# Digital Policy Office

## INFORMATION SECURITY

# Practice Guide

# for

# Security by Design

**Version 1.1**

**July 2024**

# COPYRIGHT NOTICE

| Amendment History | | | | |
|---|---|---|---|---|
| Change Number | Revision Description | Pages Affected | Revision Number | Date |
| 1 | Change “Office of the Government Chief Information Officer” (or “OGCIO” ) to “Digital Policy Office” (or “DPO”) | | 1.1 | July 2024 |

# Table of Contents

# 1 Introduction

With the rapidly evolving digital landscape, security threats have become increasingly prevalent, posing significant risks to the information systems and assets of the Government. Addressing security as an afterthought or through reactive measures is no longer sufficient. Instead, Bureaux/Departments (B/Ds) should adopt a proactive approach that integrates security considerations as a core business requirement instead of only a technical feature. This practice guide is developed to provide guidance notes for B/Ds to make reference in system development projects.

## 1.1 Purpose

This document provides a general framework for Security by Design. It should be used in conjunction with other security documents such as the Baseline IT Security Policy [S17], IT Security Guidelines [G3] and relevant procedures, where applicable.

This practice guide is intended for all level of staff within B/Ds, who are involved in all phases of the System Development Life Cycle. In addition,the document is intended for use by vendors, contractors and consultants who provide IT services to the Government.

## 1.2 Normative References

The following referenced documents are indispensable for the application of this document.

- Baseline IT Security Policy [S17], the Government of Hong Kong Special Administrative Region
- IT Security Guidelines [G3], the Government of Hong Kong Special Administrative Region
- Practice Guide for Security Risk Assessment & Audit [ ISPG-SM01], Digital Policy Office
- Practice Guide for Agile Software Development [G62], Digital Policy Office
- Information technology - Security techniques - Information security management systems - Requirements (second edition), ISO/IEC 27001:2022
- Information technology - Security techniques – Code of practice for information security controls (second edition), ISO/IEC 27002:2022
- Security-by-Design Framework, Cyber Security Agency of Singapore
- "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default", Cybersecurity and Infrastructure Security Agency
- "What Is Shift Left Security?", Fortinet

## 1.3 Terms and Convention

For the purposes of this document, the terms and conventions given in S17, G3, and the following apply.

| **Abbreviation and Terms** | |
|---|---|
| SDLC | System Development Life Cycle |
| IRS | Initial Request Statement |
| SA&D | System Analysis and Design |
| SBD | Security by Design |
| DMZ | Demilitarised zone |
| RBAC | role-based access control |

## 1.4 Contact

This document is produced and maintained by the Digital Policy Office (DPO). For comments or suggestions, please send to:

Email: it_security@digitalpolicy.gov.hk

Lotus Notes mail: IT Security Team/DPO/HKSARG@DPO

CMMP mail: IT Security Team/DPO

# 2 Information Security Management

Information security is about the planning, implementation and continuous enhancement of security controls and measures to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission and its associated information systems. Information security management is a set of principles relating to the functions of planning, organising, directing, controlling, and the application of these principles in harnessing physical, financial, human and informational resources efficiently and effectively to assure the safety of information assets and information systems.

Information security management involves a series of activities that require continuous monitoring and control. These activities include, but are not limited to, the following functional areas:

- Security Management Framework and the Organisation;
- Governance, Risk Management, and Compliance;
- Security Operations;
- Security Event and Incident Management;
- Awareness Training and Capability Building; and
- Situational Awareness and Information Sharing.

**Security Management Framework and Organisation**

B/Ds shall establish and enforce departmental information security policies, standards, guidelines and procedures in accordance with the business needs and the government security requirements.

B/Ds shall also define the organisation structure on information security and provide clear definitions and proper assignment of security accountability and responsibility to involved parties.

**Governance, Risk Management and Compliance**

B/Ds shall adopt a risk based approach to identify, prioritise and address the security risks of information systems in a consistent and effective manner.

B/Ds shall perform security risk assessments for information systems and production applications periodically and when necessary so as to identify risks and consequences associated with vulnerabilities, and to provide a basis to establish a cost-effective security program and implement appropriate security protection and safeguards.

B/Ds shall also perform security audits on information systems regularly to ensure that current security measures comply with departmental information security policies, standards, and other contractual or legal requirements.

**Security Operations**

To protect information assets and information systems, B/Ds should implement comprehensive security measures based on their business needs, covering different technological areas in their business, and adopt the principle of "Prevent, Detect, Respond and Recover" in their daily operations.

- Preventive measures avoid or deter the occurrence of an undesirable event;
- Detective measures identify the occurrence of an undesirable event;
- Response measures refer to coordinated actions to contain damage when an undesirable event or incident occurs; and
- Recovery measures are for restoring the confidentiality, integrity and availability of information systems to their expected state.

**Security Event and Incident Management**

In reality, security incidents might still occur due to unforeseeable, disruptive events. In cases where security events compromise business continuity or give rise to the risk of data security, B/Ds shall activate their standing incident management plan to identify, manage, record, and analyse security threats, attacks, or incidents in real-time. B/Ds should also prepare to communicate appropriately with relevant parties by sharing information on response to security risks to subdue distrust or unnecessary speculation. When developing an incident management plan, B/Ds should plan and prepare the right resources as well as develop the procedures to address necessary follow-up investigations.

**Awareness Training and Capability Building**

As information security is everyone's business, B/Ds should continuously promote information security awareness throughout the organisations and arrange training and education to ensure that all related parties understand the risks, observe the security regulations and requirements, and conform to security best practices.

**Situational Awareness and Information Sharing**

As the cyber threat landscape is constantly changing, B/Ds should also constantly attend to current vulnerabilities information, threat alerts, and important notices disseminated by the security industry and the GovCERT.HK. The security alerts on impending and actual threats should be disseminated to and shared with those responsible colleagues within B/Ds so that timely mitigation measures could be taken.

B/Ds could make use of threat intelligence platforms to receive and share information regarding security issues, vulnerabilities, and cyber threat intelligence.

Staff may also raise their security awareness by participating in security drills, attending seminars, showcases or visiting theme pages containing security intelligence information and general security information (e.g. Cyber Security Information Portal, InfoSec website).

# 3 Security by Design

To truly appreciate the significance of Security by Design (SBD) and its synergy with the System Development Life Cycle (SDLC), it is essential to grasp the fundamentals of the SDLC itself.

## 3.1 System Development Life Cycle (SDLC)

The SDLC serves as a structured framework encompassing the various stages of system development, including planning, analysis, design, implementation, testing, deployment, and maintenance. It provides a framework for managing the entire life cycle of a system, from its inception to its retirement. The SDLC illustrated in G3 is recapped as below:

- ***Project Initiation:*** To request an IT solution, users should submit an Initial Request Statement (IRS). The IRS will be assessed, and a decision will be made on whether the project should proceed to the next phase.

- ***Feasibility Study***: To assess the feasibility of an IT solution and to quantify the requirements, scope, costs, benefits and other implications of the proposed solution.

- ***Systems Analysis and Design (SA&D):*** To investigate the existing system, specify the new system, and detail the implementation requirements by performing systems analysis and logical system design.

- ***Implementation:*** To implement the findings of the SA&D by performing Physical System Design, Program Development, various kinds of testing, installation and Project Evaluation Review.

- ***Post-Implementation Review:*** To evaluate the cost-effectiveness of an implemented system and assess whether the system has achieved its agreed objectives and realised the intended benefits in a timely manner.

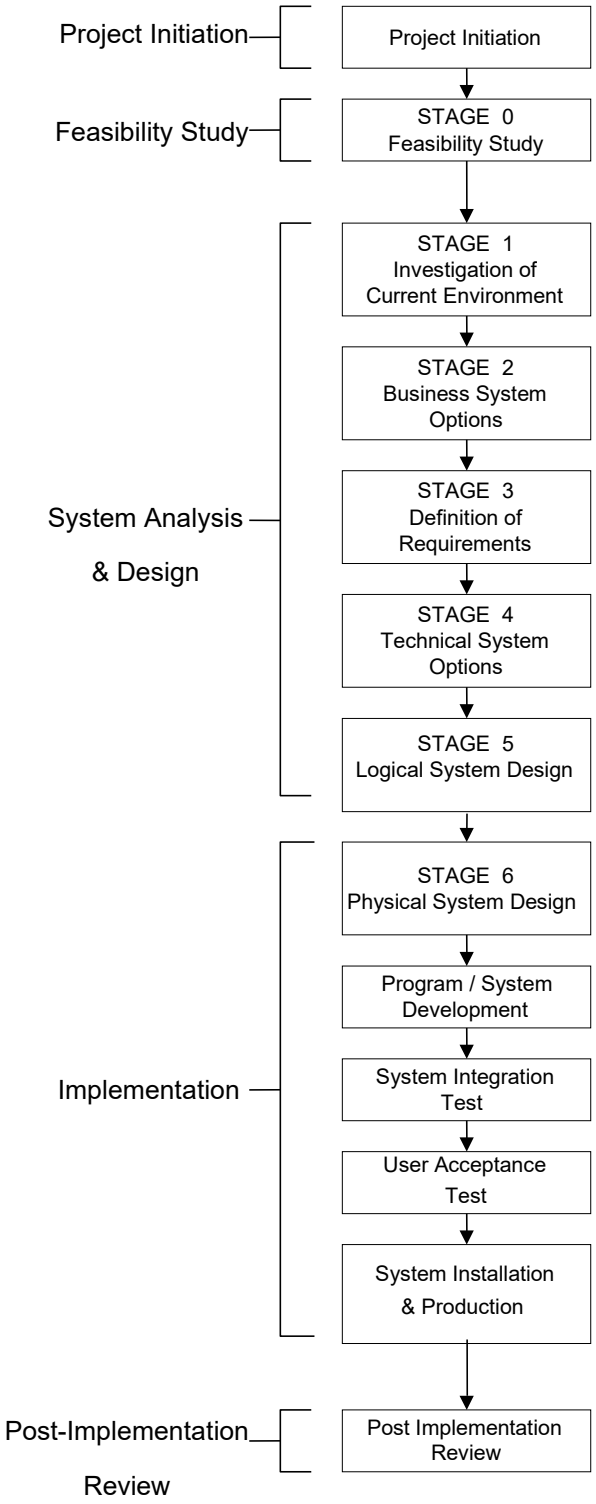


**Figure 3.1: Different Phases of System Development Life Cycle**

There are different methodologies within the SDLC, such as Waterfall and Agile. Waterfall follows a linear and sequential progression through the phases,

