Office of the Government Chief Information Officer

INFORMATION SECURITY

Practice Guide

for

Security Risk Assessment & Audit

[ISPG-SM01]

Version 2.0

April 2024

© The Government of the Hong Kong Special Administrative Region
of the People's Republic of China

The contents of this document remain the property of and may not be reproduced in whole or in part without the express permission of the Government of the Hong Kong Special Administrative Region of the People's Republic of China.

COPYRIGHT NOTICE

© 2024 by the Government of the Hong Kong Special Administrative Region of the People's Republic of China

Unless otherwise indicated, the copyright in the works contained in this publication is owned by the Government of the Hong Kong Special Administrative Region of the People's Republic of China. You may generally copy and distribute these materials in any format or medium provided the following conditions are met –

(a) the particular item has not been specifically indicated to be excluded and is therefore not to be copied or distributed;
(b) the copying is not done for the purpose of creating copies for sale;
(c) the materials must be reproduced accurately and must not be used in a misleading context; and
(d) the copies shall be accompanied by the words "copied/distributed with the permission of the Government of the Hong Kong Special Administrative Region of the People's Republic of China. All rights reserved."

If you wish to make copies for purposes other than that permitted above, you should seek permission by contacting the Office of the Government Chief Information Officer.

Amendment History				
Change Number	Revision Description	Pages Affected	Revision Number	Date
1	G51 Security Risk Assessment & Audit Guidelines version 5.0 was converted to Practice Guide for Security Risk Assessment & Audit. The Revision Report is available at the government intranet portal ITG InfoStation: (http://itginfo.ccgo.hksarg/content/itsecure/review2016/amendments.shtml)	Whole document	1.0	December 2016
2	Added a new chapter on information security management, revised description on security risk assessment and security audit, and aligned references with other practice guides.	Whole document	1.1	November 2017
3	To incorporate updates in accordance with the changes in the latest version of Baseline IT Security Policy [S17] version 7.0 and IT Security Guidelines [G3] version 9.0	Whole document	1.2	June 2021
4	To incorporate updates in accordance with the changes in the latest version of Baseline IT Security Policy [S17] version 8.0 and IT Security Guidelines [G3] version 10.0	Whole document	2.0	April 2024

Table of Contents

1. Introduction

Information Technology (IT) security risk assessment and security audit are the major components of information security management. This document provides a reference model to facilitate the alignment on the coverage, methodology and deliverables of the services to be provided by independent security consultants or auditors. With this model, managerial users, IT managers, system administrators and other technical and operational staff can have more understanding about security risk assessment and audit. They should be able to understand what preparations are required, which areas should be noted, and what results would be obtained. It is not the intention of this document to focus on how to conduct a security risk assessment or audit.

1.1 Purpose

This document shows a general framework for IT security risk assessment and security audit. 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 staff who are involved in a security risk assessment or security audit as well as for the security consultants or auditors who perform the security risk assessment or security audit for 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 the Hong Kong Special Administrative Region
- IT Security Guidelines [G3] , the Government of the Hong Kong Special Administrative Region
- Information technology - Security techniques - Information security management systems - Overview and vocabulary (fifth edition), ISO/IEC 27000:2016
- ISO/IEC 27001:2022 Information Technology - Security Techniques - Information Security Management Systems - Requirements (third edition)
- ISO/IEC 27002:2022 Information Technology - Security Techniques - Code of Practice for Information Security Controls (third edition).
- ISO/IEC 27005:2022 Information Technology - Security Techniques - Information Security Risk Management (fourth edition)
- ISO 31000:2018 Risk Management – Guidelines
- NISTIR 8286 Integrating Cybersecurity and Enterprise Risk Management (ERM)

1.3 Definitions and Conventions

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

Abbreviation and Terms	
Security Risk Assessment	It is a process of identifying, analysing and evaluating the security risks, and determining the risk treatment measures to reduce the risks to an acceptable level.
Security Audit	It is an audit on the level of compliance with the security policy or standards as a basis to determine the overall state of the existing protection and to verify whether the existing protection meansures have been performed properly.

1.4 Contact

This document is produced and maintained by the Office of the Government Chief Information Officer (OGCIO). For comments or suggestions, please send to:

Email: it_security@ogcio.gov.hk

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

CMMP mail: IT Security Team/OGCIO

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 audit 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 risk of data security, B/Ds shall activate their standing incident management plan to identifying, managing, recording, and analysing security threats, attacks, or incidents in real-time. B/Ds should also prepare to communicate appropriately with relevant parties by sharing information on response for 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 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 the cyber risk information sharing platform to receive and share information regarding security issues, vulnerabilities, and cyber threat intelligence.

