Security-by-Design Framework

Version: 1.0

Document History

Version No.	Date	Author	Changes
1.0	09 November 2017	Cyber Security Agency of Singapore	Release

Contents

1. Introduction

1.1 Most organisations adopt a Systems Development Lifecycle (SDLC) methodology for the development and implementation of computer systems. SDLC is a multi-step lifecycle process to deliver computer systems to ensure good-quality systems that meet specifications and, within time and cost estimates.

1.2 While most organisations acknowledge that security is an important consideration in developing computer systems, costs and business performance often take precedence over security. Even though awareness has been elevated on security issues, most organisations focus on applying security only at the commissioning stage of the system development and try to forced fit security into the final design, resulting in ineffective application of security.

1.3 An effective way to protect computer systems against cyber threats is to integrate security into every step of the SDLC, from initiation, to development, to deployment and eventual disposal of the system. This approach is the Security-by-Design (SBD) approach.

1.4 Security-by-Design is an approach to software and hardware development that seeks to minimise systems vulnerabilities and reduce the attack surface through designing and building security in every phase of the SDLC. This includes incorporating security specifications in the design, continuous security evaluation at each phase and adherence to best practices. The values of integrating security into SDLC include:

- Early identification and mitigation of security vulnerabilities and misconfigurations of systems.
- Identification of shared security services and tools to reduce cost, while improving security posture through proven methods and techniques.
- Facilitation of informed key stakeholder decisions through comprehensive risk management in a timely manner.
- Documentation of important security decisions throughout the lifecycle of the system, ensuring that security was full considered during all phases.
- Improved systems operability that would otherwise be hampered by isolated security of systems.

1.5 Specific to cybersecurity, Security-by-Design addresses the cyber protection considerations throughout a system's lifecycle. This includes security design specifically for the identification, protection, detection, response and recovery capabilities to strengthen the cyber resiliency of the system.

2. Purpose

2.1 This document establishes a framework to guide organisations in building security into their SDLC, through the alignment of security-related processes/activities alongside SDLC processes. This would result in more cost-effective and risk-appropriate security considerations and controls in all phases of the SDLC.

The objectives of this document are to:

(a) Establish a Security-by-Design framework that stakeholders can take reference where Security-by-Design approach is mandated.

(b) Establish SBD processes to ensure that security risks are managed from the start, and continuously assessed during the SDLC through a lifecycle approach.

(c) Establish activities to support the SBD processes to manage security risks during the SDLC.

(d) Provide control gates and decision point considerations at phases to ensure that no decision is made without an assessment of the security risks.

3. Scope and Applicability

3.1 This document covers the framework overview and provides approaches and guidelines to processes and activities for the Security-by-Design approach within a SDLC.

3.2 The framework, processes, activities and control gates described in this document are applicable to all computer system development projects. “Computer system” refers to all systems and network infrastructures including: Infocomm Technologies, Operational Technologies and Internet of Things (IoT).

3.3 The framework is intended to be used in conjunction with any existing SDLC methodologies adopted by organisations, as well as complementing government policies, standards, guidelines and directives.

3.4 Detailed technical implementation of the security activities described under the framework can be adopted from relevant organisation standards or IT standards bodies (e.g. NIST, ISO/IEC, IEEE).

4. Audience

4.1 This document covers details specific to secure systems development. The reader of this document should be acquainted with general systems development lifecycle and security concepts; however, the document provides the necessary background to understand the topics that are discussed.

4.2 The intended audience of this document is varied and includes the following:

- Critical Information Infrastructure (CII) and government systems development projects that requires the adoption of Security-by-Design development process.
- Security professionals, systems developers, systems administrators, and others who are responsible for planning, implementing, maintaining, monitoring and disposal of the systems in their organization that wants to adopt Security-by-Design into their development process.
- Senior management who are trying to understand the benefits of applying Security-by-Design to the systems in their organization.
- Vendors, external consultants that are developing solutions and products that will be deployed to systems that requires the adoption of Security-by-Design development process.

5. Framework Overview

5.1 Systems Development Lifecycle (SDLC)

5.1.1 It is important to understand the basics of the SDLC in order to appreciate how this framework complements SDLC.

5.1.2 SDLC is the overall process for developing systems from initiation through implementation to disposal. There are many activities associated with each phase of the SLDC. While the activities performed in each systems development project may vary, a typical SDLC begins with a business need and ends when the maintenance costs outweigh the benefits of the system, hence, a 'lifecycle'.

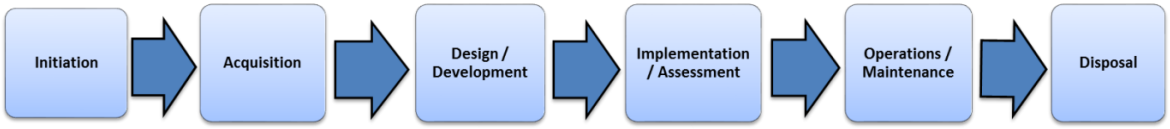

Figure 1: Systems Development Lifecycle

5.1.3 SDLC comprises of six phases:

1. **Initiation** – The need for a system is expressed and the functional specifications of the system are documented.

2. **Acquisition** – The system is purchased through the procurement process.

3. **Design/Development** – The system is designed, programmed, developed, or otherwise constructed.

4. **Implementation/Assessment** – The system is installed, tested, accepted for release and commissioned.

5. **Operation/Maintenance** – The system is operational and producing the work as per specification. Modifications and enhancements are managed through change management process. Maintenance of the hardware, software and system upgrades.

6. **Disposal** – When the system is redundant or obsolete, the system will be disposed. Orderly termination of the system, safeguarding vital systems information, and migrating data to a new system, or preserving it in accordance with applicable records management regulation and policies.

5.1.4 Different SDLC methodologies may be adopted by organisations. For example, the Whole-of-Government (WoG) adopts the IM8's IT Project Lifecycle[1], while in MINDEF, a similar lifecycle approach called the Defence Capability Management (DCM) Framework[2], is adopted. A mapping of these SDLC methodologies against SDLC phases is shown in Figure A-3 of ANNEX A. Regardless, the six phases of the SDLC should be generic across all SDLC methodologies.

5.2 Notes on Agile Development Lifecycle

5.2.1 Section 5.1 above describes a conventional SDLC model (Waterfall model). More and more, organisations are adopting another SDLC model called Agile Development Lifecycle. Agile Development Lifecycle describes a set of principles for systems development under which requirements and solutions evolve through the collaborative effort of self-organising cross-functional teams. It arises as a need to develop quick iterations of working systems to users who have changing requirements and priorities.

[1] Figure A-1 - IT Project Lifecycle (IM8)
[2] Figure A-2 - DCM Framework

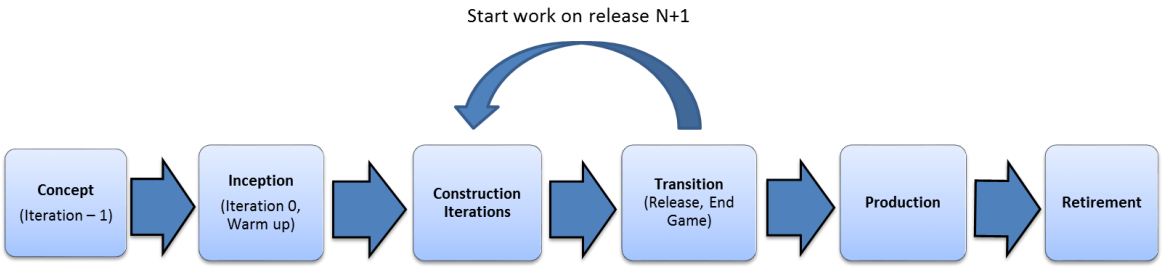

Figure 2: Agile Development Lifecycle

5.2.2 Agile development lifecycle comprises of six phases:

1. **Concept** – This is a pre-iteration phase where the need for a system is expressed and the functional specifications of the system are documented.

2. **Inception/Warmup** – The first week of an agile project is often referred to as Iteration 0 and is used to setup the environment, and gather support and funding for the project.

3. **Construction Iterations** – The system is incrementally and iteratively delivered which meets the changing needs of the stakeholders. Continual testing is also performed during this phase.

4. **Transition** – Final testing and rework are performed on the system before it is released into production. Finalised documentation and training are also performed at this phase.

5. **Production** – The system is operational and producing the work as per specification. Modifications and enhancements are managed through change management process. Maintenance of the hardware, software and system upgrades are also performed at this phase.

6. **Retirement** – When the system is redundant or obsolete, the system will be disposed. Orderly termination of the system, safeguarding vital systems information, and migrating data to a new system, or preserving it in accordance with applicable records management regulation and policies are performed at this phase.

5.2.3 The SBD Framework, described in this document, is adaptable to the Agile development lifecycle. Refer to Figure A-4 of ANNEX A for the mapping of Security-by-Design lifecycle processes against the Agile development lifecycle.

5.3 Security-by-Design Lifecycle

5.3.1 The emphasis of the SDLC is to ensure effective development of a system and often security becomes an afterthought in the development. Addressing inherent vulnerabilities and patching security holes as they are found can be a hit-and-miss process and costly; and, will never be as effective as designing systems to be secure from the start.

5.3.2 The SBD lifecycle parallels the SDLC phases by incorporating security considerations into processes at every phase. It spans across all the phases as security risks will need to be identified as early as the planning phase and addressed accordingly throughout the phases. At a broad level, security risks can be addressed through:

(a) Changing the requirements or deployment to avoid the security risk

(b) Implementing alternative or mitigating controls

(c) Accepting the risk through proper risk management process

(d) Iterative processes where security are evaluated at each phase and determined whether the security processes are required to be repeated to produce a satisfactory output.

5.3.3 The advantage of introducing security alongside each SDLC phase is to ensure that security risks are visible, well understood by senior management and key personnel, and appropriate decisions are taken timely to reduce risk to an acceptable level.

