 CM-D-2 CM-D-3 CM-D-4 CM-D-5
		Assessment		CM-A-1 CM-A-2	CM-A-1 CM-A-2 CM-A-3
SM	Development Environment Security Measures	Engineering		SM-E-1	SM-E-1 SM-E-2
		Documentation Content			SM-D-1
		Assessment		SM-A-1	SM-A-1 SM-A-2
DT	Development Tools	Engineering	DT-E-1	DT-E-1	DT-E-1 DT-E-2
		Documentation Content			DT-D-1 DT-D-2 DT-D-3
		Assessment	DT-A-1	DT-A-1	DT-A-1 DT-A-2
SDP	Secure Development Practices	Engineering	SDP-E-1	SPD-E-1 SPD-E-2	SPD-E-1 SPD-E-2
		Documentation Content		SDP-D-1	SDP-D-1
		Assessment	SDP-A-1	SDP-A-1 SDP-A-2	SDP-A-1 SDP-A-2
ST	Security Testing	Engineering	ST-E-1 ST-E-2	ST-E-1 ST-E-2	ST-E-1 ST-E-2 ST-E-3
		Documentation Content	ST-D-1 ST-D-2 ST-D-3	ST-D-1 ST-D-2 ST-D-3	ST-D-1 ST-D-2 ST-D-3 ST-D-4
		Assessment	ST-A-1	ST-A-1	ST-A-1
OSP	Operational Security Procedures	Engineering	OSP-E-1	OSP-E-1	OSP-E-1
		Documentation Content	OSP-D-1	OSP-D-1 OSP-D-2	OSP-D-1 OSP-D-2 OSP-D-3
		Assessment	OSP-A-1	OSP-A-1	OSP-A-1

ID	Security Assurance Topic	Security Assurance Levels			
		Task Type	SAL1	SAL2	SAL3
SIP	Security Installation Procedures	Engineering	SIP-E-1	SIP-E-1	SIP-E-1
		Documentation Content	SIP-D-1	SIP-D-1	SIP-D-1
		Assessment	SIP-A-1	SIP-A-1	SIP-A-1
VA	Vulnerability Assessment	Engineering	VA-E-1 VA-E-4	VA-E-1 VA-E-2 VA-E-4 VA-E-5	VA-E-1 VA-E-2 VA-E-3 VA-E-4 VA-E-5
		Documentation Content		VA-D-1	VA-D-1
		Assessment		VA-A-1	VA-A-1 VA-A-2
SIV	Security Installation Verification	Engineering	SIV-E-1 SIV-E-3	SIV-E-2 SIV-E-3 SIV-E-4	SIV-E-2 SIV-E-3 SIV-E-4
		Documentation Content		SIV-D-1	SIV-D-1
		Assessment	SIV-A-1	SIV-A-1 SIV-A-2	SIV-A-1 SIV-A-2

8.4 Definitions of Security Assurance Requirements

8.4.1 BNS - Business Needs for Security

Objective:

The business needs for security form a concise statement, in business terms, of the security needs of the business processes and related information that the information system supports.

Engineering Tasks:

BNS-E-1 The security practitioner shall produce a statement of business needs for security.

BNS-E-2 The security practitioner shall produce a business needs for security rationale.

Documentation Content Requirements:

BNS-D-1 The statement of business needs for security shall describe all security needs relating to the business processes and information.

BNS-D-2 The statement of business needs for security shall trace each business need to the organizational objectives that it supports (e.g., policy, legal, or contractual obligations).

Assessment Tasks:

BNS-A-1 The security assessor shall confirm that the information produced meets all documentation content requirements.

8.4.2 SCS - Security Control Specification

Objective:

The security control specification forms a clear, unambiguous, and well-defined description of applicable security controls.

Engineering Tasks:

SCS-E-1 The security practitioner shall produce a security control specification.

SCS-E-2 The security practitioner shall produce a security control rationale.

Documentation Content Requirements:

SCS-D-1 The security control specification shall describe the security controls in sufficient detail to allow for their allocation during design phases, and in an unambiguous manner to guide the detailed designer.

SCS-D-2 The security control specification shall trace security controls to the business needs for security that they satisfy (e.g., SRTM).

SCS-D-3 All subjects, objects, operations, security attributes, external entities, and other terms that are used in the security control specification shall be defined.