3. Introduction to Security Risk Assessment and Audit

3.1 Security Risk Assessment and Audit

Security risk assessment and audit is an ongoing process of information security practices to discovering and correcting security issues. They involve a series of activities as shown in Figure 3.1. They can be described as a cycle of iterative processes that require ongoing monitoring and control. Each process consists of different activities and some of which are highlighted below as examples.

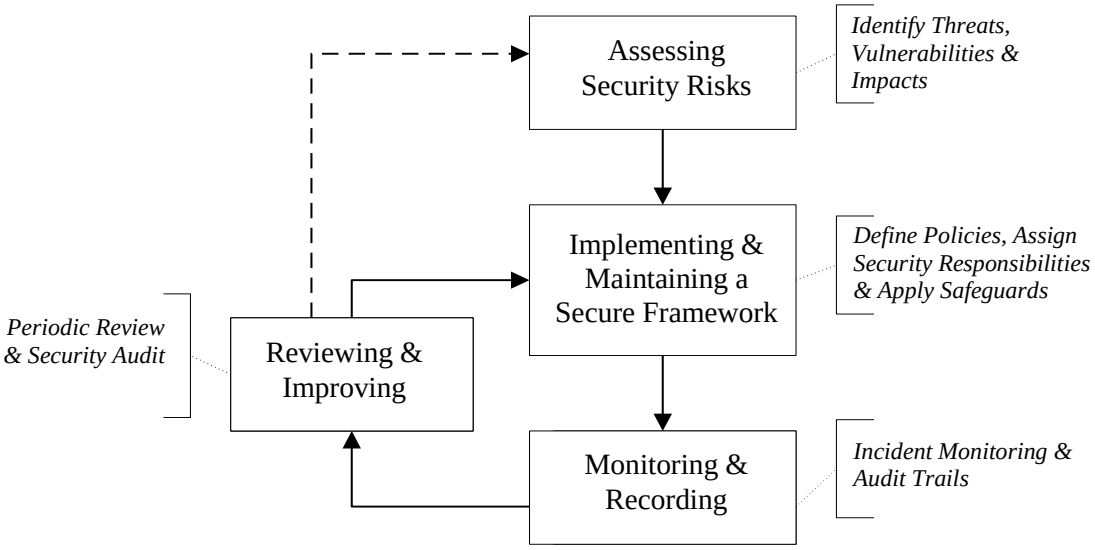

Figure 3.1 An Iterative Process of Security Risk Assessment and Audit

Assessing security risk is the initial step to evaluate and identify risks and consequences associated with vulnerabilities, and to provide a basis for management to establish a cost-effective security program.

Based on the assessment results, appropriate security protection and safeguards should be implemented to maintain a secure protection framework. This includes developing new security requirements, revising existing security policies and guidelines, assigning security responsibilities and implementing technical security protections.

With implementation of a secure protection framework, there is also the need for constant monitoring and recording so that proper arrangements can be made for tackling a security incident. In addition, day-to-day operations such as users' access attempts and activities while using a resource, or information, need to be properly monitored, audited, and logged.

This step is then followed by cyclic compliance reviews and re-assessments to provide assurance that security controls are properly put into place to meet users' security requirements, and to cope with the rapid technological and environmental changes. This model relies on continuous feedback and monitoring. The review can be done by conducting periodic security audits to identify what enhancements are necessary.

3.2 Security Risk Assessment vs Security Audit

Both the security risk assessment and the security audit are on-going processes but are different in terms of both nature and functions.

Security risk assessment is the process to identify, analyse and evaluate the security risks, and determine the mitigation measures to reduce the risks to an acceptable level. The risk assessment is an integral part of a risk management process designed to provide appropriate levels of security for information systems. It helps 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.

For a new information system, the security risk assessment is typically conducted at the beginning of the system development life cycle. For an existing system, the assessments shall be conducted on a regular basis throughout the system development life cycle or when major changes are made to the IT environment.

An information security audit is an audit on the level of compliance with the security policy and standards as a basis to determine the overall state of the existing protection and to verify whether the existing protection measures have been performed properly. The security audit is an on-going process to ensure that current security measures comply with departmental IT security policies, standards, and other contractual or legal requirements.