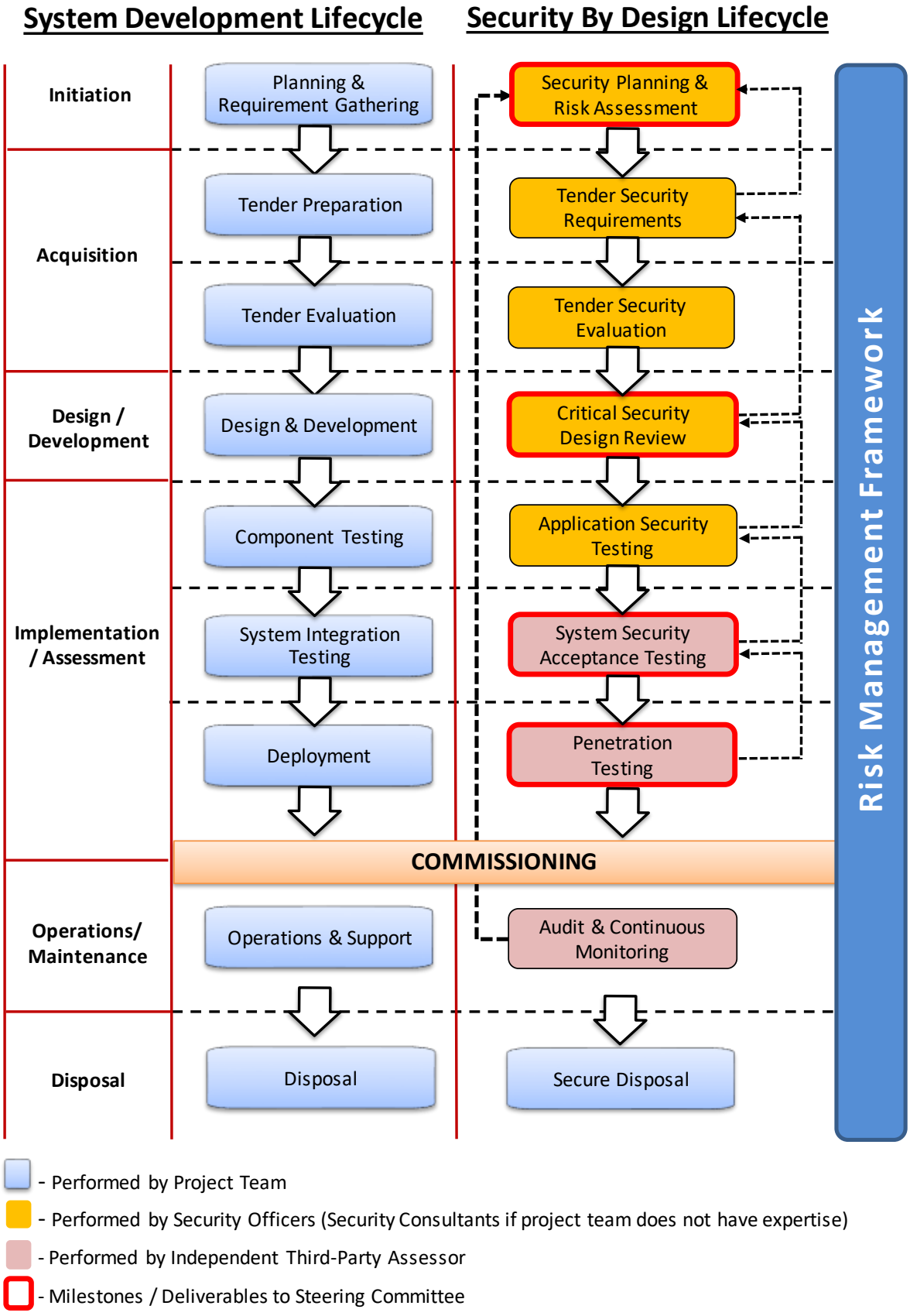

Figure 3: SDLC / Security-by-Design Lifecycle

5.4 Security-by-Design Approach

5.4.1 The SBD approach consists of three components, namely,

a. **Lifecycle** - Aligning security-related processes with SDLC to guide projects to meet Security-by-Design objectives

b. **Activities** - Security-related activities that support the security lifecycle processes

c. **Control Gates** - A point in time when the system development effort will be evaluated for security and when management will determine whether the project should continue as is, change direction or be discontinued

5.4.2 Figure 4 below, shows the hierarchical relationship of the processes, activities and control gates.

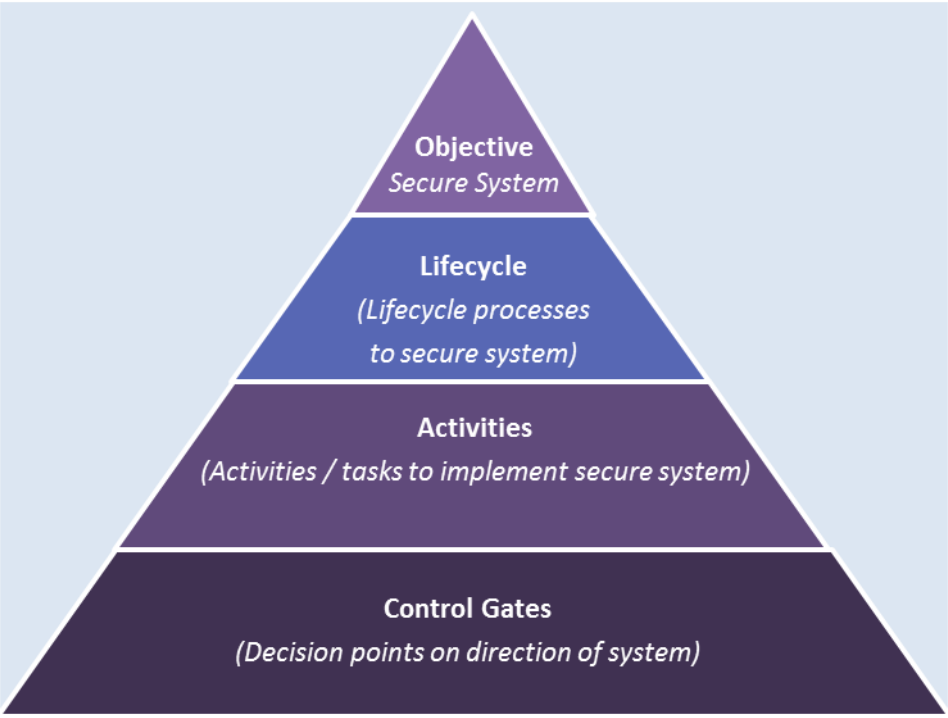

Figure 4: Security-by-Design Approach

5.4.3 The SBD approach ensures security considerations are addressed at every phase through the security lifecycle processes. Activities within these security processes focus on adding security elements that should be present in any SDLC methodologies.

5.4.4 SBD processes begin early in the SDLC phase and are important in shaping the security capabilities and posture of the computer system throughout the SDLC phases. If these processes are not performed adequately at each phase of the SDLC, they may be costlier to implement later.

5.5 Security-by-Design Framework

5.5.1 The SBD Framework (illustrated in Figure 5 below) provides a disciplined and structured approach that integrates security processes into the SDLC.

5.5.2 While the approach diagram in Figure 4 shows a hierarchical relationship of the processes, activities and control gates, Figure 5 below maps the framework processes and activities against the phases.

5.5.3 Each process can be repeated if the output is unsatisfactory and if there are significant changes to the project, the security of the project should be re-evaluated from the initiation phase.

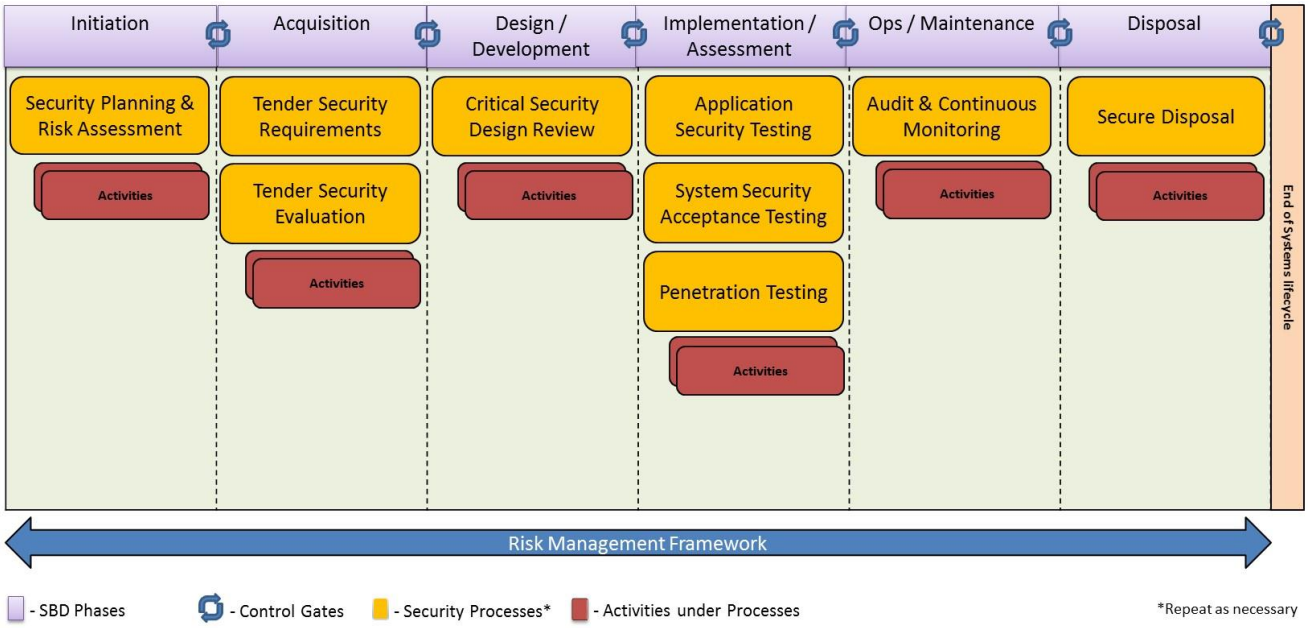

Figure 5: Security-by-Design Framework

5.5.4 In addition, the framework requires that risks be continually managed through a risk management framework. For SBD approach to be effective, organisations must have a consistent and effective risk approach applied to all security processes.

5.5.5 The risk management framework can be part of an organisation-wide risk program that involves the management of organisation risk; that is, the risk to the organisation associated with the operation of a computer system.

5.6 Security Processes

5.6.1 In Figure 5 above, nine security processes are identified within the lifecycle, each corresponding to a SDLC process. These processes map into the six distinct phases to provide security guidance throughout the lifecycle of the system.

5.6.2 At the end of each security process, one or more deliverables are produced as outputs and could be fed as inputs to the subsequent process. Key processes (depicted with red outline), under Figure 3, have key milestones / deliverables that must be approved and accepted by the appropriate approving authority, e.g. steering committee, before a project can proceed to the next phase. The lifecycle of a system ends when it has been securely disposed of and formally closed.

5.6.3 The security processes can be iterative if, at the control gates, the security activities are found to be inadequate and need to be re-performed to meet security requirements.

5.7 Activities

5.7.1 Under each security process is a set of security-focused activities that describes the key security actions to be taken. Figure 6 below, highlights how the activities are aligned with, and performed within each SBD Security Process.

5.7.2 Each activity will minimally cover the following:

(a) Description – Describe the actions to be taken in parallel with SBD processes and activities.

(b) Roles and Responsibilities – Describe key roles and responsibilities within each activity and the actions that they are responsible for.

(c) Expected Outputs – Describe the required security-related artefacts that are expected from this activity, which may be inputs into other related activities.

(d) Inter-dependencies – Describe the Inter-dependencies with other SDLC / SBD activities and outputs and how they work together to enhance security of the system.

5.7.3 The level of details of each activity shall provide sufficient guidance on (a) the objective of the activity, (b) key roles and responsibilities, (c) expected outputs to ensure adequate security has been performed, and (d) shows inter-dependencies with SBD processes and activities in order to enhance the security development of the system.