SCS-D-4 Each business need for security shall be satisfied. Deviations shall be justified in a security control rationale.

Assessment Tasks:

SCS-A-1 The security assessor shall confirm that the information produced meets all documentation content requirements.

8.4.3 DS - Design Specifications

Objective:

The design specifications satisfy all the security controls. The design specification is used to guide the implementation of the information system.

Engineering Tasks:

DS-E-1 The security practitioner shall specify the security design as part of the information system's design specifications.

Documentation Content Requirements:

DS-D-1 The design specifications shall describe[14] the elements of the system design that satisfy the security controls. Example: The web application uses the centralized authentication system (i.e., the design element) to authenticate user access (i.e., the security control).

DS-D-2 The design specifications shall trace[15] the correspondence of the design elements to the security controls that they satisfy.

Assessment Tasks:

DS-A-1 The security assessor shall confirm that the information produced meets all documentation content requirements.

DS-A-2 The security assessor shall determine that the design specifications represent an accurate and complete instantiation of all security controls.

8.4.4 TRA - Threat and Risk Assessment

Objective:

The security design of the information system is supported by an adequate TRA process.

Engineering Tasks:

TRA-E-1 The security practitioner shall use a formal, established TRA process.

[14] As per Annex 5 of ITSG-33 (Glossary) [Reference 11], the term *describe* means to provide specific details of an entity.
[15] As per Annex 5 of ITSG-33 (Glossary), the term *trace* means to perform an informal correspondence analysis between two entities with only a minimal level of rigour. Tracing provides assurance that design specifications cover all design requirements. A requirements traceability matrix (or RTM) is a good example of tracing.

TRA-E-2 The security practitioner shall produce a threat protection rationale.

Documentation Content Requirements:

TRA-D-1 The project documentation shall describe the threats against which IT assets are to be protected.

TRA-D-2 All risk scenarios shall be described in terms of IT assets, threats, vulnerabilities, and risk levels.

TRA-D-3 The project documentation shall trace each security control or mechanism to threats countered by that security control or mechanism.

Assessment Tasks:

TRA-A-1 The security assessor shall confirm that the information produced meets all documentation content requirements.

8.4.5 CM - Change Management During Development

Objective:

All changes to items composing the information system under development (e.g., source code, documentation item) are appropriately managed.

Engineering Tasks:

CM-E-1 The development team shall use a change management system.

CM-E-2 The development team shall produce change management documentation.

CM-E-3 The development team shall uniquely identify all configuration items.

CM-E-4 The development team shall apply measures such that only authorised changes are made to the configuration items.

CM-E-5 The development team shall apply automated measures such that only authorised changes are made to the configuration items.

Documentation Content Requirements:

CM-D-1 The change management documentation shall describe the method used to uniquely identify the configuration items.

CM-D-2 The change management documentation shall describe the measures used to enforce only authorized changes.

CM-D-3 The change management documentation shall include a change management plan.

CM-D-4 The change management plan shall describe how the change management system is used for the development of the information system.

CM-D-5 The change management plan shall describe the procedures used to accept modified or newly created configuration items.

Assessment Tasks:

CM-A-1 The security assessor shall confirm that the information produced meets all documentation content requirements.

CM-A-2 The security assessor shall confirm that all configuration items are being maintained under the change management system.

CM-A-3 The security assessor shall confirm that the CM system is being operated in accordance with the change management plan.

8.4.6 SM - Development Environment Security Measures

Objective:

The development environment is adequately protected in confidentiality, integrity, and availability.

Engineering Tasks:

SM-E-1 The development team shall implement security measures to protect the confidentiality, integrity, and availability of the development environment (e.g., physical security, access control, authorization of changes to the development environment)

SM-E-2 The development team shall produce security documentation for the development environment.

Documentation Content Requirements:

SM-D-1 The security documentation shall describe all security measures that are used to protect the confidentiality, integrity, and availability of the development environment.

Assessment Tasks:

SM-A-1 The security assessor shall confirm that the security measures are being applied.

SM-A-2 The security assessor shall confirm that the information produced meets all documentation content requirements.

8.4.7 DT - Development Tools

Objective:

The development team selects and uses appropriate development tools. This includes, but is not limited to, programming languages, implementation standards, and supporting runtime libraries.

Engineering Tasks:

DT-E-1 The development team shall select, install, and configure the appropriate tools for the development of the information system.