While there are similarities in certain functions, below is a highlight of the key differences between security risk assessment and security audit.

Security Risk Assessment	**Security Audit**
The identification of threat and vulnerabilities, evaluation of the levels of risk involved, and determination of an acceptable level of risk and corresponding risk mitigation strategies	The processes to ascertain the effective implementation of security measures against the departmental IT security policies, standards, and other contractual or legal requirements
Focus on the risk perspective, assessment areas not necessarily related to security policies and standards	Focus on the compliance perspective, assess against security policies, standards or other pre-defined criteria
It can be a self-assessment by B/D or completed by an independent third party	Must be completed by an independent third party
Key deliverables: risk register and risk treatment measures	Key deliverable: compliance checklist

Table 3.1 Security Risk Assessment VS Security Audit

The details of the security risk assessment and security audit processes are described in Sections 4 and 5 respectively.

4. Security Risk Assessment

Security risk assessment is the process of identifying, analysing and evaluating the security risks, and determining the risk treatment measures to reduce the risks to an acceptable level. The assessment process of a system includes 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 shall be made available as inputs to the identification and analysis activities. Interviews with relevant parties such as administrators, computer / network operators, or users can also provide additional information for the analysis. The analysis may also involve the use of automated security assessment tools depending on the assessment scope, requirements and methodology. After evaluation of all collected information, a list of observed risk findings will be reported. For each of the observed risks, appropriate security measures will be determined, implemented and deployed.

Due to the high demand of expert knowledge and experience in analysing the collected information and justifying security measures, a security risk assessment should be performed by qualified security expert(s).

4.1 Benefits of Security Risk Assessment

- To provide a complete and systematic view to management on existing IT security risks and the necessary security safeguards.
- To provide a reasonably objective approach for IT security expenditure budgeting and cost estimation.
- To enable a strategic approach to information security management by providing alternative solutions for decision making and consideration.
- To provide a basis for future comparisons of changes made in IT security measures.

4.2 Types of Security Risk Assessment

Depending on the purpose and the scope of the assessment, security risk assessment can be categorised into different types. The exact timing depends on your system requirements and resources.

- Departmental Level Assessment: This type of assessment focuses on evaluating the security posture of individual B/D. It entails a strategic and systematic approach to analyse the overarching infrastructure or design of the B/D's systems. Departmental Level Assessments are particularly beneficial for B/Ds that manage numerous information systems and require a broad risk analysis rather than an in-depth technical control review. This assessment is suitable for:
    - Gauging the current security measures in place within a B/D.
    - Providing a high-level overview of potential risks to the B/D's information systems.

  The goal is to identify and mitigate risks before they can impact the B/D's operations, providing a proactive measure in maintaining a robust security posture.

- System Level Assessment: This detailed assessment is specifically designed to be conducted on a new information system before it is rolled out or when there is a major functional change to ensure the security integrity of individual information systems within a B/D. The key features of a System Level Assessment include:
    - Risk Identification: This initial step involves pinpointing potential threats and vulnerabilities to the information systems within a B/D. By identifying the sources of risk, the foundation for a comprehensive analysis is established.
    - Risk Analysis: Subsequent to risk identification, this phase conducts a detailed examination to evaluate the potential impact and likelihood of identified risks. This analysis is crucial for understanding the threat landscape and for prioritising the risks based on their potential impact on the information system.
    - Risk Evaluation: In this phase, the analysed risks are compared against the B/D’s risk criteria to determine their significance. This evaluation assists in understanding which risks need to be addressed in line with the B/D's risk appetite and security objectives.
    - Risk Treatment: Following the evaluation, this step involves selecting and applying the appropriate controls to mitigate, transfer, accept, or avoid significant risks. Decisions made in this stage lead to the development of a risk treatment plan that outlines how the B/D will deal with the assessed risks.

- Verification Process: After the implementation of risk treatment measures, a verification process is crucial to ensure that the controls are properly applied and are effectively securing the information systems. This step confirms that the risk treatment results meet the required security standards.

Before diving into a full-scale System Level Assessment, a Preliminary Risk Analysis can be performed.

- Preliminary Risk Analysis: Commonly conducted during the design stage of an information system, the Preliminary Risk Analysis is a proactive measure intended to identify and evaluate threats and vulnerabilities early on. This lightweight yet critical process ensures that necessary security requirements are recognised and seamlessly integrated into the system design. By addressing security at the outset, it helps to avoid costly retrofits or security overhauls later in the system's lifecycle. By embedding security considerations into the early stages of system design, the Preliminary Risk Analysis facilitates a security-by-design approach that can significantly reduce risks and inform the development of a more secure system. Please refer to Practice Guide for Security by Design for more details.