5.8 Control Gates

5.8.1 Control Gates or decision points are specific milestones of the SBD phases where the security implementations are evaluated. They provide the organisation with an opportunity to verify that security considerations are addressed, adequate security controls are built in, and identified risks are clearly understood before the system development advances to the next lifecycle phase.

5.8.2 At these milestones, the project manager should present the pre-determined deliverables to approving authority (i.e. project steering committee and system owner). The approving authority should be briefed on the status of the security implementation and validation results, and approved any changes to security implementations or schedule.

5.8.3 Approving authority, for example the project steering committee, shall ensure that they are adequately advised on security control matters. For example, having independent security subject matter expert in the committee or as advisor to the committee.

6. Security-by-Design Framework Implementation

This section describes in detail how to implement the SBD Framework using the lifecycle approach. Each phase will be described and organised in the manner below:

- The Phase within the context of Security-by-Design.
- The Security Process and its objective.
- The Activities underpinning the Security Process and defining the expected outputs.
- The Control Gate for validation of activities. The objectives of the control gate and check points at the control gate will be described.

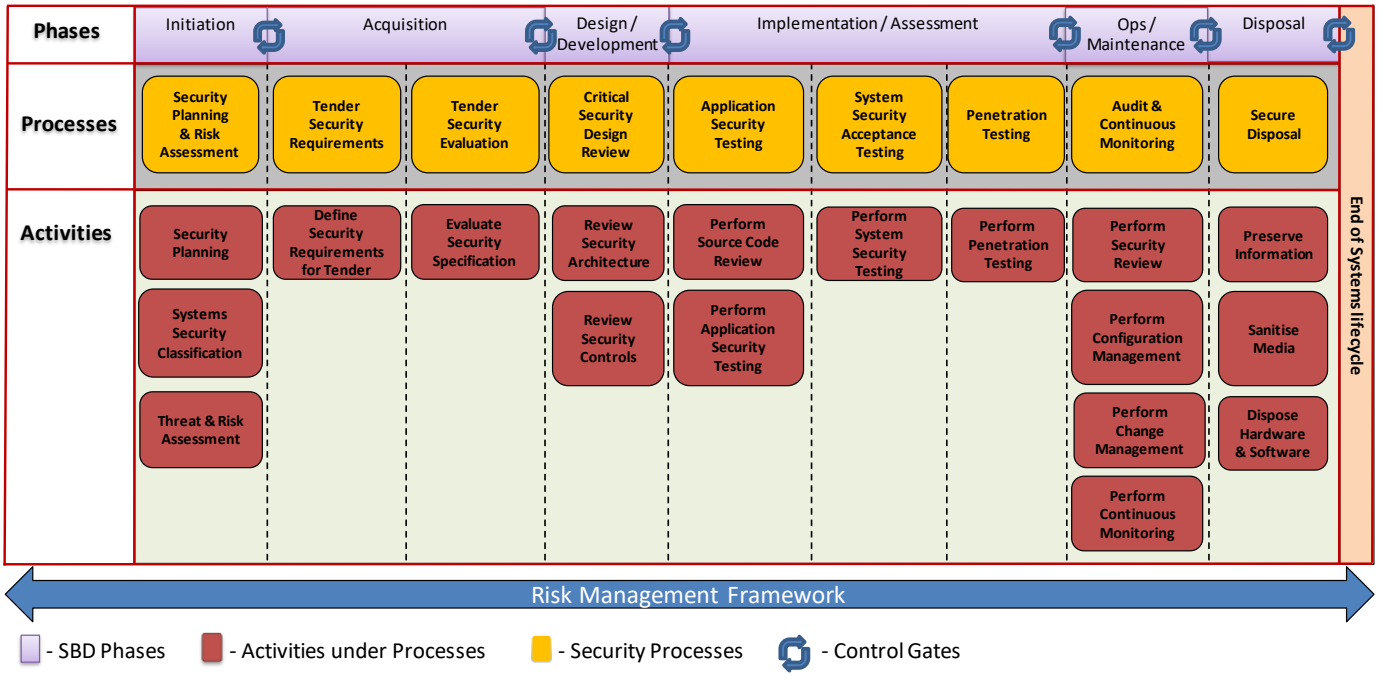

Figure 6: Phase/Process / Activity Mapping

6.1 Phase: INITIATION

At the Initiation phase, early integration of security considerations is key to the success of the implementing a secured system. Threats, security requirements and potential constraints of functionality and integration are considered at this phase. Security is looked at from the perspective of business risks with inputs from the security team.

Security Process	Activities
Security Planning & Risk Assessment	Security Planning
	Systems Security Classification
	Threat & Risk Assessment

6.1.1 Security Process: Security Planning and Risk Assessment

The Security Planning and Risk Assessment process within the Initiation phase aims to integrate security considerations at the start of SDLC. Activities under this process include:

- Security planning to set common understanding of security goals and objectives, identify key security roles and develop high level security schedule.
- Classify system to the appropriate security classification.
- Threat and Risk Assessment to ensure threats, risk, and security decisions are documented, assessed, and approved by key stakeholders.

Through proper security threat identification and risk management planning early in the lifecycle, cost-effective security can be established.

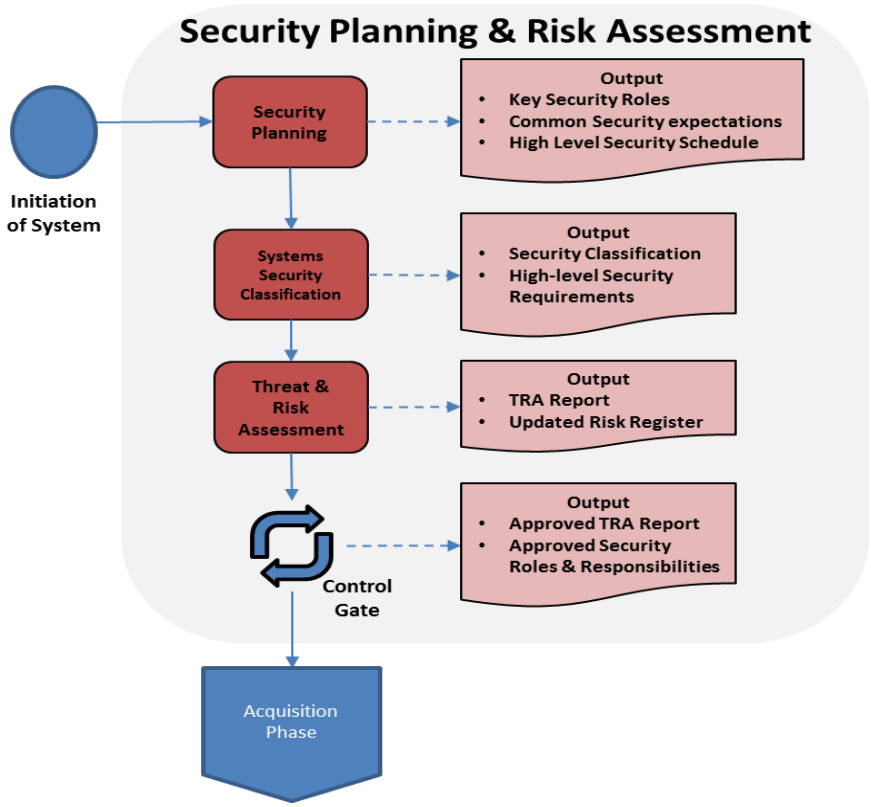

Figure 7: Security Planning and Risk Assessment

6.1.1.1 Activity: Security Planning

Description:	Security planning is to be conducted as part of the initiation and planning phase. It includes: • Identifying and confirming key security roles in the system development project • Ensuring all key stakeholders have a common understanding of the goals, implications, considerations and requirements of performing security • Outlining key security milestones and activities for the system development. • Identifying the use of secure design, architecture and coding standards. This planning activity is crucial as it highlights to key stakeholders that as the systems development progress, decisions made will have security implications.
Roles and Responsibilities[3] :	Project Manager The Project Manager is responsible to identify and confirm the key security roles that must be present in this project. This may

[3] Detailed overview can be found in ANNEX B – Roles and Responsibilities

	include whether the security assessment is performed in-house or outsourced. The Project Manager is also responsible to outline key security milestones and activities with inputs from the Security Officer / Consultant. Developer The Developer is consulted as part of security planning to ensure that key security milestones and activities is aligned with the system development. The Developer is also consulted on the design, architecture and coding standards so as to be aligned against secure practices. Security Officer / Consultant The Security Officer, or Consultant if the security assessment is outsourced, is responsible to ensure that all key stakeholders have a common understanding of security concepts and that everyone is speaking the "same language". System Administrator The System Administrator's role in this activity is to understand the current standards and practices. This activity provides the System Administrator a common understanding of security expectations required for this development. Users N.A.
Expected Outputs:	• Key security roles and resources for the system development • Common understanding of security expectations • High level schedule of security milestones and activities
Inter-dependencies:	The security milestones and activities should be integrated into the project schedule to ensure proper security planning is performed.

6.1.1.2 Activity: System Security Classification

Description:	In order to perform threat and risk assessment, it is important to first determine the security classification of the system. The security classification will be used in conjunction with the threats and vulnerability information in assessing the risks.

Roles and Responsibilities:	Project Manager The Project Manager is responsible to ensure that the system is appropriately classified and hence its information will be protected accordingly throughout the systems development project. Developer The Developer provides input to the high-level security requirements that needs to be fulfilled as per the security classification. Security Officer / Consultant The Security Officer / Consultant is responsible to classify the security classification of the system based on the protection of classified information and provide the high-level security requirements that needs to be fulfilled as per the security classification. System Administrator The Systems Administrator provides input to the high-level security requirements that needs to be fulfilled as per the security classification. Users The Users provide input to the types and security classification of information that they will be assessing from the system.
Expected Outputs:	• Security classification of the system • High-level Security Requirements that needs to be fulfilled as per the security classification
Inter-dependencies:	The security classification of the proposed system should be communicated to the system architect team so that the team put in appropriate level of security in the architecture design.

6.1.1.3 Activity: Threat and Risk Assessment

Description:	Threat and Risk Assessment (TRA) is the systematic process of identifying the various threats and vulnerabilities to systems, determining the level of risk these systems are exposed to, and recommending the appropriate level of protection.

	The objective of TRA is to maximise the protection of confidentiality, integrity and availability while minimising risk. A typical TRA includes: • Review of functional requirements specification • Threats and vulnerabilities identification • Risk identification, analysis and evaluation • Recommendations of appropriate security controls TRA must take into consideration to all relevant regulatory practices and standards.
Roles and Responsibilities:	<u>Project Manager</u> The Project Manager is responsible to ensure that the TRA is performed adequately and completed and all inputs from stakeholders are considered. <u>Developer</u> The developer provides input to the TRA on threats and risk pertaining to systems development. <u>Security Officer / Consultant</u> The Security Officer / Consultant is responsible to perform the TRA to determine the level of risk these systems are exposed to, and recommending the appropriate level of protection. <u>System Administrator</u> The Systems Administrator provides input to the TRA on threats and risk pertaining to operations and systems administration. <u>Users</u> The Users provide input to the TRA on threats and risk pertaining to their business operations.
Expected Outputs:	• TRA report detailing the potential threats and risks that could impact the organisation business and the security controls needed to be put in place to reduce the risks to an acceptable level. • Updated Project Risk Register addressing cyber risks.
Inter-dependencies:	The security classification of the proposed system has to be considered when performing TRA.