while Agile promotes iterative development cycles with flexibility and adaptability. Depending on the nature of the project, B/Ds may flexibly adopt more than one software development approach and apply multiple practices according to project needs.

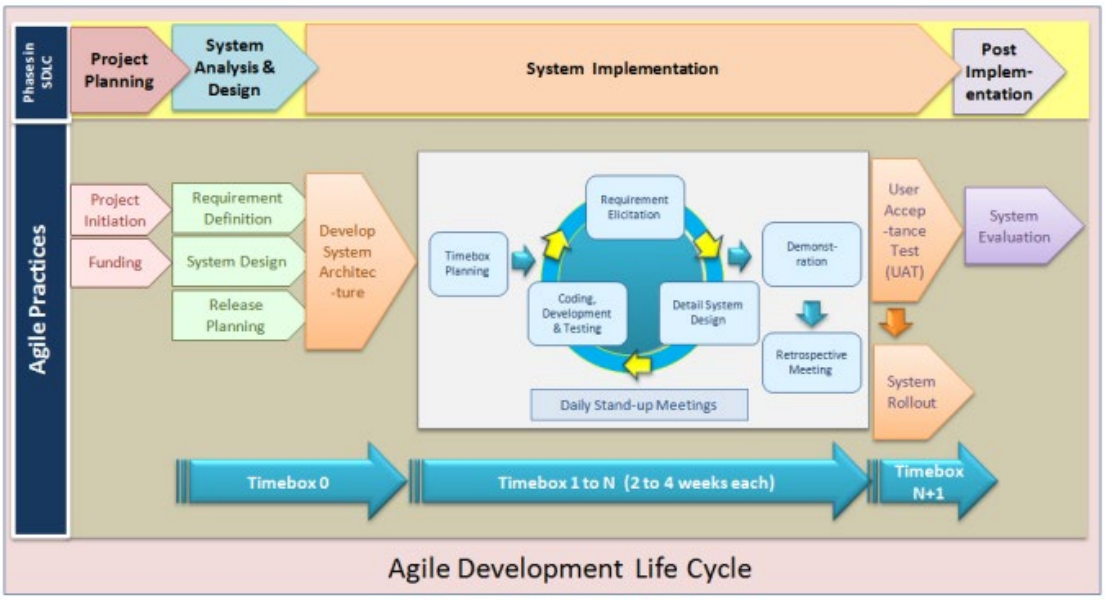


**Figure 3.2: Agile Development Life Cycle from Practice Guide for Agile Software Development**

For more information about the agile software development methodology, please refer to the following document for details:

- **Practice Guide for Agile Software Development**
  Available at ITG InfoStation.
  (https://itginfo.ccgo.hksarg/content/bpg/Agile/agile.html)

The SBD Framework, described in this document, is adaptable to both the Waterfall and Agile development life cycle.

## 3.2 Introduction to Security by Design and its Importance

SBD is a concept of system development that prioritises and integrates security measures throughout the entire development life cycle. SBD aims to proactively identify and address security risks and vulnerabilities early in the development process, reducing the possibility of security breaches and ensuring the creation of robust and resilient systems. By incorporating security principles from the

outset, B/Ds can minimise the likelihood of costly security incidents and protect the confidentiality, integrity, and availability of their systems and data. The SBD framework consists of principles that guide the design and development of secure systems. While different frameworks may have variations, here are some common principles found in many SBD frameworks:

- ***Core Government Requirement:*** Recognise SBD as a fundamental government requirement, aligning it with strategic goals, operational needs, and regulatory requirements. Treat security as a competitive advantage and prioritise it alongside other core government requirements, ensuring necessary attention, resources, and executive support.

- ***Proactive Approach:*** Adopt a proactive mindset to address security concerns from the early stages of system design. Security should not be an afterthought but an integral part of the development process.

- ***End-to-End Security:*** Consider security across the entire system, including hardware, software, networks, and user interfaces. Address security requirements at each layer and ensure they work together to provide comprehensive protection.

- ***Risk Management:*** Conduct a thorough risk assessment to identify potential threats, vulnerabilities, and impacts. Develop risk mitigation strategies and prioritise security measures based on the level of risk and potential impact.

- ***Security Governance:*** Establish clear roles, responsibilities, and processes for managing security throughout the system's life cycle. This includes defining accountability, decision-making authority, and mechanisms for monitoring and enforcing security requirements.

- ***Secure Architecture:*** Design a secure and resilient architecture incorporating security controls at various levels. This includes network design, data flow, access controls, and separation of duties. Follow established architectural patterns and best practices for security**.**

- ***Secure Development Practices:*** Employ secure coding practices and development methodologies that prioritise security. This includes secure coding guidelines, threat modelling, code reviews, and testing for vulnerabilities. Regularly update and patch software components to address known security issues.

- ***Third-Party Security:*** Assess the security posture of third-party components, services, and vendors. Establish criteria for selecting

trustworthy and secure partners. Define contractual agreements and perform security due diligence when integrating external systems.

- ***Integration into the SDLC:*** Embed security activities and considerations into each SDLC phase. This includes requirements gathering, design, implementation, testing, deployment, and maintenance. Security should be an ongoing and iterative process throughout the entire development life cycle.

- ***Security Testing and Verification:*** Implement comprehensive security testing and verification activities throughout the SDLC. This includes vulnerability scanning, penetration testing, configuration review and source code scanning, to identify and address security weaknesses and vulnerabilities.

These considerations should be considered in all SDLC phases. There are, however, specific areas in certain SDLC phases which need special attention. These areas are highlighted in the right hand column of the chart on the following page.