DT-E-2 The development team shall produce documentation for the development tools being used.

Documentation Content Requirements:

DT-D-1 The documentation shall describe all development tools and identify their dependencies and customizations.

DT-D-2 The documentation of each development tool shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.

DT-D-3 The documentation of each development tool shall unambiguously define the meaning of all implementation-dependent options.

Assessment Tasks:

DT-A-1 The security assessor shall confirm that the appropriate development tools have been implemented.

DT-A-2 The security assessor shall confirm that the information provided meets all documentation content requirements.

8.4.8 SDP - Secure Development Practices

Objective:

The development team follows secure development best practices (e.g., use of source code analysis tools and techniques, source code review) appropriate to their development environment.

Engineering Tasks:

SDP-E-1 The development team shall follow secure development best practices appropriate to their development environment.

SDP-E-2 The development team shall produce documentation identifying the security practices that the development team is using to develop the information system.

Documentation Content Requirements:

SDP-D-1 The documentation of each security development practice shall provide a reference for the practices and describe their purpose and intended use.

Assessment Tasks:

SDP-A-1 The security assessor shall confirm that secure development best practices are being used.

SDP-A-2 The security assessor shall confirm that the information produced meets all documentation content requirements.

8.4.9 ST - Security Testing

Objective:

Ensure that the security solutions of the information system are operating as expected. Security testing includes development testing and integration testing.

Engineering Tasks:

ST-E-1 The development team shall test all the security solutions of the information system.

ST-E-2 The development team shall produce test documentation.

ST-E-3 The development team shall produce an analysis of the security testing.

Documentation Content Requirements:

ST-D-1 The test documentation shall consist of test plans, expected test results, and actual test results.

ST-D-2 The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ST-D-3 The actual test results shall be consistent with the expected test results and deviations shall be documented.

ST-D-4 The analysis of the security testing shall trace the correspondence between the tests in the test documentation and the security mechanisms in the design specifications or security solutions in the information system representation.

Assessment Tasks:

ST-A-1 The security assessor shall confirm that the information provided meets all documentation content requirements.

8.4.10 OSP - Operational Security Procedures

Objective:

Ensure the secure use, administration, and maintenance of the information system during its operational period.

Engineering Tasks:

OSP-E-1 The security practitioner shall produce operational security procedures.

Documentation Content Requirements:

OSP-D-1 The security procedures shall, for each user role, describe the schedule of security-relevant actions to be performed in order to maintain the security of the information system in the operational environment (e.g., access control officer: create end user system account, unlock account, delete inactive account; end user: change password; system administrator: change password rules).

OSP-D-2 The security procedures shall describe, for each user role, how to use the available interfaces (e.g., systems administrator's use of SSH to remotely access servers for maintenance purposes, end user's remote logging).

OSP-D-3 The security procedures shall, for each user role, clearly describe each scheduled action and how the user is expected to perform it.

Assessment Tasks:

OSP-A-1 The security assessor shall confirm that the information provided meets all documentation content requirements.

8.4.11 SIP – Security Installation Procedures

Objective:

Ensure that the information system can be installed in a secure manner in accordance with the implementation representation[16].

Engineering Tasks:

SIP-E-1 The security practitioner shall produce security installation procedures for the information system.

Documentation Content Requirements:

SIP-D-1 The security installation procedures shall describe all the steps necessary for the secure installation of the information system and for the secure preparation of the operational environment.

Assessment Tasks:

SIP-A-1 The security assessor shall confirm that the information provided meets all documentation content requirements.

8.4.12 VA - Vulnerability Assessment

Objective:

Discover and mitigate vulnerabilities.

Engineering Tasks:

VA-E-1 The security practitioner shall perform a search of public domain sources to identify potential vulnerabilities in the information system.

VA-E-2 The security practitioner shall perform a vulnerability scan of the information system using publicly available commercial or open-source software to identify potential vulnerabilities.

VA-E-3 The security practitioner shall determine through penetration testing those identified potential vulnerabilities that can be exploited by an attacker.

VA-E-4 The security practitioner shall implement patches and other corrective measures to resolve vulnerabilities.

[16] As per Annex 5 of ITSG-33 (Glossary) [Reference 11], the term *implementation representation* means the least abstract representation of the information system. It consists of source code, hardware and software products, physical network diagrams, configuration documentation such as build books, and so on. Collectively, these elements allow for the construction of the information system without having to make any further design or implementation decisions.