6.1.2 Control Gates

The approving authority for this phase is the Steering Committee. Recommended control validations for this phase include:

- Threat and Risk Assessment Report that is approved by steering committee. This is the main deliverable for this phase. It will be used extensively to develop the security requirements, controls and design of the system.
- Checking if all high level security requirements been included or expressed as a set of security controls in the Threat and Risk Assessment Report.
- Checking if the security team roles and responsibilities been established.
- Evaluate if the project is supported with the security resources currently available or projected to be available in the timeframe desired.

6.1.3 Key Milestone

The TRA report is a key milestone that needs to be approved by the project steering committee prior to the submission of tender requirements.

6.2 Phase: ACQUISITION

The Acquisition phase of the development lifecycle is concerned primarily with the identification of security requirements, evaluation of proposed security controls, and reviewing and finalising security design prior to acquiring or developing the system. Key security processes for this phase looks at:

- Deriving security design objectives and specifications for tenders
- Evaluating and assessing adequacy of proposed security controls of submitted proposals in meeting requirements in the tender

Security Process	Activities
Tender Security Requirements	Define Security Requirements for Tender
Tender Security Evaluation	Evaluate Security Specification

6.2.1 Security Process: Tender Security Requirements

The purpose of the Tender Security Requirements process is to determine and produce a set of security specifications for the purpose of the tender. The security

requirements are part of the overall system requirements that need to be approved for tender submission.

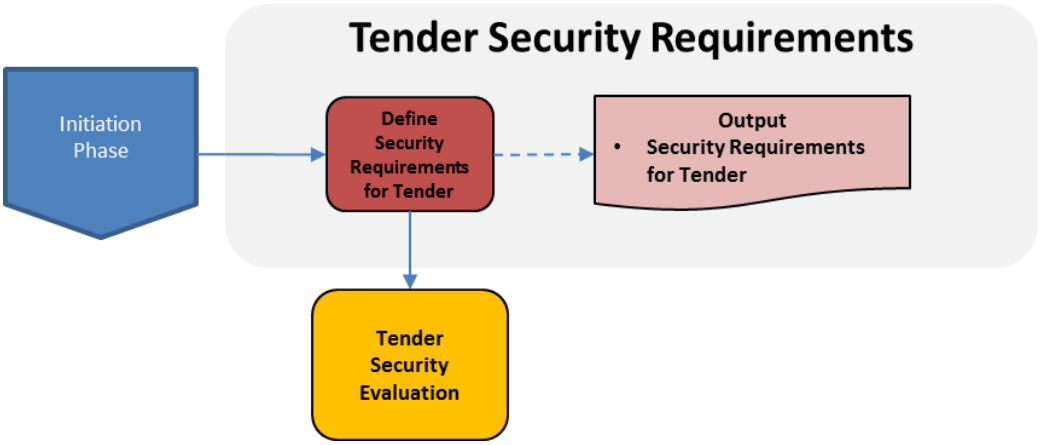

Figure 8: Tender Security Requirements

6.2.1.1 Activity: Define Security Requirements for Tender

Description:	Security Requirements are defined and refined as part of the overall tender requirements submission. Security requirements should be clearly articulated, its purpose and objective clearly stated, so that tenderers are able to provide adequate measures or controls to meet the requirements. Security requirements should also include organisation security standards or references from International Standards (e.g. ISO2700X standards), which are minimum security controls that must be put in place to protect systems in the area of Confidentiality, Integrity and Availability.
Roles and Responsibilities:	Project Manager The Project Manager is responsible to ensure that the defined security requirements are aligned with the main tender requirements so that security integration activities will be not negatively impacted by other IT processes. Developer The Developer provides input to the Security Officer / Consultant to define the security requirements. Security Officer / Consultant The Security Officer / Consultant is responsible to define and refine security requirements as part of the overall tender requirements submission. The security requirements should be

	clearly articulated, its purpose and objective clearly stated and aligned with the main tender requirements. <u>System Administrator</u> The Systems Administrator provides input to the Security Officer / Consultant to define the security requirements. <u>Users</u> Users are consulted on the security requirements that will be defined, against the business requirements under the main tender.
Expected Outputs:	• Approved Security Requirements for Tender
Inter-dependencies:	This activity feeds security requirements directly into the main tender requirements and should be performed alongside the SDLC requirements gathering activity to ensure that security integration activities are not negatively impacted by other IT processes. The Threat and Risk Assessment Report is a primary tool to identify if the security requirements are effective to address an organisation's risk tolerance.

6.2.2 Security Process: <u>Tender Security Evaluation</u>

The process of Tender Security Evaluation occurs after the tender submissions have been received and is an integral part of the overall evaluation of the tender submissions.

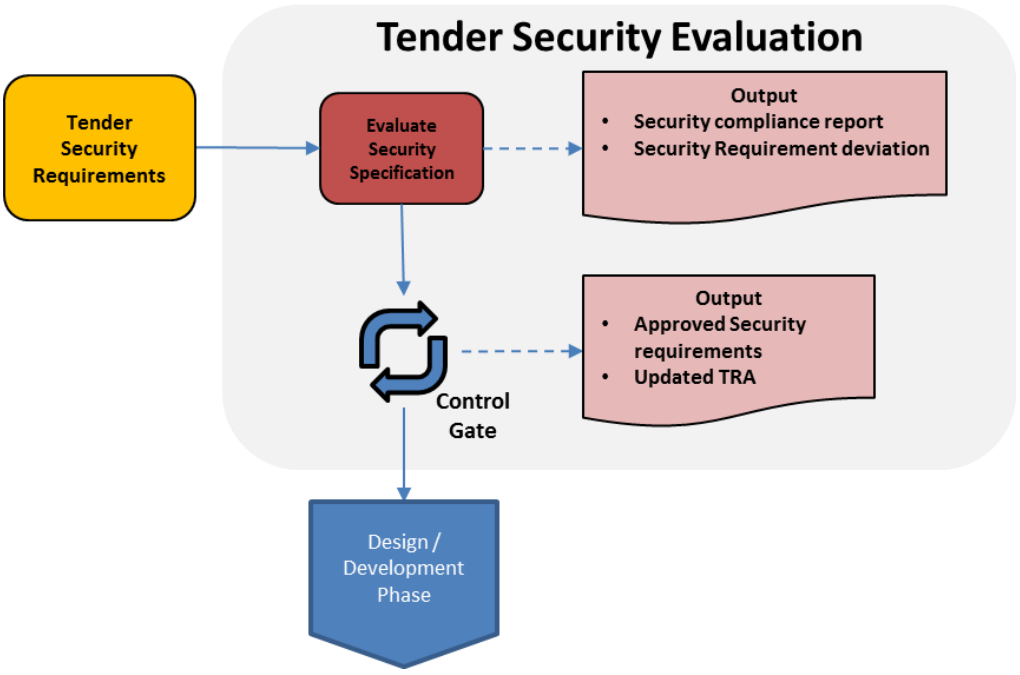

Figure 9: Tender Security Evaluation

6.2.2.1 Activity: Evaluate Security Specification

Description:	This activity focuses on the assessing of security control specifications proposed by the vendors. The activity includes a series of documentation review, proposal evaluation and clarifications, assessment of security controls proposed. It may include software/hardware demonstrations and testing which the controls involve software and/or hardware solutions. Recommendations are incorporated into the Tender Evaluation Report.
Roles and Responsibilities:	Project Manager The Project Manager is responsible to ensure that security evaluation recommendations are completed and incorporated into the Tender Evaluation Report. Developer The Developer is responsible to review the vendor's security controls proposal and to provide recommendations to the security evaluation recommendations. Security Officer / Consultant

	The Security Officer / Consultant is responsible to review the vendor's security controls proposal and complete the security evaluation recommendations based on the compliance and deviations of security requirements. The Security Officer / Consultant should also take inputs from other stakeholders' recommendations. <u>System Administrator</u> The System Administrator is responsible to review the vendor's security controls proposal and to provide recommendations to the security evaluation recommendations. <u>Users</u> N.A.
Expected Outputs:	• Assessment and Recommendations for incorporation into the Tender Evaluation Report
Inter-dependencies:	This activity should be performed closely with the overall system tender evaluation to ensure that the security requirements are reviewed and assessed appropriately.

6.2.3 Control Gates

The objective of this control gate is to match the security requirements expressed against the security functionality defined by the vendors. All security controls should be included in the vendor proposal. The approving authority of the control gate is the Steering Committee.

Recommended control validations for this phase include:

- All the agreed upon security controls been included in the vendor proposal.
- Vendor's planned activities and outcome are compliant with organisation security policy and procedures.
- Formal key stakeholder acceptance of the risks based on the vendor proposal.

6.3 Phase: <u>DESIGN / DEVELOPMENT</u>

The design / development phase begins after the tender has been awarded. As part of the design of the system, critical security design review shall be conducted to check that the system architecture is secured and appropriate security controls are put in place in the design of the system.

Security Process	Activities
Critical Security Design Review	Review Security Architecture
	Review Security Controls

6.3.1 Security Process: Critical Security Design Review

The Critical Security Design Review focuses on the review of security systems architecture and controls. This process ensures that security requirements and controls are met through the systems design and can be implemented to meet security requirements.