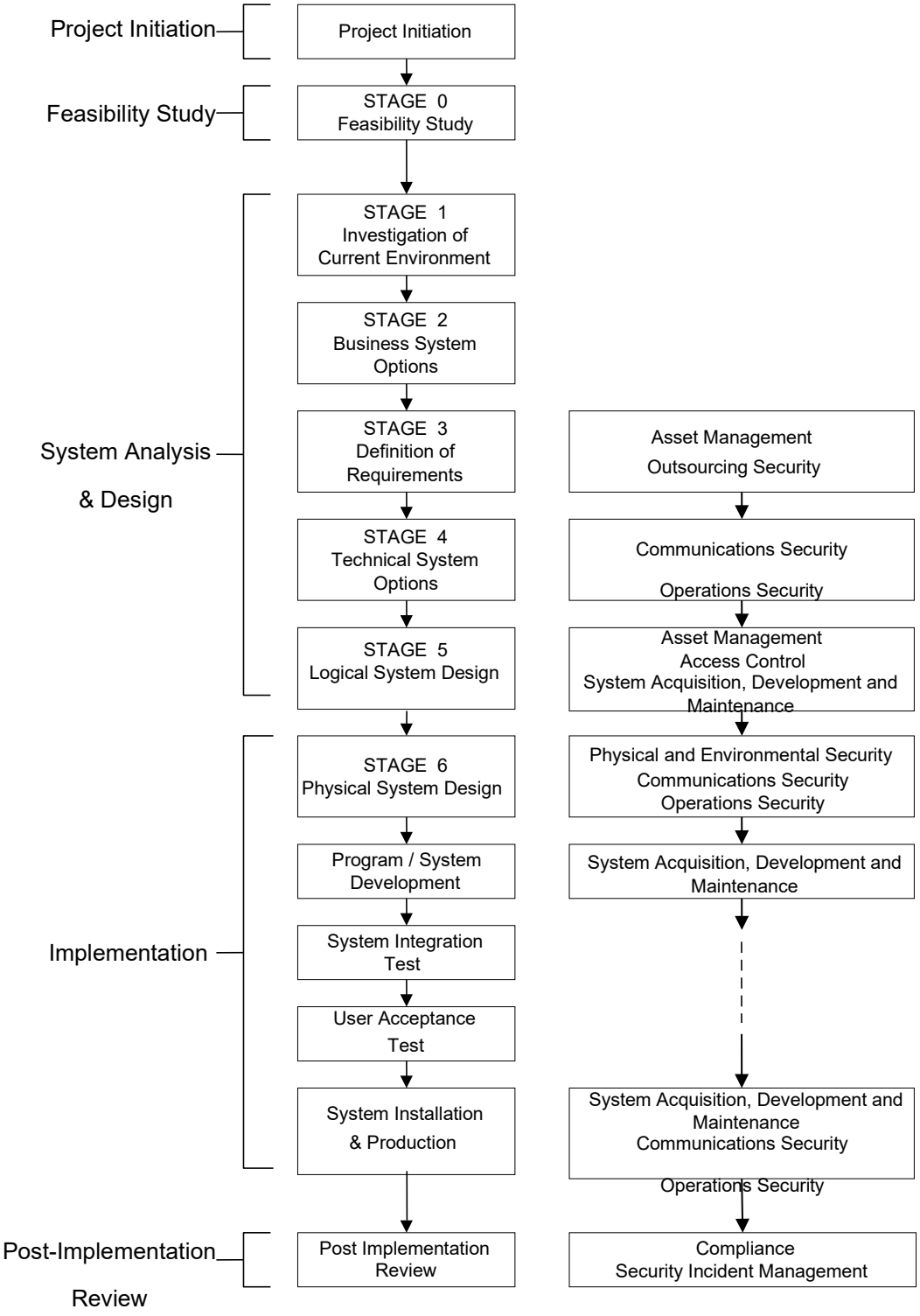


**Figure 3.3: Security Considerations Related to Different Phases of SDLC**

One concept closely related to SBD is Security Shift-left. It involves considering security right from the planning and assessment phase.

Traditionally, security tends to be addressed only during the testing phase and after the software is built, which can slow down development and often require re-work when security issues are identified during the testing phase. With Security Shift-left, security control activities are performed before testing, anticipating security needs and reducing potential issues later in development. It is important to recognise that SBD extends beyond the SDLC and Security Shift-left, encompassing the overall system design and architecture. SBD emphasises the integration of security considerations and practices into the design, architecture, and implementation of systems rather than treating security as an afterthought.

To ensure the implementation of information systems and applications with appropriate security and data protection measures, B/Ds should integrate the SBD concept into the SDLC. SBD emphasises incorporating security practices from the initial design phase and throughout all stages of the SDLC. By doing so, B/Ds can proactively identify and mitigate security risks and vulnerabilities, ultimately reducing the potential costs associated with cybersecurity damages to their reputation, data integrity, and operations.

Some key benefits of incorporating SBD into the SDLC are highlighted below:

- ***Risk mitigation:*** Reduce the potential entry points for attackers by eliminating unnecessary and vulnerable components.

- ***Cost savings:*** Minimise the need to fix security issues discovered during the late phase of the development process, which can be costly and time-consuming.

- ***Enhanced system resilience:*** Increase scalability and adaptability of information systems to changing security requirements and evolving threats by easily incorporating security updates, enhancements, and new features. Hence, information systems can be better protected from unauthorised access, data breaches, and other security incidents.

## 3.3 Security by Design Life Cycle and Framework

### 3.3.1 Security by Design Life Cycle

In the SDLC, the primary focus is on effectively developing a system, often leaving security considerations as an afterthought. Addressing vulnerabilities and patching security holes as they arise can be unreliable and costly. Designing systems to be secure from the start is a more effective approach.

The SBD life cycle aligns with the phases of the SDLC by integrating security considerations into each phase's processes. It extends across all phases because security risks need to be identified early during the planning phase and addressed throughout the subsequent phases. Security risks can be addressed through:

a) Adjusting requirements or deployment to avoid the identified security risks.
b) Implementing alternative or mitigating controls to minimise the risks.
c) Accepting the risk through a proper risk management process when necessary.
d) Employing iterative processes that evaluate security at each phase and determine if additional security measures are required to achieve satisfactory outcomes.

The following diagram illustrates how the SBD life cycle runs parallel to the SDLC:

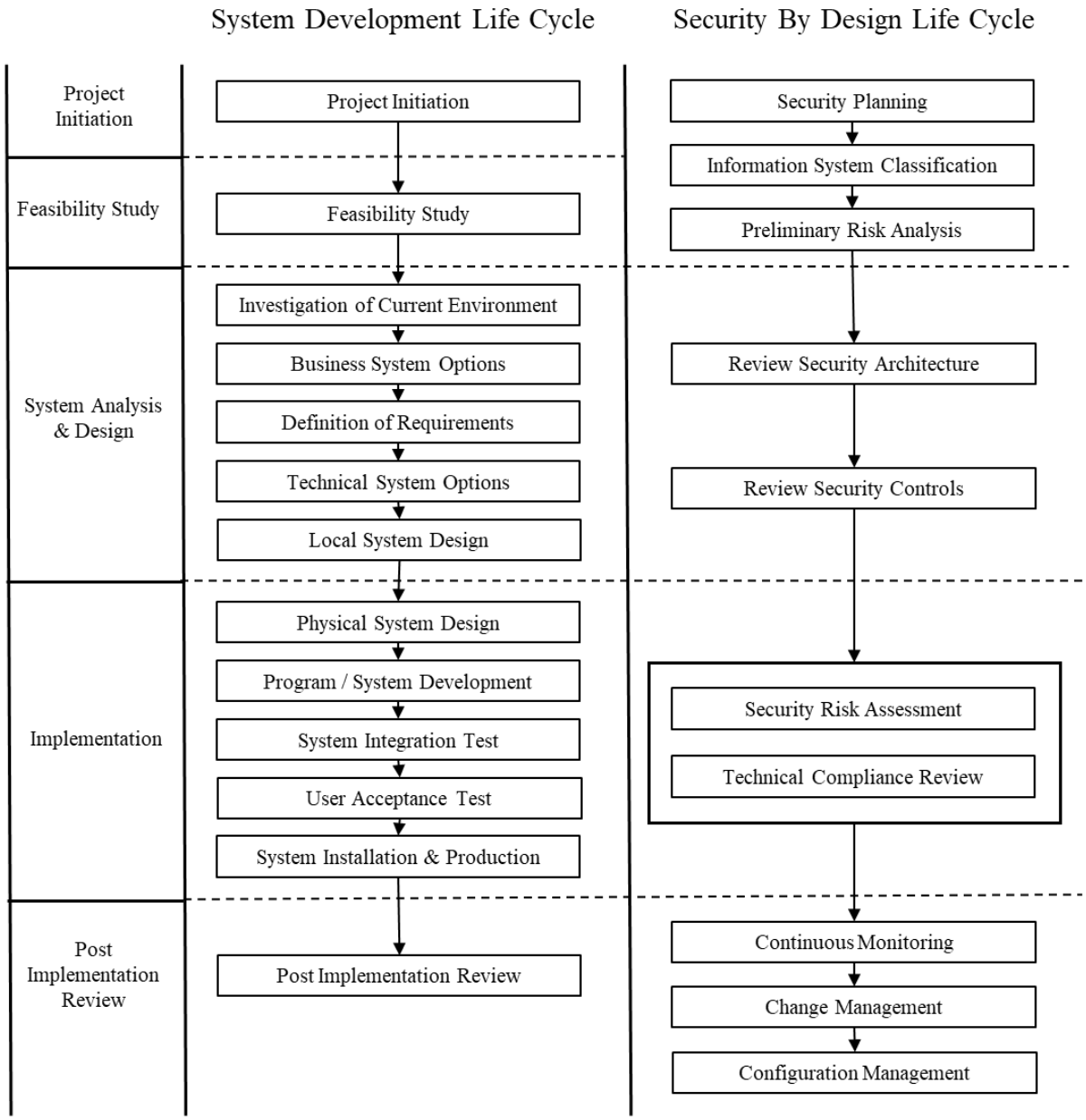


**Figure 3.4: SDLC / SBD Life Cycle**

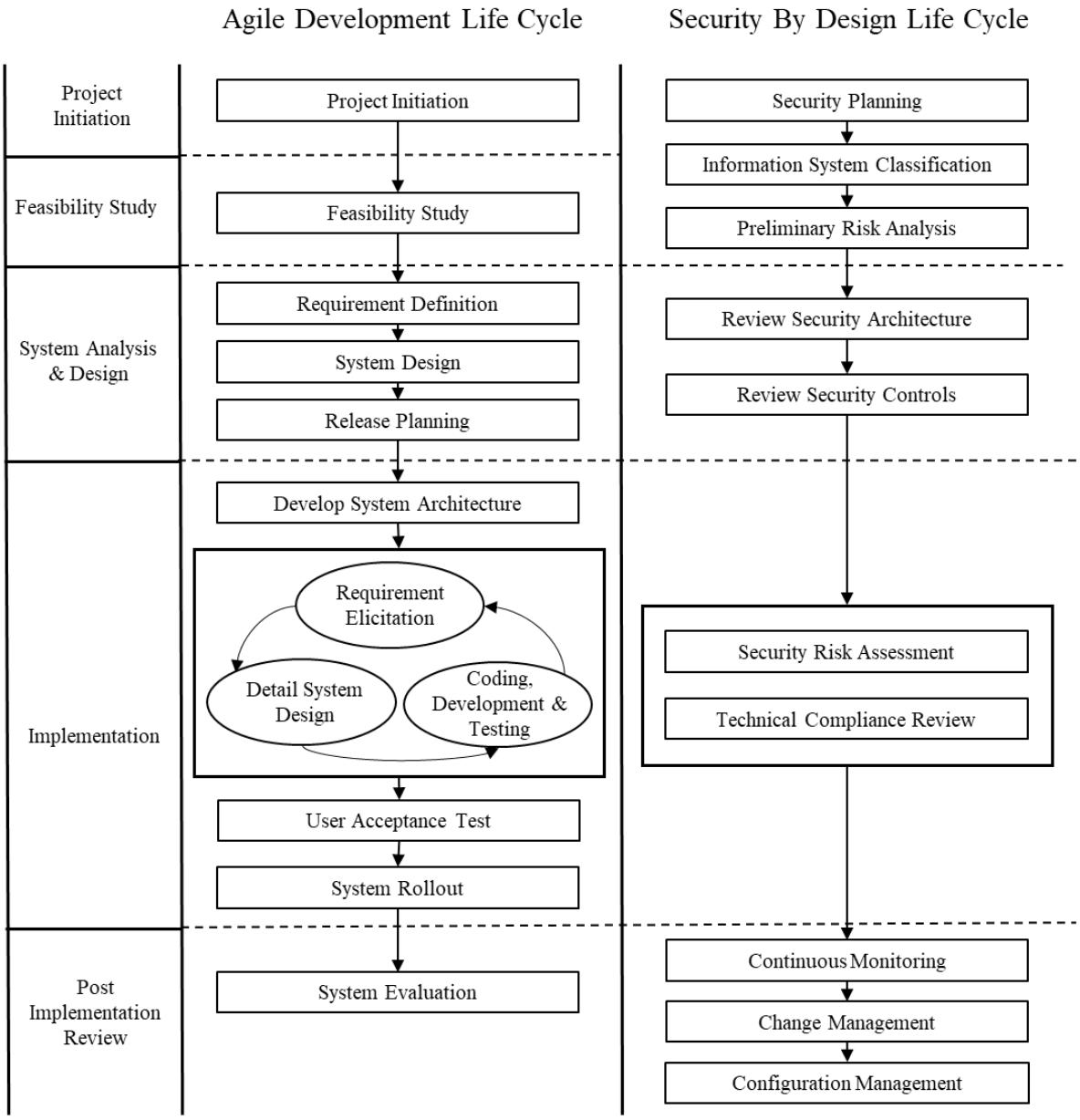


**Figure 3.5: Agile Development Life Cycle / SBD Life Cycle**

Introducing security alongside each SDLC phase offers several advantages. It ensures that security risks are visible and well understood by senior management and key personnel. This visibility enables timely and informed decisions to reduce risks to an acceptable level. By incorporating security considerations throughout the SDLC, B/Ds can proactively address security concerns and minimise potential risks more effectively.

## 3.4 Security by Design Approach

The SBD approach consists of three components, namely,

- Life Cycle: Aligning security-related processes with SDLC to guide projects to meet SBD objectives.
- Activities: Security-related activities that support the security life cycle processes.
- Control Gates: A point in time when the system development effort will be evaluated from a security perspective and when management will determine whether the project should continue as is, change direction or be discontinued.

The SBD approach is important for integrating security considerations into every phase of the security life cycle processes. These processes involve activities incorporating essential security elements into the SDLC methodology. SBD processes begin early in the SDLC phase and play a critical role in shaping the security capabilities and posture of the information system being developed throughout the entire SDLC.

Failure to adequately execute these processes at each phase of the SDLC can result in higher implementation costs. Therefore, prioritising and effectively performing these security processes at each stage of the SDLC is vital to establishing a robust and cost-effective security framework.

Incorporating an SBD approach into the SDLC is essential for developing robust and secure information systems. B/Ds should strive to adopt SBD principles wherever possible. The objectives of implementing SBD within the SDLC include:

- ***Establishing a SBD Framework:*** Create a comprehensive SBD framework that serves as a reference for stakeholders when a SBD approach is mandated. This framework should outline the SDLC's key principles, standards, and guidelines.
- ***Implementing SBD Processes:*** Develop and implement SBD processes that ensure security risks are managed from the beginning and continuously assessed throughout the SDLC. These processes should be integrated into each phase of the SDLC and follow a life cycle approach.
- ***Conducting Security Risk Assessments:*** Perform security risk assessments as part of the SBD processes to identify and evaluate potential security risks

and vulnerabilities. Regularly assess and update the system's risk profile to ensure appropriate security measures are in place.

- ***Implementing Security Activities:*** Integrate specific security activities into the SDLC to manage security risks effectively. These activities may include threat modelling, secure coding practices, security testing, vulnerability scanning, and code reviews. Ensure that security activities are conducted during the appropriate stages of the SDLC.

- ***Control Gates and Decision Point Considerations:*** Establish control gates and decision points at various phases of the SDLC to ensure that no decision is made without a comprehensive assessment of the associated security risks. This includes conducting security reviews and obtaining necessary approvals before progressing to the next phase.

# 4 Security by Design Framework

## 4.1 Framework Overview

The following diagram depicts a structured and disciplined approach to integrating security processes for systems development in the Government.

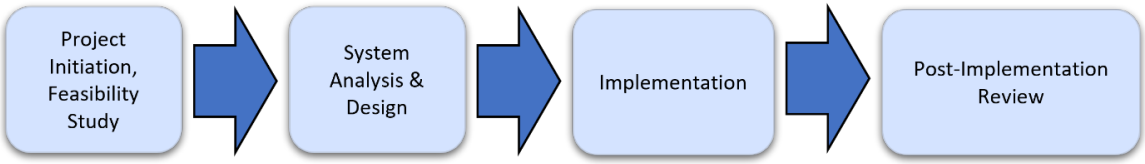


**Figure 4.1: System Development Life Cycle**

The SBD framework consists of four major phases that emphasise the continuous management of risks. An overview of these phases is provided below. The activities in each phase are described in more detail in the corresponding sections. To implement the SBD approach effectively, B/Ds should adopt a consistent risk management approach across all security processes. Information security should be considered in all stages of the SDLC.

B/Ds should embrace the SBD approach in system development, ensuring information assets' confidentiality, integrity, and availability and addressing other security aspects in response to the evolving threat landscape and technologies. By implementing straightforward measures, B/Ds can effectively mitigate and control potential information security risks associated with human and operational issues, maintaining an acceptable and manageable level of risk. B/Ds should also consider adopting best practices tailored to their business and operational environments.

Security measures and controls should be responsive and adaptive to defend against emerging security threats and mitigate risks. B/Ds should stay well-informed about emerging security threats and associated risks in systems development.

In the SBD framework, each phase is accompanied by a set of security-focused activities that outline the key actions to be taken. Figure 4.2 illustrates how these activities are aligned with each other and executed. Each activity includes essential information, such as a description of the actions to be taken, the roles and responsibilities of key personnel, and expected outputs, all aimed at enhancing system security.

After each phase, B/Ds should perform control validations to assess whether security considerations have been adequately addressed, adequate security controls have been implemented, and identified risks are thoroughly understood before advancing to the next phase of the life cycle.

## 4.2 Framework Implementation

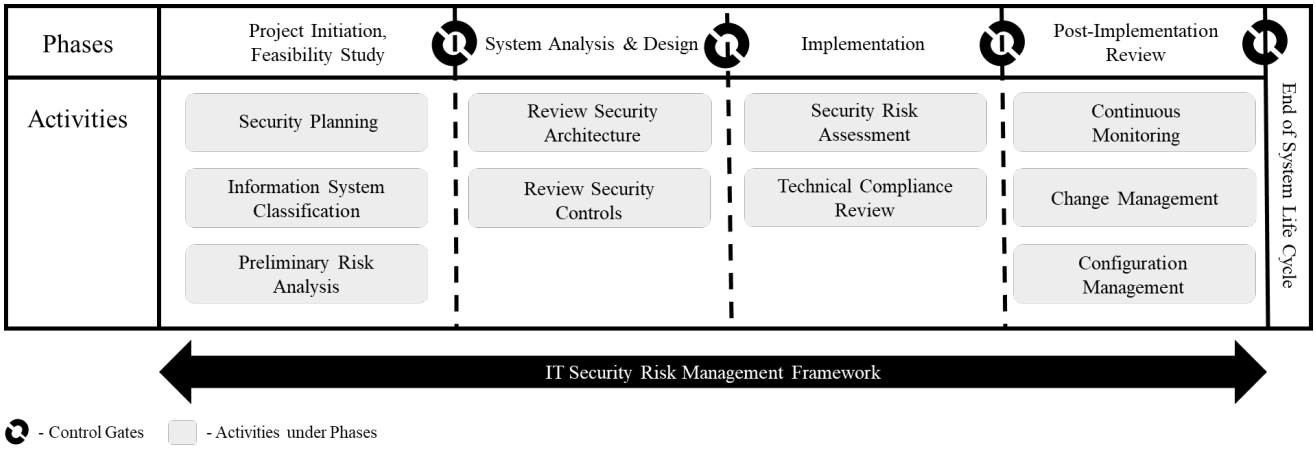


**Figure 4.2 - SBD Framework**

A. Project Initiation, Feasibility Study (Section 5)

Proper planning ensures the identification of essential security controls, policies, and procedures. In this phase, B/Ds should clearly define the security objectives, scope, and system requirements.