VA-E-5 The security practitioner shall produce vulnerability analysis documentation.

Documentation Content Requirements:

VA-D-1 The vulnerability analysis documentation shall consist of the list of identified vulnerabilities, the required patches and corrective measures, the status of the implementation of patches and corrective measures in the operational environment, and associated change management records.

Assessment Tasks:

VA-A-1 The security assessor shall confirm that the information provided meets all documentation content requirements.

VA-A-2 The security assessor shall confirm, through inspection of the operational environment, the status of the implementation of required patches and corrective measures.

8.4.13 SIV - Security Installation Verification

Objective:

Confirm that the security of the information system has been installed and configured correctly in the operational environment.

Engineering Tasks:

SIV-E-1 The security practitioner shall perform a verification of the installation and configuration of key security solutions within the operational environment of the information system.

SIV-E-2 The security practitioner shall perform a comprehensive verification of the installation and configuration of security solutions within the operational environment of the information system.

SIV-E-3 The security practitioner shall correct installation and configuration errors and omissions.

SIV-E-4 The security practitioner shall produce security installation verification documentation.

Documentation Content Requirements:

SIV-D-1 The security installation verification documentation shall consist of a verification plan, expected verification results, actual results, identified installation and configuration errors, and a confirmation that installation and configuration errors have been corrected.

Assessment Tasks:

SIV-A-1 The security assessor shall confirm that installation and configuration errors and omissions have been corrected (e.g., by reviewing related change management records).

SIV-A-2 The security assessor shall confirm that the information provided meets all documentation content requirements[17].

[17] The combination of SIV-E-4/SIV-A-2 builds on the assurance requirements under SIV-E-3/SIV-A-1 by requiring formal evidence of all security verification procedures instead of limiting evidence to the identification and correction of installation and configuration errors and omissions.

9 Security Control Tailoring Guidance

9.1 Introduction

This section contains security control tailoring guidance[18] to apply during the definition, design, and development of information systems. This tailoring guidance is presented from the perspective of IT projects. However, they apply equally to the development of departmental and business domain security control profiles.

9.2 Overview

When selecting security controls for a specific information system from an applicable security control profile, IT projects tailor security controls to more closely align them with conditions specific to the information system. The tailoring process includes several activities:

1) Application of scoping guidance to the initial security control selection;
2) Specification of compensating security controls, if needed; and
3) Specification of organization-defined parameters in the security controls via explicit assignment and selection statements.

IT projects document tailoring decisions, including the specific rationale for those decisions, in information system documentation in accordance with applicable security assurance requirements. IT projects also assess and approve tailoring decisions as part of the ISSIP's security control assessment and approval process.

9.3 Scoping Guidance

There are several considerations that can potentially affect how security controls apply to specific information systems. These are described in the sub-sections below.

9.3.1 Common Security Controls Considerations

Security controls designated by TBS or departmental security authorities as common security controls are, in most cases, managed by a departmental entity other than the information system owner. IT projects need to be aware of the existence of, or the requirement to use, common security controls, determine if they apply to the information system that they are implementing, and negotiate the terms and conditions of their use.

9.3.2 Operational/Environmental Considerations

Security controls that are dependent on the nature of the operational environment are applicable only if the information system is deployed in an environment necessitating such security controls. For example,

[18] The tailoring procedures are based in part on the guidance found in NIST's Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Departments* [Reference 12].

certain physical security controls may not be applicable to space-based information systems, and temperature and humidity controls may not be applicable to remote sensors that exist outside of the indoor facilities that contain information systems.

9.3.3 Physical Infrastructure Considerations

Security controls that refer to departmental facilities (e.g., physical controls such as locks and guards, environmental controls for temperature, humidity, lighting, fire, and power) are applicable only to those sections of the facilities that directly provide protection to, support for, or are related to the information system.

9.3.4 Public Access Considerations

When public access to departmental information systems is allowed, security controls should be applied with discretion as some (e.g., identification and authentication, personnel security controls) may not be applicable to public access. For example, while a domain security control profile may require identification and authentication of departmental personnel that maintain and support information systems providing the public access services, the same controls might not be required for access to those information systems through public interfaces to obtain publicly available information. On the other hand, identification and authentication would be required for users accessing information systems through public interfaces in some instances, for example, to access or change their personal information.