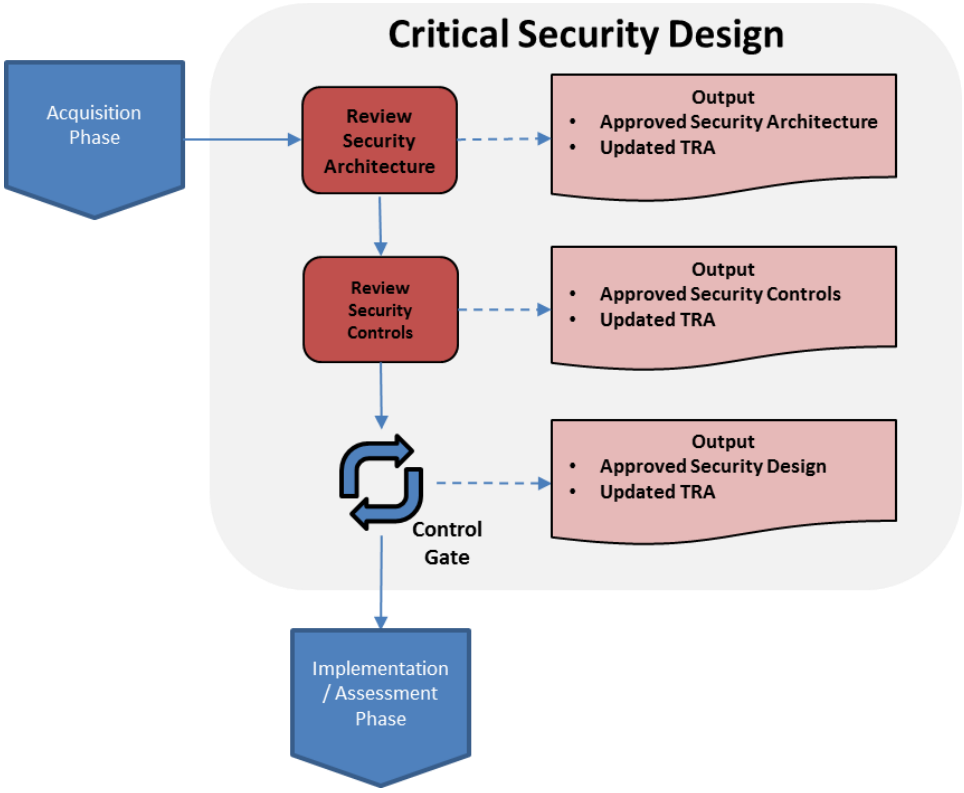

Figure 10: Critical Security Design

6.3.1.1 Activity: Review Security Architecture

Description:	This activity focuses on the security review of system architecture. The systems architecture should be decomposed into finer components and its inner workings must be documented. This is to identify trust boundaries, information entry and exit points and data flows. It includes a series of architecture documentation reviews, design vulnerability assessments and security recommendations.

Roles and Responsibilities:	Project Manager The Project Manager is responsible to ensure that the Security Officer / Consultant has the resources and documentation required in order to perform adequate security review of the system architecture. Developer The Developer provides inputs to the security review of the system architecture. Security Officer / Consultant The Security Officer / Consultant is responsible to perform a security review of the system architecture with inputs from stakeholders. System Administrator The System Administrator provides inputs to the security review of the system architecture. Users The User provides inputs to the security review of the system architecture.
Expected Outputs:	• Approved Security Architecture
Inter-dependencies:	The activity should be performed with systems architecture review to ensure that the security design is congruent with the functions of the proposed architecture. This activity should also be iteratively performed whenever changes are made to the architecture.

6.3.1.2 Activity: Review Security Controls

Description:	This activity focuses on the review of security controls put in place as part of the systems design. The activity includes a series of documentation review of security controls proposed in the system design, assessment of its effectiveness and recommendations. Security Controls must be justified and documented based on the TRA and security requirements. Security Controls must be sufficiently documented to enable verification of the controls'

	adherence to security requirements. An analysis of the cost of implementing a potential security control should also be documented.
Roles and Responsibilities:	<u>Project Manager</u> The Project Manager ensures that selected Security Controls are justified and sufficiently documented for the Steering Committee to make appropriate decisions. <u>Developer</u> The Developer provides input to the Security Officer / Consultant to the review of security controls. <u>Security Officer / Consultant</u> The Security Officer / Consultant, in consultation with the Developer and System Administrator, is responsible to document security controls that must be put in place as part of systems design. <u>System Administrator</u> The System Administrator provides input to the Security Officer / Consultant to the review of security controls. <u>Users</u> N.A
Expected Outputs:	• Approved Security Controls
Inter-dependencies:	Security Controls should be matched against the approved security requirements. The security controls selected should mitigate security risk adequately for all business processes and the systems that support these processes.

6.3.2 Control Gates

Prior to the development of the system, the proposed security design and controls must be validated and accepted by key stakeholders. Updates and changes to the initial risk assessment must be updated to reflect changes to security requirements and design.

Recommended control validations for this phase include:

- The system design is consistent with the enterprise architecture, including the security components of that architecture.
- The system design addresses the agreed upon security requirements.
- The TRA Report reflects the updated risks after consideration of the security architecture, security controls that has been put in place.
- The key stakeholders formally accepted the proposed system design taking into consideration of the updated Threat and Risk Assessment Report.

6.3.2.1 Key Milestone

An updated TRA, including updated risk, assessments and recommendations must be approved by the steering committee before the system can proceed for implementation.

6.4 Phase: IMPLEMENTATION / ASSESSMENT

The Implementation / Assessment phase begins after the architecture design of the system has been approved. As the system is being implemented, security source code reviews and application testing should be conducted to ensure that security has been properly built from a bottom-up. A final round of security source code review and application testing shall be part of acceptance testing, the system should be tested against a set of security test cases.

Prior to the deployment of the system, penetration testing shall be performed on the system to check for and address any vulnerabilities that are not identified or addressed adequately during the previous phases.

Security Process	Activities
Application Security Testing	Perform Source Code Review
	Perform Application Security Testing
System Security Acceptance Testing	Perform System Security Testing
Penetration Testing	Perform Penetration Testing

6.4.1 Security Process: Application Security Testing

The process of Application Security Testing is to ensure that, through a bottom-up approach, vulnerabilities are surfaced and addressed. Bottom-up approach allows problems to be detected early during the development of the system components, which would be costlier to fix during systems integration testing.

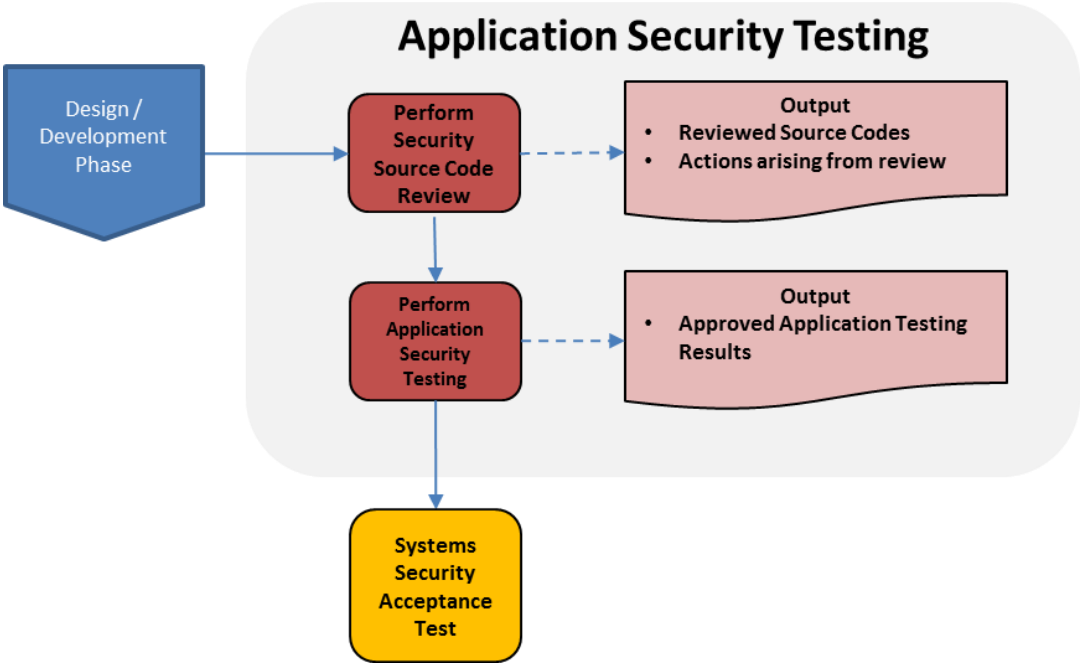

Figure 11: Application Security Testing

6.4.1.1 Activity: Perform Security Source Code Review

Description:	Source code review is a systematic examination of the source code of an application with the intent of finding security issues due to insecure coding practices or malicious intent or coding errors. A secure code review should examine the codes for the following: • Common application vulnerabilities[4] (e.g. input validation, authentication and access control) • Weak implementation of security functions (e.g. encryption, access control) • Backdoors, logic bombs, and malware • Undocumented/unnecessary functions • Known language-specific vulnerabilities • Application logic vulnerabilities For outsourced or turnkey projects, the secure coding standards should be incorporated into the requirement specifications for vendors' compliance. Adherence to secure coding standards should also be one of the user acceptance criteria. Organisations should take utmost diligence to obtain the rights to review

[4] OWASP Top 10 Application Vulnerabilities - https://www.owasp.org/index.php/Top_10_2013-Top_10

	vendor's application source code for projects which they do not own the source codes. After every source code review, a mitigation plan has to be put in place to address all vulnerabilities found. Follow-up review has to be conducted to validate the effectiveness of the mitigation actions and needs to be approved or risk accepted prior to performing application testing.
Roles and Responsibilities:	Project Manager The Project Manager is responsible to prepare the source code review report, the mitigation plan and follow-up review report. Developer The Developer provides inputs to the Security Officer / Consultant for the source code review. Security Officer / Consultant The Security Officer / Consultant is responsible for the source code review report with inputs from the Developer and System Administrator. System Administrator The System Administrator provides inputs to the Security Officer / Consultant for the source code review. Users N.A.
Expected Outputs:	• Source Code Review Report on vulnerabilities and recommendations • Mitigation action plan • Follow-up review report
Inter-dependencies:	Source Code Review should be performed on each system module prior to application testing. This ensures that common vulnerabilities are addressed at the source code level which otherwise would be costlier to fix later during the Operations / Maintenance Phase of the SDLC. Systems should not proceed to application testing prior to fixing major source code defects.

6.4.1.2 Activity: Perform Application Testing

Description:	Application testing must be performed on systems to determine if modules are fit for use. The goal of unit testing is to isolate each part of the system and show that the individual parts are correct. Proper Application testing ensures that: • Problems can be detected early in the development lifecycle especially prior to an acceptance test. • Simplifies integration by testing the parts of a system first and then testing the sum of its parts. After every test, a mitigation plan has to be put in place to address all vulnerabilities found. Follow-up regression test has to be conducted to validate the effectiveness of the mitigation actions and needs to be approved or risk accepted prior to performing systems acceptance testing.
Roles and Responsibilities:	Project Manager The Project Manager is responsible to ensure that Application Testing is performed adequately and approved, mitigation plan is put in place to address all vulnerabilities and all follow up test is conducted. Developer The Developer is responsible to perform application testing of the system. Security Officer / Consultant The Security Officer / Consultant is responsible to perform mitigation action plans on the application testing results to address all vulnerabilities and follow up on all follow up tests. System Administrator N.A. Users N.A.
Expected Outputs:	• Approved Application Testing Results • Mitigation action plan • Follow-up regression test report

Inter-dependencies:	All major application defects that are detected should be remediated through the application change management process. Systems should not proceed to acceptance testing prior to fixing major defects.

6.4.2 Security Process: Systems Security Acceptance Testing

Systems Acceptance Testing is to verify that the complete system satisfies the specified requirements and is acceptable to end users. Systems Security Acceptance Testing is a subset of Systems Acceptance Testing where the focus is on satisfying security requirements.