The major activities involved in this phase are:

- Security Planning
- Information System Classification
- Preliminary Risk Analysis

B. System Analysis & Design (Section 6)

System Analysis & Design is a vital stage in the system development life cycle where the system or application takes shape based on defined requirements. Its objective is to evaluate the security architecture and controls of the system or application to be developed. Through a comprehensive review, potential security vulnerabilities and weaknesses can be identified and addressed before deployment, hence enhancing the overall

system security. In addition, B/Ds should ensure compliance with government regulations, IT security policies and guidelines.

The major activities involved in this phase are:

- Review Security Architecture
- Review Security Controls

C. Implementation (Section 7)

In this phase, B/Ds should focus on thorough testing to validate functionality and prepare the system for deployment.

The major activities involved in this phase are:

- Security Risk Assessment
- Technical Compliance Review

D. Post-Implementation Review (Section 8)

After the system has been deployed, B/Ds should manage, monitor, and maintain the deployed application or systems continuously to ensure its ongoing security, stability, and optimal performance throughout its life cycle.

The major activities involved in this phase are:

- Continuous Monitoring
- Change Management
- Configuration Management

## 4.3 Roles and Responsibilities

B/Ds should clearly define, identify, and authorise the roles and responsibilities of all staff involved in the SDLC. Staff involved in the SDLC may include:

### 4.3.1 Senior Management (for large-scale public-facing IT system)

- Provide strategic project leadership and ensures alignment with B/D's goals.

### 4.3.2 IT Security Management Unit ("ITSMU")

- Offers security advices on implementing the security controls.

### 4.3.3 Information Owner

- Define the information's sensitivity, confidentiality, integrity, and availability requirements.
- Classify information and communicates its security requirements to the Project Manager.
- Provide final approval on implementing security controls related to the information they own.

### 4.3.4 Project Manager

- Manage the project within agreed constraints and coordinates all project activities.
- Coordinates security risk management activities and ensures compliance with relevant security standards.
- Ensure security activities are integrated into the project plan.
- Facilitate communication between teams to ensure a cohesive approach to security.
- Escalate security risks and issues as needed.

### 4.3.5 IT Security Administrators

- Execute specific security tasks, such as identifying and mitigating system vulnerabilities.

### 4.3.6 LAN/System Administrators

- Manage the system's daily operations, ensuring security mechanisms are maintained as designed.
- Implement configuration changes and security patches under the guidance of IT Security Administrators.

### 4.3.7 Application Development & Maintenance Team

- Develop systems that adhere to established procedures, incorporating security requirements from the outset.
- Engage in secure coding practices and remediates vulnerabilities.
- Ensure continuous integration of security throughout the SDLC in close collaboration with the Information Owner.

### 4.3.8 Users

- Provide early-stage input on security requirements based on their knowledge and needs.
- Offer feedback on the system's security and participates in security audits by providing information and assistance as required.
- Report any security concerns promptly.

# 5 Project Initiation, Feasibility Study

Proper and advanced planning ensures that necessary security controls, policies, and procedures are identified. During this phase, B/Ds should define the security objectives, scope, and requirements for the system. In addition, preliminary risk analysis helps prioritise security efforts and determine the most effective risk mitigation strategies.

## 5.1 Activities

Major activities involved in planning and assessment are as follows:

- Security Planning
- Information System Classification
- Preliminary Risk Analysis

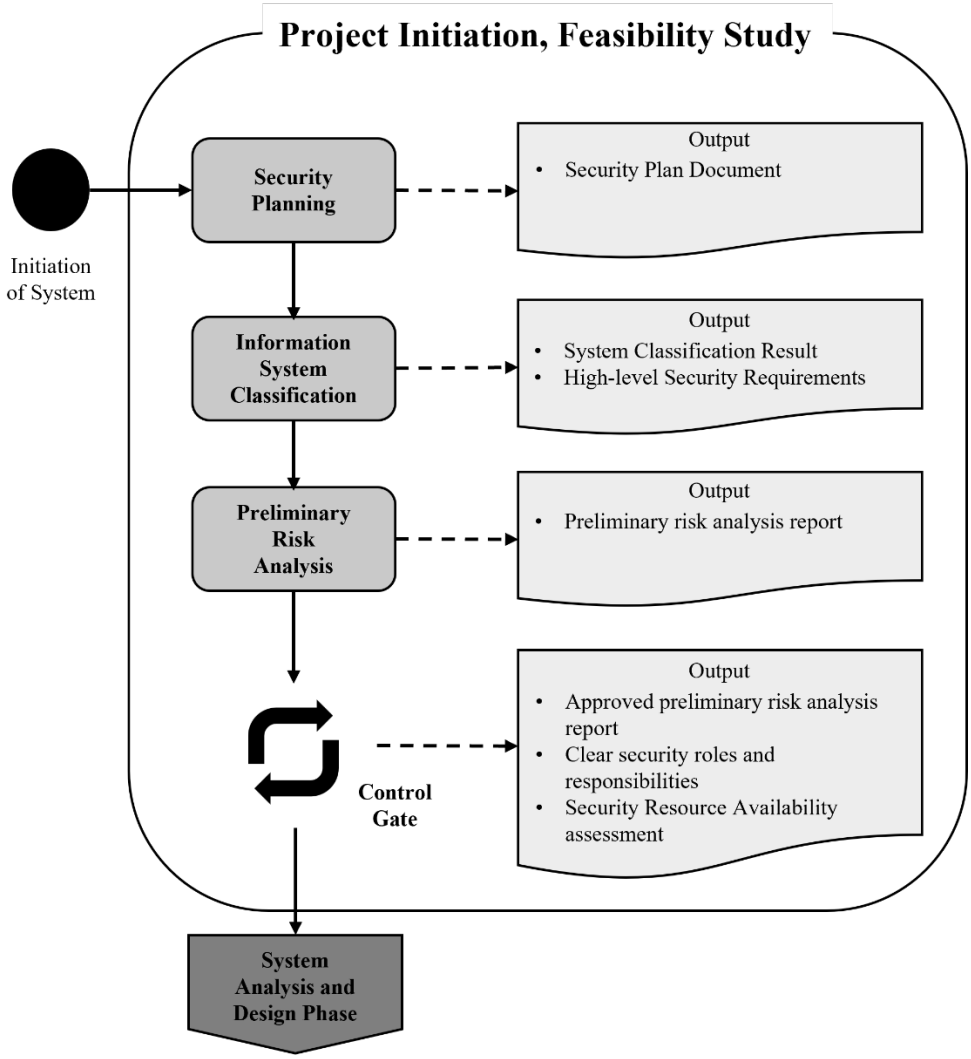


**Figure 5.1: Project Initiation, Feasibility Study**

### 5.1.1 Security Planning

B/Ds should establish a security plan which covers at least the following:

- Define the security objectives, scope, and requirements for the system;
- Establish the governance structure and responsibilities for ensuring security is incorporated throughout the SDLC;
- Identify relevant security standards, regulations, and best practices to guide the security planning process; and
- Outline key security milestones and activities.

### 5.1.2 Information Systems Classification

B/Ds shall assess the classification of the information system to ensure the system will be protected by security controls commensurate with the corresponding risk level. For more information about the system classifications, please refer to the following document for details:

- **IT Security Guidelines [G3]**
  Available at ITG InfoStation.
  (https://itginfo.ccgo.hksarg/content/itsecure/docs/Guidelines/DocRoadmap.shtml )

### 5.1.3 Preliminary Risk Analysis

Preliminary risk analysis aims to identify the threats and vulnerabilities to information systems, determine the level of risk the systems are exposed to, and recommend the appropriate level of protection.

The analysis process should include:

- Identifying and analysing all system assets and related processes.
- Assessing threats that could impact system confidentiality, integrity, or availability.
- Identifying system vulnerabilities and associated threats.
- Evaluating potential impacts and risks.
- Determining protection requirements to mitigate risks.
- Selecting appropriate security measures and analysing risk relationships.

In case of acquisition, B/Ds should define the specific security requirements such as the more stringent security requirements required per the information system classification, the determined risk mitigations or selected security measures that need to be included in the tender documents.

## 5.2 Roles and Responsibilities

### 5.2.1 Application Development & Maintenance Team

- Provide technical expertise on high-level security requirements and system development risks.
- Assist with system classification and contribute to risk analysis from a development perspective.

### 5.2.2 Project Manager

- Outline and integrate key security milestones and activities within the project plan.
- Ensure proper system and information classification and that the preliminary risk analysis is thorough and timely.
- Coordinate the preliminary risk analysis, identifying and evaluating threats, vulnerabilities, and risks and determining appropriate protective measures.

### 5.2.3 Information Owner

- Communicate high-level security requirements based on information classification.
- Participate in risk analysis, offering insights into business-specific threats and risks.

### 5.2.4 Users

- Contribute user-based insights on security requirements and operational risks, enhancing the practicality of the risk analysis.