9.3.5 Technology Considerations

Security controls that refer to specific technologies (e.g., wireless, cryptography, public key infrastructure) are applicable only if those technologies are deployed or planned for deployment within the information system.

Security controls are applicable only to the components of the information system that provide or support the security capability addressed by the security control and are sources of potential risk being mitigated by the security control. For example, when information system components are single-user, not networked, or part of a physically isolated network, one or more of these characteristics may provide appropriate rationale for not applying selected security controls to that component.

Security controls should be implemented to the maximum extent possible by automated mechanisms. Many security controls can be implemented using mechanisms that already exist in commercial or government off-the-shelf products. For example, access enforcement to objects such as files can be implemented by the built-in access control mechanisms of operating systems. If automated mechanisms are not readily available to implement a specific security control or enhancement, and it is not cost-effective or technically feasible to develop them, compensating security controls, implemented through non-automated mechanisms or procedures, should be used instead (see terms and conditions for applying compensating controls below).

9.3.6 Policy and Regulatory Considerations

Security controls that address mandatory security requirements specified by applicable GC legislation and TBS policies, directives, and standards (e.g., privacy impact assessments) are required only if the employment of those controls is consistent with the types of information and information systems covered by the applicable GC legislation and TBS policies, directives, and standards.

9.4 Compensating Security Controls

With the diverse nature of today's information systems, IT projects may find it necessary to specify and employ compensating security controls. A compensating security control is a management, operational, or technical security control implemented in lieu of a required security control (from an applicable security control profile) that provides equivalent or comparable protection for an information system.

When considering the use of compensating security controls for an information system, IT projects should apply the following guidelines:

1) The IT project should select the compensating control from ITSG-33, Annex 3 *Security Control Catalogue* [Reference 7] whenever possible.
2) The IT project should provide supporting rationale for how the compensating control delivers an equivalent security capability for the information system and why the security control in the applicable security control profile could not be employed.
3) The IT project should assess and document the risk associated with employing the compensating control in the information system.

9.5 Organization-Defined Security Control Parameters

Many of the security controls and control enhancements contain organization-defined security control parameters. They are essentially place holders for security practitioners to specify, during the selection process, values that are specific to their organization's context. Organization-defined parameters give departments the flexibility to define certain portions of a security control to support specific departmental requirements or objectives. These parameters may be defined, in whole or in part, in the departmental security control profile or an applicable domain security control profile.

Where parameters have not been defined, IT projects need to review the list of security controls, after the application of scoping guidance and selection of compensating security controls, and determine appropriate values based on departmental and GC security policies, directives, and standards, or as indicated by TRA activities or based on security best practices.

10 References

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

[Reference 2] Communications Security Establishment. *IT Security Risk Management: A Lifecycle Approach – Overview*. ITSG-33. 1 November 2012.

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

[Reference 4] Treasury Board of Canada Secretariat. *Directive on Departmental Security Management*. 1 July 2009.

[Reference 5] Treasury Board of Canada Secretariat. *Operational Security Standard: Management of Information Technology Security (MITS)*. 31 May 2004.

[Reference 6] International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC). *Information Technology – Systems Security Engineering – Capability Maturity Model (SSE-CMM)*. Reference Number ISO/IEC 21827:2002(E), 1 October 2002.

[Reference 7] Communications Security Establishment. *IT Security Risk Management: A Lifecycle Approach – Security Control Catalogue*. ITSG-33, Annex 3. 1 November 2012.

[Reference 8] Communications Security Establishment. *User Authentication Guidance for IT Systems*. ITSG-31. March 2009.

[Reference 9] International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC). *Information Technology – Security Techniques – Information Security Management Systems – Requirements*. Reference Number ISO/IEC 27001:2005. 2005.

[Reference 10] National Security Agency. *Information Assurance Technical Framework*. Release 3.1. September 2002. (*Archived*)

[Reference 11] Communications Security Establishment. *IT Security Risk Management: A Lifecycle Approach – Glossary*. ITSG-33, Annex 5. 1 November 2012.

[Reference 12] National Institute of Standards and Technology. *Recommended Security Controls for Federal Information Systems and Organizations*. NIST Special Publication 800-53, Revision 3. August 2009.

[Reference 13] National Institute of Standards and Technology. *Managing Information Security Risk: Organization, Mission, and Information System View*. NIST Special Publication 800-39, March 2011.