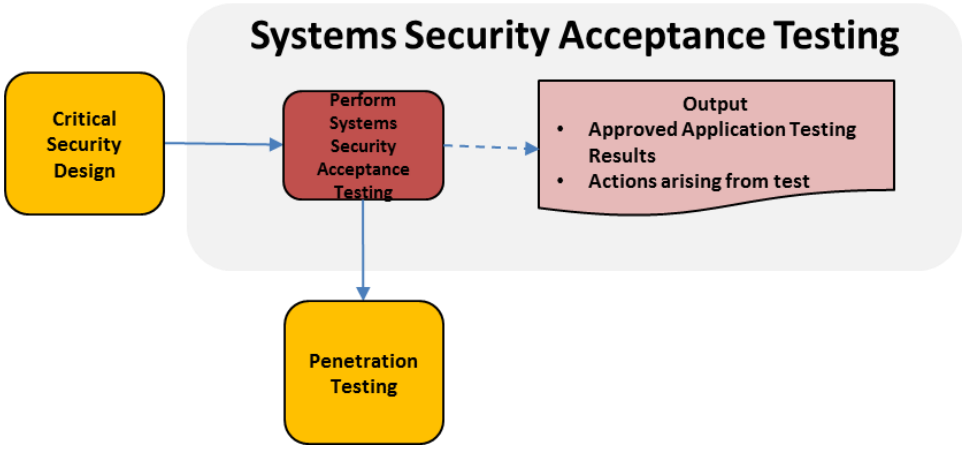

Figure 12: Systems Security Acceptance Testing

6.4.2.1 Activity: Perform Systems Security Acceptance Testing

Description:	This activity focuses on the acceptance testing of the security requirements and controls that has been approved as part of the systems design and is acceptable to be deployed. Activities include: • Checking of system configuration against security specifications and baseline standards (if any) • Test Case Review (focusing on testing the security controls) • Validation of the Acceptance Test • Assessment and Recommendations Systems Security Acceptance Testing should be performed by independent third party assessors and thoroughly performed in a test environment that are identical to the production environment.

	All test results must be accepted or mitigated by the Steering Committee prior to the completion of the Systems Security Acceptance Testing.
Roles and Responsibilities:	Project Manager The Project Manager is responsible to ensure that Systems Security Testing is performed adequately by the independent Security Officer / Consultant, mitigation plan is put in place to address all vulnerabilities, and all follow up test is conducted. Developer N.A. Security Officer / Consultant The Security Officer / Consultant, who should be an independent third party assessor, should perform the Systems Security Acceptance Testing. System Administrator N.A. Users N.A.
Expected Outputs:	• Approved Systems Acceptance Test (with Security Requirements and Controls in place)
Inter-dependencies:	Systems Security Acceptance Testing is performed together with overall Systems Acceptance Testing.

6.4.3 Security Process: Penetration Testing

The objective of the Penetration Testing is to evaluate the security of the accepted system and validate the efficacy of the implemented security controls and policies.

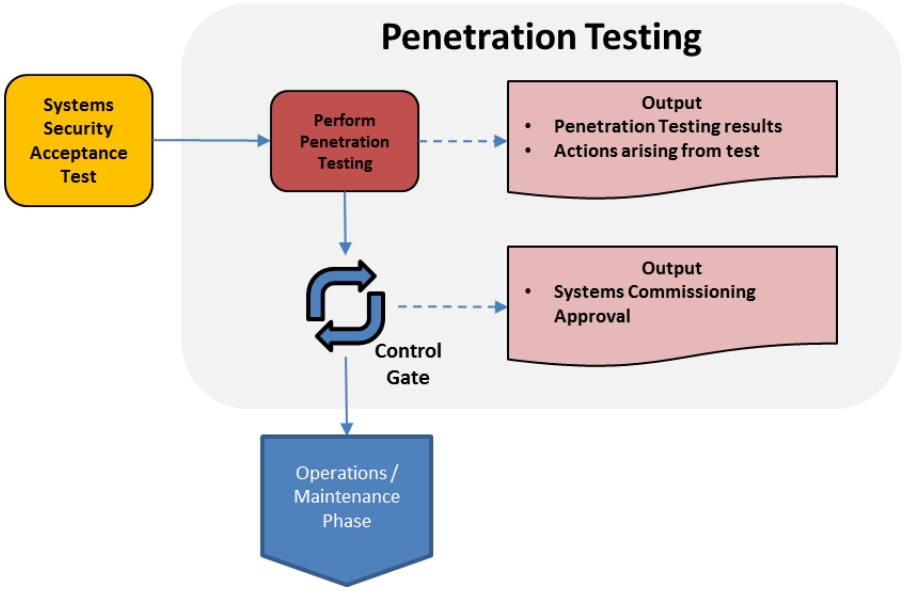

Figure 13: Penetration Testing

6.4.3.1 Activity: Perform Penetration Testing

Description:	Penetration Testing, also called pen testing, is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit. These vulnerabilities may exist in operating systems, service and application flaws, improper configurations, or risky end-user behaviour. Pen tests can either be performed manually or with the assistance of automated software tools. The pen test also includes gathering information about the target to identify entry points for penetration. The pen test should include a follow-up regression testing to validate that the mitigating actions are implemented effectively. All test results must be accepted or mitigated by the Steering Committee prior to the completion of this activity. The main objective of performing penetration testing is to determine security weaknesses from an organisation policy posture, to its systems, the employee's security awareness and the organisation's ability to identify and respond to security incidents. Penetration testing should be performed by independent third party assessors.
Roles and Responsibilities:	Project Manager

	The Project Manager is responsible to ensure that Penetration Testing is performed adequately by the independent Security Officer / Consultant, mitigation plan is put in place to address all vulnerabilities and all follow up test is conducted. <u>Developer</u> N.A. <u>Security Officer / Consultant</u> The Security Officer / Consultant, who should be an independent third party assessor, should perform the Penetration Testing to find vulnerabilities that an attacker could exploit. The Security Officer / Consultant is responsible to prepare the results and recommendations and perform follow up test. <u>System Administrator</u> N.A. <u>Users</u> N.A.
Expected Outputs:	• Penetration Testing results and recommendations • Mitigation action plan • Regression testing report to validate the effectiveness of the mitigation actions
Inter-dependencies:	The activities performed here should be taken with consideration to the Systems Security Acceptance Testing Process so as to ensure that security controls tested under the Systems Security Acceptance Testing Process is effective.

6.4.4 Control Gates

In the implementation phase, the system is built and tested. The key stakeholders rely on the outcome of security tests to assess whether the security controls put in place are effective. The approving authority for this control gate is the Steering Committee.

Recommended control validations for this phase include:

- Security controls defined by the agreed upon requirements are implemented in the system correctly.

- Mitigation actions arising from source code review reports, security test reports and penetration test reports are addressed, risk accepted and formally approved by the Steering Committee.

- Users are adequately trained in the security components of the systems.

6.4.4.1 Key Milestone

Both System Security Acceptance Testing and Penetration Testing must be performed. Results from both tests including mitigation actions should be reported to the Steering Committee and approved prior to the commissioning of the system. All project documentation (outputs from current and previous SBD phases) must be handed over and accepted by the operations team (e.g. Systems Administrator) prior to entering the Operations/Maintenance phase.

6.5 Phase: OPERATIONS / MAINTENANCE

Operations and Maintenance is the phase where systems are in place and operating. Enhancements and/or modifications to the system, from a software and hardware perspective, are developed and tested in this phase.

Security Process	Activities
Audit & Continuous Monitoring	Perform Security Review
	Perform Change Management
	Perform Configuration Management
	Perform Continuous Monitoring

6.5.1 Security Process: Audit and Continuous Monitoring

The purpose of the Audit and Continuous Monitoring process is to ensure that the operational system is periodically assessed to check the effectiveness of the security controls against current threats. Key activities of this phase include:

- Performing regular general and technical security controls reviews to determine if the security controls in place continue to be effective over time.

- Performing proper change management to prevent unintended consequences to the security baseline and to reduce the security risks posed by changes to the systems.

- Performing proper configuration management to ensure that security baseline of the system remains effective.

- Performing continuous monitoring such as vulnerability assessment to determine the current state of the system security.

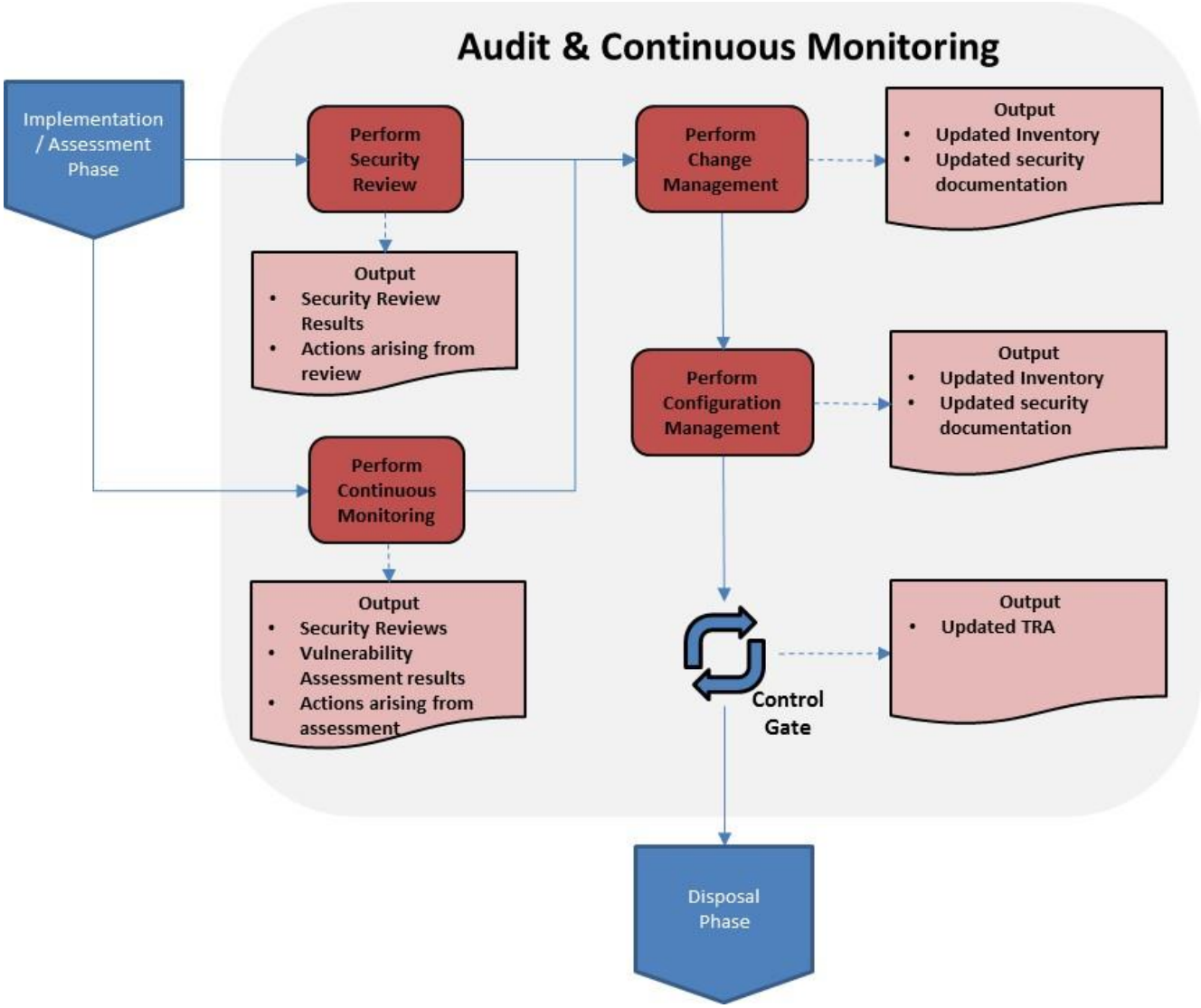

Figure 14: Audit & Continuous Monitoring

6.5.1.1 Activity: <u>Perform Security Review</u>

Description:	Security Review is an essential function to determine if the security controls in place continue to be effective over time, in light of system and environmental changes. In addition to assessing technology assets and technical security controls, security policies addressing issue such as acceptable use, network rights should be reviewed to determine if administrative security controls are effective.