## 5.3 Expected Outputs/Deliverables

- Security Plan Document, which includes:
  - A clear definition of the security objectives, scope, and requirements for the system.
  - An established governance structure with detailed responsibilities for ensuring security is incorporated throughout the SDLC.
  - A list of identified relevant security standards, regulations, and best practices that will guide the security planning process.
  - A timeline with key security milestones and activities.
- System classification result and High-level Security Requirements that need to be fulfilled as per the system classification.
- Preliminary risk analysis report detailing the potential threats and risks that could impact the operation and the security controls needed to be implemented to reduce the risks to an acceptable level.

## 5.4 Control Gates

The project initiation and feasibility study phase lays the foundation for successful project execution. Recommended control validations for this phase include the following:

| Control Validation | Validation Criteria | Control Gate Action |
|---|---|---|
| Approval of Preliminary Risk Analysis Report | • Ensure the preliminary risk analysis report is comprehensive, approved, and leveraged to develop detailed security requirements and controls.<br>• Verify that the report includes an evaluation of potential impacts and risks, along with the protection requirements and proposed security measures. | • Review and approve the preliminary risk analysis report.<br>• Confirm that the report will inform the subsequent development of detailed security requirements and system design.<br>• Integration of High-Level Security Requirements |
| Integration of High-Level Security Requirements | • Confirm that all high-level security requirements are included within the preliminary risk analysis report.<br>• Validate that these requirements are specified as security controls to be integrated into system design. | • Ensure the transition from high-level requirements to detailed system security controls is clear and traceable. |
| Confirmation of Roles and Responsibilities | • Establish and document clear roles and responsibilities among the project | • Review the governance structure and responsibilities documentation. |

| | | |
|---|---|---|
| | team, especially concerning security governance throughout the SDLC. | • Obtain acknowledgement from all project team members of their specific security-related roles and responsibilities. |
| Assessment of Security Resource Availability | • Evaluate the availability and adequacy of security resources, including personnel, technology, and budget, to support the project within the desired timeframe. | • Conduct a resource gap analysis if necessary and plan for resource allocation.<br>• Make decisions regarding the go/no-go status of the project based on resource availability and project timeline feasibility. |

# 6 System Analysis and Design

System Analysis and Design is a critical stage in the life cycle where the system or application begins to take shape based on the defined requirements. It aims to evaluate the security architecture and controls of a system or application being developed. By conducting a comprehensive review, potential security vulnerabilities and weaknesses can be identified and addressed before deployment, thereby enhancing the overall security posture of the system. In addition, where acquisition of third party or commercial off-the-shelf software is involved, B/Ds should ensure that the acquired system or service is in accordance with government regulations, IT security policies and guidelines.

## 6.1 Activities

There are two major activities in this phase:

- Review Security Architecture
- Review Security Controls

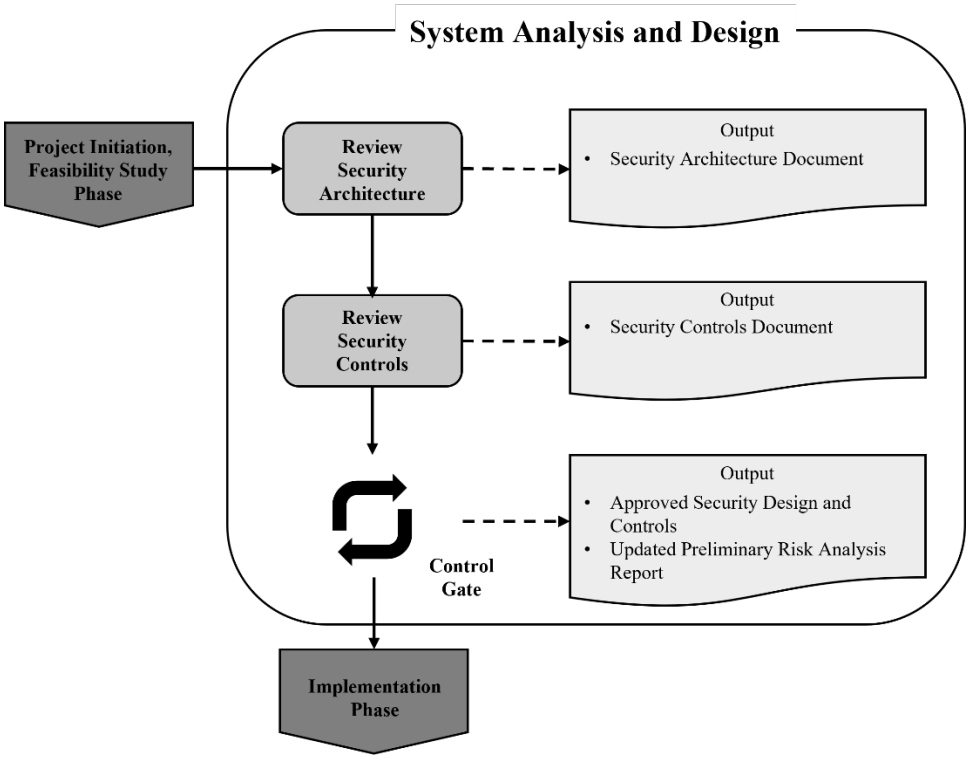


**Figure 6.1 System Analysis and Design**

### 6.1.1 Review Security Architecture

B/Ds should thoroughly review the security architecture of the system or application to assess the design and implementation of security measures and identify any potential gaps or vulnerabilities. B/Ds should focus the review on ensuring the security architecture aligns with industry best practices, regulatory and government security requirements. This includes specifying the desired security controls, compliance with relevant standards and regulations, secure data handling requirements, and any specific security expectations from the suppliers.

### 6.1.2 Review Security Controls

B/Ds should evaluate the effectiveness of the implemented security controls within the system or application. This ensures that the controls protect against potential threats, mitigate risks, and align with the defined security requirements and standards. In the case of acquisition, B/Ds should assess the security capabilities of potential suppliers and evaluate their ability to meet the defined security requirements.

In assessing the security capabilities of potential suppliers, B/Ds may include the following items:

- Security management practices;
- Incident response capabilities; and
- Security certifications.

Based on the evaluation result, B/Ds should prepare a report to serve as a basis for decision-making during the supplier selection process.

The report should include the following items:

- Third-Party Risk Assessment
- Compliance and Certifications
- Evaluation Criteria and Scoring
- Recommendations and Decision

This report should serve as a comprehensive basis for selecting the right supplier, ensuring that all security considerations are systematically addressed.

## 6.2 Roles and Responsibilities

### 6.2.1 IT Security Management Unit

- Offer advice on the security measures and controls during the system design where necessary.

### 6.2.2 Information Owner

- Clearly define the security requirements for the information based on its classification.
- Approve the security controls proposed for the protection of the information they own.

### 6.2.3 Project Manager

- Ensure security measures are seamlessly integrated into the system design.
- Coordinates security architecture review for the new system and ensure compliance with relevant standards.
- Ensure the proposed security architecture and controls align with the B/D's business objectives and security requirements.
- Ensure consistent communication between all parties about security considerations.
- Ensure that the defined security requirements are aligned with the tender requirements and that security evaluation recommendations are completed and incorporated into the tender evaluation in case of acquisition.

### 6.2.4 IT Security Administrators

- Perform specific security-related tasks during the system design, such as vulnerability assessments of the proposed design.

### 6.2.5 LAN/System Administrators

- Offer insights on the manageability and maintainability of the proposed security architecture.
- Plan for the future implementation of security configurations and patch management.

### 6.2.6 Application Development & Maintenance Team

- Develop the system design with embedded security controls.
- Plan for the remediation of potential design vulnerabilities.

- Account for the continuous integration of security throughout the remaining stages of the SDLC.

### 6.2.7 Users

- Provide input on security requirements and expectations for the system.
- Offer feedback on potential usability issues related to security measures in the system design.
- Commit to reporting any perceived security shortcomings in the proposed design.

## 6.3 Expected Outputs/Deliverables

- Security Architecture Document:
  This document comprehensively outlines the security structure within the system or application. It includes:

  - ***System Overview:*** A high-level description of the system, its components, and its purpose.
  - ***Security Objectives:*** Clear statements regarding the security goals for confidentiality, integrity, and availability.
  - ***Network Architecture:*** Diagrams and explanations of the network setup, including segmentation, firewalls, and demilitarised zones (DMZs).
  - ***Component Design:*** Details on the security aspects of each system component, including servers, databases, and applications.
  - ***Data Flows:*** Visual representations and descriptions of how data moves within the system, identifying where data may be at risk.
  - ***Access Controls:*** Descriptions of authentication and authorisation mechanisms, including role-based access control (RBAC) matrices.
  - ***Encryption Methods:*** Details on data encryption standards used both at rest and in transit.
  - ***Intrusion Detection and Prevention:*** Outline the mechanisms for detecting and preventing unauthorised access or anomalies.
  - ***Security Protocols:*** A list of all security protocols in place, such as TLS, for secure communications.
  - ***Compliance Standards:*** Identify relevant compliance standards and how the architecture adheres to them.
  - ***Security Zones:*** Definitions of network security zones and how they are isolated and protected.
  - ***Resilience and Fault Tolerance:*** Design choices that ensure the system remains operational and secure even during component failures or

attacks.

- Security Controls Document:
  This document details the specific security measures that have been implemented and how they contribute to the overall security posture of the system:
  - ***Control Inventory:*** A comprehensive list of all security controls in place, such as firewalls, antivirus software, intrusion detection systems, etc.
  - ***Control Descriptions:*** For each control, a detailed description of its function, configuration, and operation within the system.
  - ***Risk Mitigation:*** An analysis of how each control mitigates specific identified risks.
  - ***Layered Defence:*** An explanation of how the controls work together to create a layered (or defence-in-depth) security strategy.
  - ***Compliance Mapping:*** A cross-reference of controls to compliance requirements, showing how each control addresses specific mandates.
  - ***Control Ownership:*** Information on who is responsible for each control, including contact information for control owners or custodians.

## 6.4 Control Gates

Prior to the development of the system, B/Ds should validate and accept the proposed security design and controls. Updates and changes to the initial risk assessment should reflect security requirements and design changes. Recommended control validations include the following:

| Control Validation | Validation Criteria | Control Gate Action |
|---|---|---|
| Validation of Security Design and Controls | Security design and controls align with B/Ds' architectural standards and policies. | Review and approve the proposed security design and controls. |
| Consistency with B/Ds' Architecture | The system design, including security components, integrates with B/Ds' existing architecture. | Confirm integration and consistency with B/Ds' architecture; seek approval. |
| Adherence to Security Requirements | All agreed-upon security requirements are addressed in the system design. | Verify the fulfilment of requirements; document formal acceptance by stakeholders. |
| Formal Acceptance of System Design | Key stakeholders agree that the proposed system design meets the project | Obtain formal approval on the system design from key stakeholders. |

| | | |
|---|---|---|
| | objectives and security needs. | |
| Preliminary Risk Analysis Updates and Changes | Preliminary Risk analysis reflects current security requirements and design. | Update risk analysis to incorporate changes; re-validate risks and controls. |

# 7 Implementation

In the implementation phase, B/Ds should carry out a sequential approach, starting with a thorough security risk assessment and a rigorous technical compliance review. This process is critical to validate system functionality, identify, analyse, and evaluate security risks, and ensure adherence to technical standards. Maintaining a continuous monitoring stance throughout this phase is pivotal to ensure that the security posture is adjusted accordingly as the system evolves.

## 7.1 Activities

Major activities involved in implementation are as follows:

- Security Risk Assessment
- Technical Compliance Review

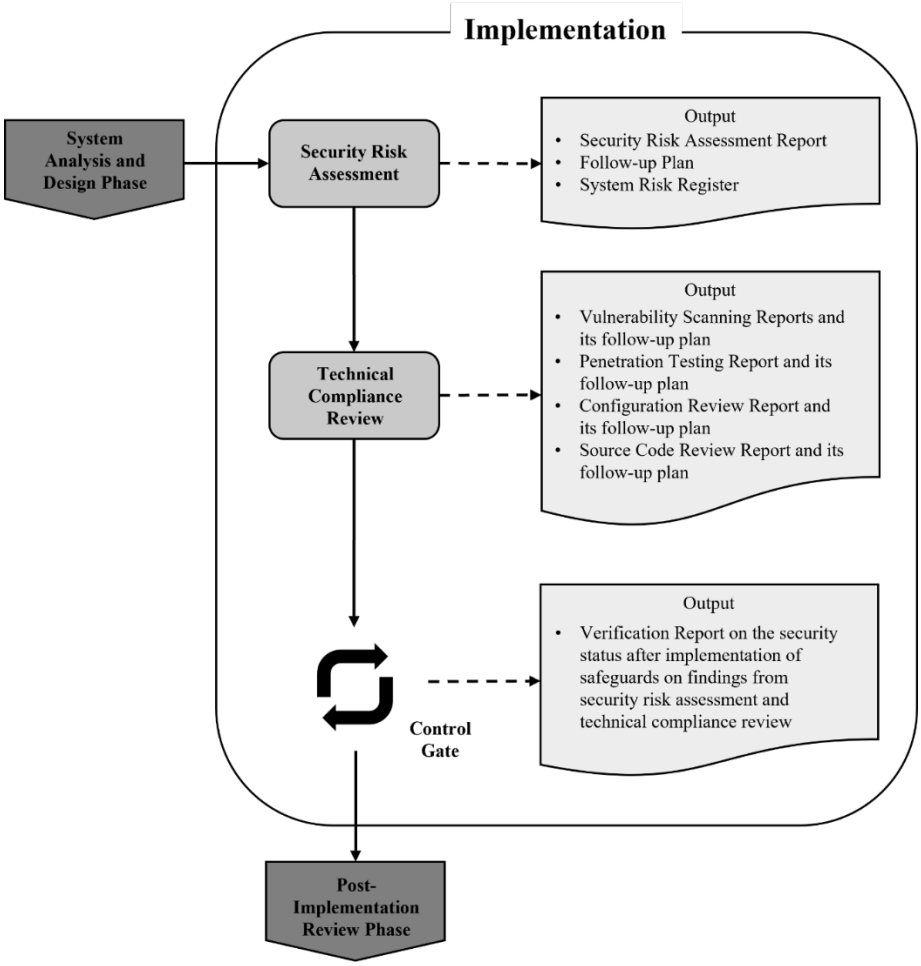

**Figure 7.1 Implementation**

### 7.1.1 Security Risk Assessment

B/Ds should conduct a security risk assessment to identify, analyse and evaluate the security risks and determine the risk treatment measures to reduce the risks to an acceptable level. The assessment process of a system should include the identification and analysis of:

- all assets of, and processes related to, the system
- threats that could affect the confidentiality, integrity or availability of the system
- system vulnerabilities and the associated threats
- potential impacts and risks from the threat activity
- protection requirements to mitigate the risks
- selection of appropriate security measures and analysis of the risk relationships

To obtain useful and more accurate analysis results, a complete inventory list and security requirements for a system should be made available as inputs to the identification and analysis activities. Interviews with relevant parties, such as LAN/System administrators, information owners, users, etc., can also provide additional information for the analysis. Depending on the assessment scope, requirements and methodology, the analysis may also involve automated security assessment tools. After evaluation of all collected information, a list of observed risk findings should be reported. For each observed risk finding, B/Ds should determine appropriate security measures to be deployed before system implementation.

For more information about performing the security risk assessment, please refer to the following document for details:

- **Practice Guide for Security Risk Assessment & Audit**
  Available at ITG InfoStation.
  (https://itginfo.ccgo.hksarg/content/itsecure/techcorner/practices.shtml)

### 7.1.2 Technical Compliance Review

B/Ds should conduct vulnerability scanning, penetration testing, configuration review, and/or source code scanning during implementation. The identified vulnerabilities and issues should be evaluated and addressed with appropriate corrective actions before the system is live-run or in production. B/Ds should

develop a follow-up plan on recommendations with an implementation schedule and review the security status after implementation of safeguards.

For more information about the technical compliance review, please refer to the following document for details:

- **IT Security Guidelines [G3]**
  Available at ITG InfoStation.
  (https://itginfo.ccgo.hksarg/content/itsecure/docs/Guidelines/DocRoadmap.shtml)

## 7.2 Roles and Responsibilities

### 7.2.1 IT Security Management Unit

- Offer advice on the security measures and controls during the system implementation where necessary.

### 7.2.2 Project Manager

- Arrange the security risk assessment and technical compliance review processes.
- Monitor the execution of technical compliance reviews, ensuring that identified vulnerabilities are addressed.
- Ensure recommendations from these assessments are implemented and verified before the system goes live.

### 7.2.3 IT Security Administrators

- Assist in performing security risk assessments and technical compliance reviews.

### 7.2.4 LAN/System Administrators

- Assist in performing security risk assessments and technical compliance reviews, providing system configuration details and applying recommended changes.

### 7.2.5 Application Development & Maintenance Team

- Participate in security risk assessments by providing information on system components and potential vulnerabilities.

- Remediate any vulnerabilities identified during the technical compliance reviews per established timelines.

### 7.2.6 Users

- Assist in security risk assessment and technical compliance review processes by providing user-centric feedback on system security concerns.

## 7.3 Expected Outputs/Deliverables

- Security risk assessment report and its follow-up plan
- System risk register
- Vulnerability scanning report, and its follow-up plan and verification report
- Penetration testing report, and its follow-up plan and verification report
- Configuration review report, and its follow-up plan and verification report
- Source code scanning report and its follow-up plan and verification report

## 7.4 Control Gates

In the implementation phase, the system is built and tested. B/Ds should assess whether the security controls put in place are effective. Recommended control validations include the following:

| Control Validation | Validation Criteria | Control Gate Action |
|---|---|---|
| Documentation of Risks and Mitigations | All identified risks and mitigation strategies are accurately documented in the risk register. | • Review the risk register to ensure completeness and accuracy.<br>• Approve the risk register before proceeding. |
| Consistency with B/Ds' Architecture | Security controls are implemented according to the requirements specified in the design phase. | • Inspect and verify security controls against requirements.<br>• Confirm implementation is correct and complete before moving forward. |
| Completion of Mitigation Actions | All mitigation actions from the security risk assessment and technical compliance reviews are | Validate each mitigation action, ensuring risks are sufficiently mitigated or |

| | | |
|---|---|---|
| | properly addressed and documented. | accepted and formal approval is obtained. |

# 8 Post-Implementation Review

B/Ds should maintain an ongoing management, monitoring, and maintenance mechanism of the deployed systems to ensure the solution's continued security, stability, and optimal performance throughout its life cycle.