	Security Review must be performed after all system and application changes to ensure that security controls continue to be effective. Security Review should be performed by independent third party assessors.
Roles and Responsibilities:	<u>Project Manager</u> N.A. <u>Developer</u> N.A. <u>Security Officer / Consultant</u> The Security Officer / Consultant, who should be an independent third party assessor, should perform the Security Review at appropriate intervals to ensure that security controls in place continue to be effective over time, in light of system and environmental changes. <u>System Administrator</u> The Systems Administrator is responsible to provide inputs (e.g. configuration settings, documentation, operating procedures, etc.) to the Security Officer / Consultant during the Security Review. <u>Users</u> N.A.
Expected Outputs:	• Documented results of the security review • Security decisions arising from the security review findings • Mitigation plan
Inter-dependencies:	Security review results should be used to improve and ensure that security controls are effective.

6.5.1.2 Activity: <u>Perform Change Management</u>

Description:	Change Management is critical to identifying significant changes and impact that alter a system's security posture. Inadequate control of changes to systems is a common cause of system or security failures. Changes to the operational

	environment, including changes from the development to production phases, can impact on the security posture of the system.
Roles and Responsibilities:	Project Manager N.A. Developer The Developer is responsible to initiate the change management and consult the Security Officer / Consultant on potential impact to the security of the system. Security Officer / Consultant The Security Officer / Consultant should be consulted on any changes that can have significant security impact. The Security Officer / Consultant is responsible to perform assessment of potential impact on the security of the system (with inputs from the Developer and System Administrator) arising from the system/application change. The Security Officer / Consultant is responsible to update the TRA report arising from changes to the systems. System Administrator The System Administrator is responsible to execute the system/application changes to the production environment upon approval of the change. Users N.A.
Expected Outputs:	• Change Control decisions • Updated security documentation • Updated TRA report
Inter-dependencies:	The security architecture and documentation should be referenced when performing change management as they provide a benchmark to evaluate the impact of the planned change.

6.5.1.3 Activity: Perform Configuration Management

Description:	Configuration Management is critical to establishing an initial baseline of the system and subsequently for controlling and maintaining an accurate inventory of any changes to the system. Changes to the system configuration can have significant security impact, therefore configuration management must include assessment of potential impact on the security of the system.
Role and Responsibilities:	Project Manager N.A. Developer The Developer is responsible to initiate the configuration management and consult the Security Officer / Consultant on potential impact to the security of the system. Security Officer / Consultant The Security Officer / Consultant should be consulted on any changes that can have significant security impact. The Security Officer / Consultant is responsible to perform assessment of potential impact on the security of the system (with inputs from the Developer and System Administrator) arising from the configuration change. The Security Officer / Consultant is responsible to update the TRA report arising from changes to the systems. System Administrator The System Administrator is responsible to execute the configuration changes upon approval of the configuration change. Users N.A.
Expected Outputs:	• Change Control decisions • Updated security documentation • Updated TRA report
Inter-dependencies:	The security architecture and documentation should be referenced when performing configuration management as they provide a benchmark to evaluate the impact of the planned change.

6.5.1.4 Activity: Perform Continuous Monitoring

Description:	The objective of continuous monitoring is to determine if the security controls in place continue to be effective over time, in light of system and environmental changes. It can include security reviews, self-assessments, vulnerability assessments and patch and end-point management. Continuous Monitoring may also be in a form of automated software that uses the baseline security controls as comparison to generate results. Automation should be leveraged where possible to reduce level of effort and ensure repeatability. For example, vulnerability assessment is necessary due to the discovery of new vulnerabilities every day. A vulnerability assessment report can be used to take appropriate risk mitigation actions and make risk-based decisions regarding the continued operations of the system and the explicit acceptance of risk that results from that decision.
Roles and Responsibilities:	Project Manager N.A. Developer N.A. Security Officer / Consultant The Security Officer / Consultant is responsible to review security results arising from continuous monitoring and provides inputs to mitigate threats and risks. The Security Officer / Consultant is responsible to perform vulnerability assessment to take appropriate risk mitigation actions make risk-based decisions regarding the continued operations of the system and the explicit acceptance of risk that results from that decision. System Administrator The System Administrator is responsible to conduct continuous monitoring such as vulnerability scanning and perform security review/ self- assessments. Users N.A.

Expected Outputs:	• Documented results of continuous monitoring such as vulnerability assessment reports • Security review / self-assessments reports • Security decisions arising from continuous monitoring
Inter-dependencies:	Continuous monitoring results and decisions provides System Owners the tools to continually prioritise security risk and update/implement the necessary security controls needed to keep systems secured.

6.5.2 Control Gates

In this phase, while using the system, we are reassessing its status based on user feedback, technology changes, policy changes, new threats and vulnerabilities and other business-related issues. The approving authority for this control gate is the System Owners.

Recommended control validations for this phase include:

- Validation of security reviews to ensure that built-in controls remain effective and reporting the results to the steering committee.
- Validation of security assessment and reviews reports to ensure that systems and environmental changes are addressed.
- Regular review of TRA reports and risk register to ensure that risks remain valid and are continually addressed.

6.6 Phase: DISPOSAL

This final phase is the disposal of a system and close out current contracts. Information and system disposal will be addressed explicitly in this phase. The process and activities in this phase ensure the orderly termination of the system, while preserving the vital information about the system so that the relevant information may be reactivated, migrated or archived in accordance with regulations and policies.

Security Process	Activities
Secure Disposal	Preserve Information
	Sanitise Media
	Dispose Hardware & Software

6.6.1 Security Process: Secure Disposal

The process addresses the proper disposal of the information, hardware, and software in a manner that prevents any possibility of unauthorised leakage of sensitive data. This also includes the proper preservation and archival of data processed by the system in accordance with the organisation's security requirements.

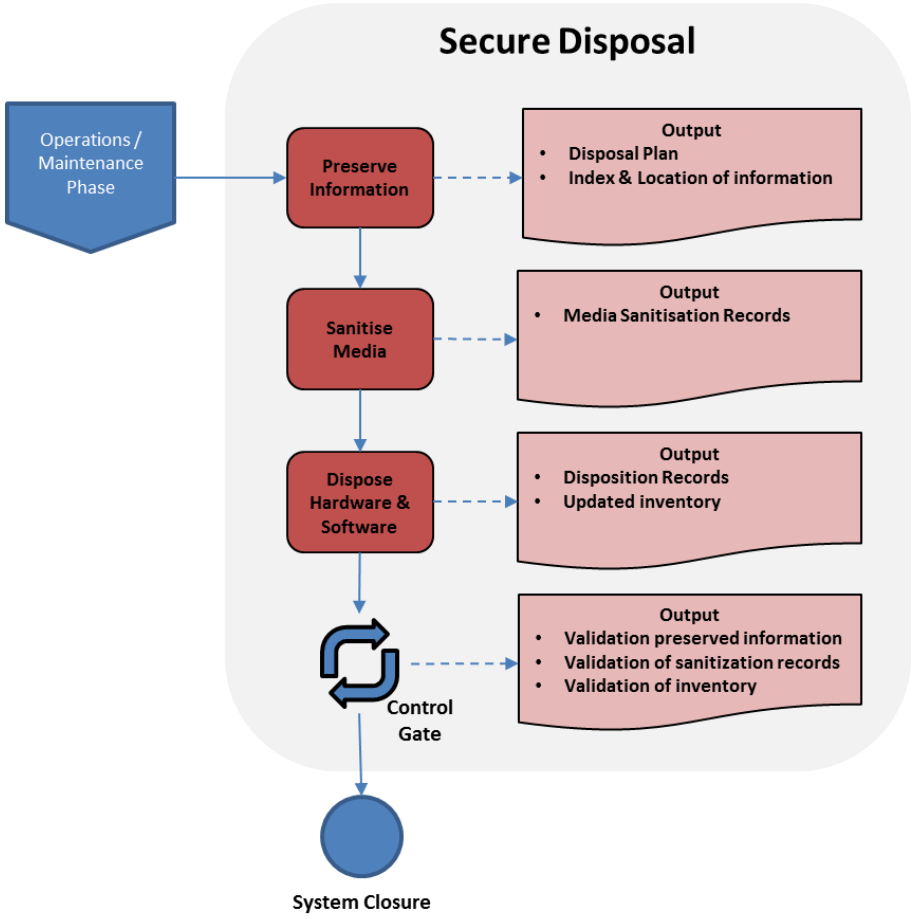

Figure 14: Secure Disposal

6.6.1.1 Activity: Preserve Information

Description:	Organisation should select the archival method that would facilitate information retrieval in the future. This should take into consideration that the following: • Obsolescence or unavailability of the archival technology in the future • Legal and regulatory obligations for minimum records retention periods The archived information should also be marked and handled in compliance with its security classification.
Roles and Responsibilities:	Project Manager

	N.A. Developer N.A. Security Officer / Consultant The Security Officer / Consultant is consulted on the appropriate controls required to be in compliance with information security classification. System Administrator The System Administrator is responsible create the Disposal Plan, which includes the selection of the archival method to archive important and classified information. The System Administrator is also responsible to ensure that archived information is marked and handled according to its information classification. Users N.A.
Expected Outputs:	• Disposal Plan • Index of preserved information and its location.
Inter-dependencies:	Security classification of the information and the respective legal and regulatory obligations for the retention of the information

6.6.1.2 Activity: Sanitise Media

Description:	Based on the security classification of the system and its information, the System Owners shall sanitise the system's digital media using approved equipment, techniques and procedures according to relevant policies and regulations. Systems owner should categorise the information, assess the nature of the medium on which it is recorded, assess the risk to confidentiality, and determined the appropriate sanitisation process. NIST SP 800-88 r1, Guidelines for Media Sanitisation provides details on media sanitisation best practices.
Roles and Responsibilities:	Project Manager N.A. Developer

	N.A. Security Officer / Consultant The Security Officer / Consultant is consulted on the appropriate sanitisation process, accorded to the security classification of the system. System Administrator The System Administrator, with the approval from System Owners, is responsible to sanitise the system's digital media that is to be disposed. The System Administrator is responsible to keep appropriate Media sanitisation records for future references. Users N.A.
Expected Outputs:	• Media sanitised according to policy and regulatory requirements • Media sanitisation records
Inter-dependencies:	Organisation security classification provides the identification and associated risk level of system information.