## 8.1 Activities

Major activities involved in testing and implementation are as follows:

- Continuous Monitoring
- Change Management

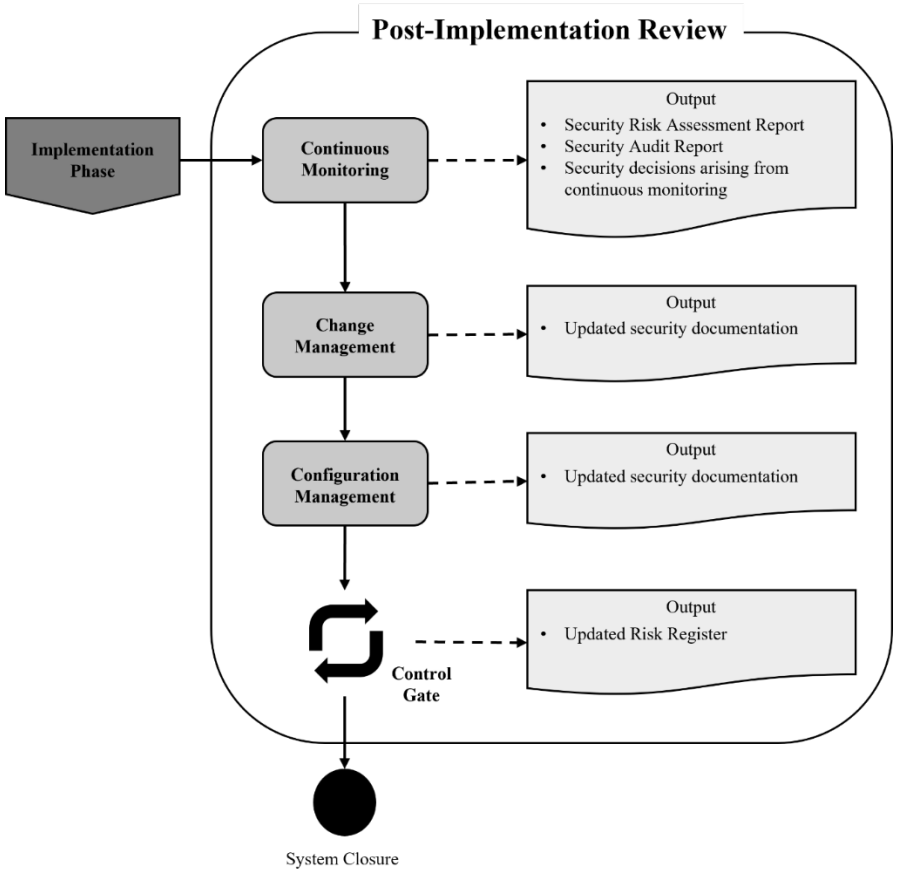


**Figure 8.1 Post-Implementation**

### 8.1.1 Continuous Monitoring

B/Ds should regularly conduct a thorough Security Risk Assessment to evaluate the system's security controls, policies, and procedures, thereby identifying potential vulnerabilities or weaknesses. Continuous monitoring, performed as part of security audits, is a vital activity ensuring the effectiveness of security controls over time, considering both system and environmental changes.

Security Risk Assessments should encompass the technological assets and technical security controls and involve a comprehensive review of security policies, such as those relating to acceptable use and network rights. This process will determine the efficacy of administrative security controls.

Through Security Audits, B/Ds can consistently monitor the security infrastructure to verify that the controls are operating as intended, and modify or update the security measures in response to any findings. This proactive approach ensures that security measures evolve in alignment with the dynamic nature of security threats and the B/D's changing environment.

### 8.1.2 Change Management

B/Ds should manage and execute changes to the system in a controlled and secure manner, underpinned by regularly updated security documentation. Inadequate control of changes to the system is a frequent cause of system or security failures. Any changes to the operational environment, from development through to production phases, can significantly impact the system's security posture.

To address this, B/Ds should:

- ***Document all proposed changes:*** Maintain a detailed record of all proposed system changes and analyse their potential security impacts.
- ***Update security documentation:*** Ensure that any changes to the system are accompanied by updates to security documentation, reflecting the new state of the system and any alterations to security controls or procedures.
- ***Conduct a security impact analysis:*** Before implementing changes, perform a rigorous security impact analysis to understand how alterations may affect the system's security.
- ***Communicate changes:*** Communicate any changes and associated security implications to all relevant stakeholders and update training materials to include new security practices.
- ***Monitor post-implementation:*** After implementing a change, monitor the system to verify that security controls are still effective and that the updated

documentation accurately represents the system's new state.

Through this process, B/Ds will ensure that the system remains secure and that all stakeholders have access to the most current and accurate security information, facilitating informed decision-making and maintaining the integrity of the security posture throughout the change management life cycle.

### 8.1.3 Configuration Management

Configuration Management is essential for establishing and maintaining a secure baseline of the system, controlling and keeping an accurate inventory of system changes. Since changes to system configuration can significantly impact security, it is important to integrate updated security documentation within the Configuration Management process. Key considerations and best practices include:

- ***Maintaining an Updated Baseline:*** Establish and document a baseline of configuration items, ensuring this baseline is updated whenever changes are made. The documentation should reflect the current state of system configurations at all times.

- ***Continuous Monitoring with Documentation Updates:*** Conduct continuous monitoring and regular audits of configuration changes, updating security documentation to capture any alterations to the system configuration. This ensures that all changes are tracked and assessed for their security impact.

- ***Documented Procedures for Backup and Recovery:*** Implement and document configuration backup and recovery procedures. Updated security documentation should include recovery processes, roles, responsibilities, and timelines to ensure rapid restoration in the event of a configuration-related incident.

- ***Inclusion of Configuration Changes in Security Documentation:*** Ensure all approved configuration changes are promptly reflected in the security documentation. This includes documenting the justification for changes, the security impact analysis, and any mitigations implemented.

- ***Automated Tools and Manual Reviews:*** Leverage automated scanning tools and conduct manual review exercises as documented in the security procedures to verify that configurations are properly set up and adhere to security best practices. The results of these tools and reviews should be documented and used to update security baselines and practices.

Configuration Management's goal is to identify and rectify potential misconfigurations that could introduce vulnerabilities, thereby compromising the security of information systems. By ensuring that updated security documentation is an integral part of Configuration Management, B/Ds can maintain robust security postures that are responsive to change and reflect the latest configuration states.

## 8.2 Roles and Responsibilities

### 8.2.1 IT Security Management Unit

- Advise on the security aspects of change management and configuration management practices.

### 8.2.2 Information Owner

- Ensure the information's security classification is considered during continuous monitoring, change and configuration management activities.

### 8.2.3 IT Security Administrators

- Lead the continuous monitoring activities to identify and assess potential vulnerabilities.
- Perform assessment of potential impact on the security of the system arising from the system change.
- Perform assessment of potential impact on the security of the system arising from the configuration change.
- Assist with implementing approved changes and configuration adjustments.

### 8.2.4 LAN/System Administrators

- Implement configuration changes and security patches as part of change management directives.
- Support continuous monitoring efforts by maintaining operational security controls.

### 8.2.5 Application Development & Maintenance Team

- Ensure that changes from continuous monitoring feedback are incorporated securely.
- Manage configuration changes in the development and maintenance of applications.

### 8.2.6 Users

- Participate in continuous monitoring by reporting any anomalies or security issues encountered.
- Comply with new configurations or changes as part of change management communication.

## 8.3 Expected Outputs/Deliverables

- Security risk assessment report and its follow-up plan
- Security audit report and its follow-up plan
- Security decisions arising from continuous monitoring
- Updated security documentation
- Updated risk register

## 8.4 Control Gates

While using the system, B/Ds should regularly reassess its status based on user feedback, technology changes, policy changes, new threats and vulnerabilities and other business-related issues. Recommended control validations include the following:

- Validation of security risk assessment and security audit reports to ensure that systems and environmental changes are addressed.
- Regular review of previous security risk assessment reports and risk register to ensure that risks remain valid and are continually addressed.

| **Control Validation** | **Validation Criteria** | **Control Gate Action** |
|---|---|---|
| Continuous Monitoring Activities | • Effectiveness of built-in controls.<br>• Timeliness and accuracy of monitoring reports. | • Adjust monitoring strategies as needed.<br>• Update control configurations.<br>• Provide training on new threats. |
| Validation of Security Risk Assessment and Audit Reports | • Relevance and coverage of risks.<br>• Adequacy of controls in light of system/environment changes. | • Update risk assessment methodologies.<br>• Remediate identified gaps.<br>• Escalate critical risks to senior management. |
| Rgular Review of Previous Security Risk | • Validity of previous risk assessments. | • Prioritise risks for action. |

| | | |
|---|---|---|
| Assessments and Risk Register | • Current status of risks in the risk register. | • Allocate resources for risk mitigation.<br>• Update risk register. |