6.6.1.3 Activity: Dispose of Hardware and Software

Description:	Depending on relevant policies and regulation, hardware can be sold, discarded or given away. The disposal of software should comply with licence agreements.
Roles and Responsibilities:	Project Manager N.A. Developer N.A. Security Officer / Consultant N.A System Administrator The System Administrator is responsible disposed the hardware according to the disposal plan and updates the disposition

	records and asset inventory accordingly. The System Administrator is responsible to keep disposition records for future references and also update the asset inventory to reflect the disposed assets. <u>Users</u> N.A.
Expected Outputs:	• Disposition records for hardware and software, including redeployment. Records should be retained according to relevant polices and regulation. • Updated inventory of assets to reflect disposed hardware and software.
Inter-dependencies:	Hardware and software inventory under the System Owner's charge should be updated accordingly after disposal is completed.

6.6.2 Control Gates

In the disposal phase, the key concern is that the system is terminated in an orderly manner, and that vital information about the system is preserved according to applicable records management regulations and policies for future access. All media is accorded the correct sanitisation method and finally the hardware and software are disposed according to policy. The approving authority of this gate is the System Owners.

Recommended control validations for this phase include:

- Validating information of the system has been correctly preserved and accorded with the right security classification.
- Validating that media sanitisation records has been properly recorded and filed.
- Validating the disposition records against actual hardware/software inventory.

References

1. *National Institute of Standards and Technology. (2008). Special Publication 800-64 Revision 2 - Security Considerations in the System Development Life Cycle.*

2. *National Institute of Standards and Technology. (2010). Special Publication 800-37 Revision 1 - Guide for Applying the Risk Management Framework to Federal Information Systems.*

3. *National Institute of Standards and Technology. (2014). Special Publication 800-88 Revision 1 - Guide for Media Sanitisation.*

4. *Scott W. Ambler. (2012). The Agile System Development Life Cycle. Retrieved from http://www.ambysoft.com/essays/agileLifecycle.html*

ANNEX A – Diagrams and Mappings of SDLC Methodologies

Figure A-1 shows the phases of a IT Project Lifecycle which government agencies adopt under IM8[5].

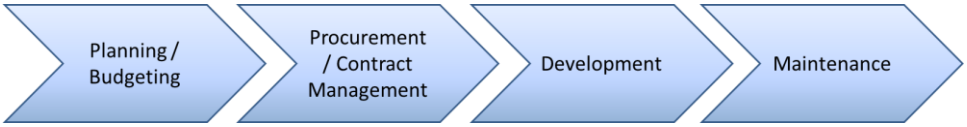

Figure A-1: IT Project Lifecycle (IM8)

Figure A-2 shows the phases under the Defence Capability Management (DCM) Framework, adopted by MINDEF, by which the need for a new defence capability is transformed into operational and support system requirements.

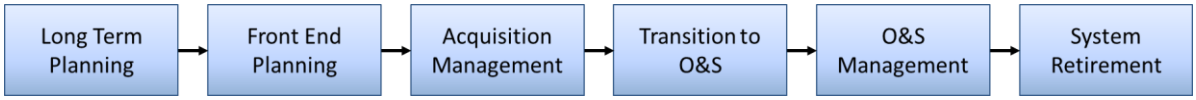

Figure A-2: DCM Framework

Figure A-3 illustrates examples of how various methodologies are aligned against SBD Phases.

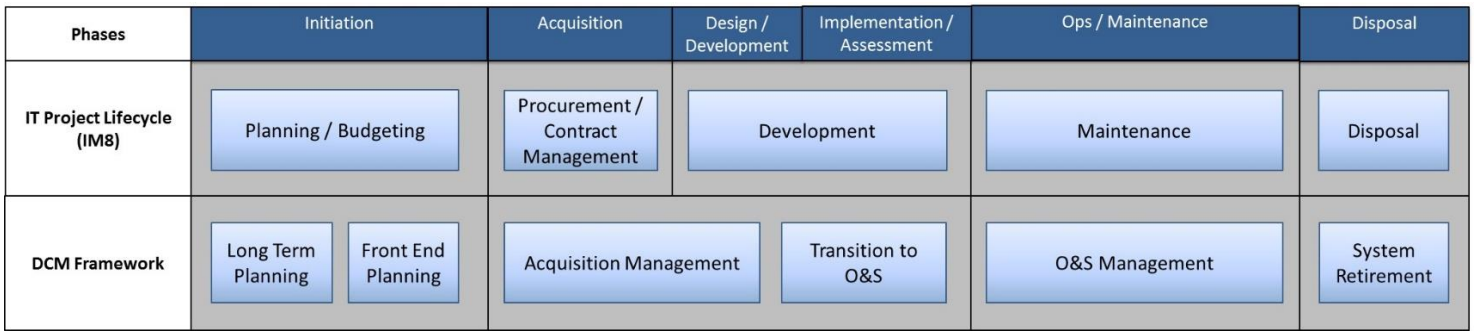

Figure A-3: Mapping of development lifecycles[6]

[5] Government Instruction Manual 8 – IT Management
[6] O&S refers to Operations and Support

Figure A-4 illustrates how Agile Development Lifecycle can adopt the Security-by-Design through its mapping against SBD security processes. The SBD processes shown are identical to the processes described under the SBD Framework.

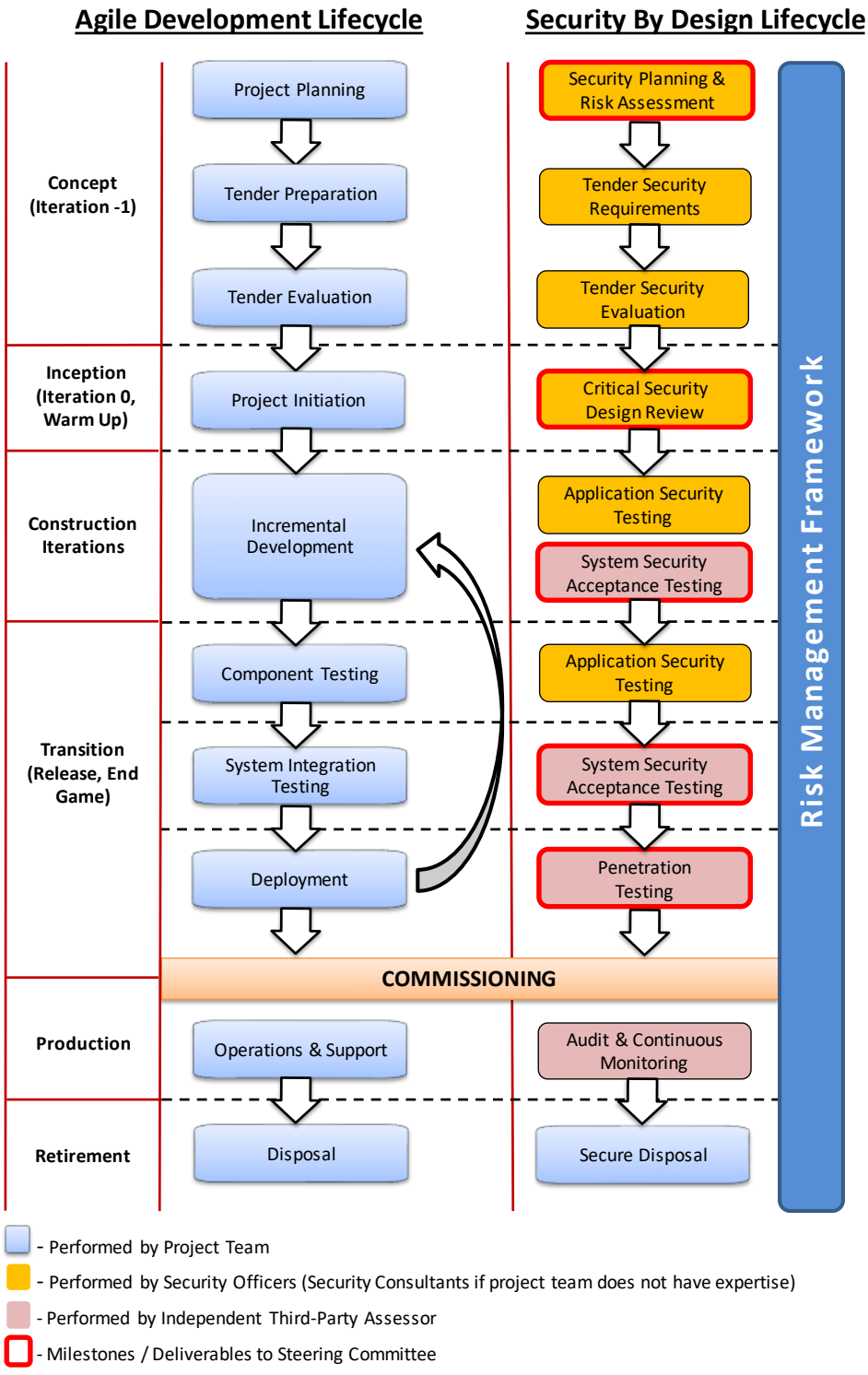

Figure A-4: Agile development lifecycle mapping against SBD Framework

ANNEX B – Roles and Responsibilities

Roles	Responsibilities
Steering Committee	The Steering Committee provides project leadership to ensure the successful delivery of the project and is accountable for approval of key security deliverables and milestones.
System Owner	The System Owner is responsible for the system and its operations and maintenance.
Project Manager	The Project Manager has the authority to run the project on a day-to-day basis and is responsible to ensure that all project activities are delivered within the agreed constraints of cost, time, risk, resource, quality and scope.
Developer	The Developer is responsible to develop the system and is often consulted on the technical feasibility of a system requirement. This role may be performed by the vendor if the project is outsourced.
Security Officer / Consultant	The Security Officer / Consultant is the subject matter expert on all security tasks. This role may be performed in-house or externally if the project team does not have the necessary security expertise. Security Consultant, in the context of this framework, refers to external resources such as vendors or external agencies.
System Administrator	The System Administrator is responsible for the day to day operations of the commissioned system.
User	The Systems User represents the users who will interact with the system, typically through an interface, to extract some functional benefit.

Table B-1 Roles and Responsibilities

ANNEX C – Glossary

TERM	DEFINITION
Critical Information Infrastructure (CII)	Infocomm or operational technology system or network infrastructure that is vital to the continuous delivery of Essential Services which Singapore relies on; services which, the loss or compromise, would (a) lead to debilitating impact on security, economy or public health and safety; or (b) threaten Singapore's survival during National Emergency.
Operational Technology (OT)	A category of hardware and software that monitors and controls how physical devices perform. OT is primarily used in industrial control systems for manufacturing, transportation and utilities; technology that control operations. (See also industrial control systems)