The overarching goal of the System Level Assessment is to provide a comprehensive review of an information system's security within a B/D, integrating security throughout the system's development lifecycle.

4.3 Prerequisite for Security Risk Assessment

4.3.1 Planning

Before a security risk assessment can start, planning is required for proper preparation, monitoring and control. One suggestion is to inform the stakeholders, such as the network team, the application team and the security incident handling team in advance if risk assessment exercises covering penetration testing or vulnerability scanning are to be carried out to avoid excessive false alarms generated that might impact the daily operation. Listed below are several major items that should be defined first.

- Project Scope and Objectives
- Background Information
- Constraints
- Roles & Responsibilities of Stakeholders
- Approach and Methodology
- Project Size and Schedule
- Data and Tools Protection
- External Vendors Selection

4.3.1.1 Project Scope and Objectives

The project scope and objectives can influence the analysis methods and types of deliverables of the security risk assessment. The scope of a security risk assessment may cover the security measures of individual systems, the interactions between these systems, and the overall security posture of the system infrastructure within the B/D. Thus, the corresponding objectives may be to identify the security requirements, such as protecting individual systems, pinpointing potentially risky areas in system interactions, or assessing the overall information security level of a system infrastructure. The security requirements should be based on business needs, typically driven by the senior management, to identify the desired level of security protection in the B/D.

4.3.1.2 Background Information

It refers to any relevant information that can provide initial ideas to the consultant about the assessment. For example, the historical and current information of the system under study, the related parties, brief information about the last assessment, or the near future changes which may affect the assessment.

4.3.1.3 Constraints

Constraints like time, budget, cost, technology and other restrictions should also be considered. B/Ds are advised to submit their funding applications earlier in order to secure funding for their SRAA exercises. This may affect the project schedule and the available resources to support the assessment.

4.3.1.4 Roles and Responsibilities of Stakeholders

Roles and responsibilities of all parties involved should be carefully defined. A team or group of individuals representing a variety of disciplines with assigned responsibilities is recommended to best accomplish the assessment. Depending on the availability and requirements, some or all of the following members may be included:

- System or information owners
- IT security administrators or officers
- Computer operational staff
- System or network administrators
- Application or system developers
- Database administrators
- Users or senior users

- Senior management
- External contractors

4.3.1.5 Approach and Methodology

The assessment approach or methodology analyses the relationships among systems, threats, vulnerabilities and other elements. There are numerous methodologies. Generally, they can be classified into two main types: quantitative and qualitative analysis.

To be more useful, the methodology chosen should be able to produce a quantitative statement about the impact of the risk and the effect of the security problems, together with some qualitative statements describing the impact and appropriate security measures for minimising these risks. Details of the two analysis methods will be explained in subsequent sections.

4.3.1.6 Project Size and Schedule

One of the most important tasks is to prepare a project schedule stating all major activities that will be performed in the assessment study. The planned project size such as project cost and the number of staff involved can directly affect the project schedule. This project schedule can be used for progress control and project monitoring.

4.3.1.7 Data and Tools Protection

Throughout stages of the security risk assessment, a tremendous amount of data and system configurations will be collected where some of them may contain sensitive information.

Therefore, the assessment team should ensure all the collected data are stored securely. File encryption tools and lockable cabinet/room should be arranged at the planning stage to prevent unauthorised access to the sensitive data.

Besides, the assessment tools should also be properly maintained, controlled and monitored to avoid misuse. Such tools should only be run by the subject experts within the assessment team to avoid potential damages to the system. These tools as well as the data generated by them should also be removed immediately after use unless there is proper control to protect them from unauthorised access.

At the end of the assessment process, a security risk assessment report will be compiled to document all the risk findings. Any unauthorised access to such information, especially before rectification, may pose immediate threats to the B/D concerned. Hence, it is crucial that the assessment team enforces proper protection on the interim and final security risk findings and assessment report during and after

the documentation process. Senior management should also be reminded to treat the security risk assessment report in strict confidence. Lastly, the assessment team should also return all requested data or documents to the B/D concerned, and B/D should revoke temporary access rights assigned to the auditors upon completion

4.3.1.8 External Vendors Selection

B/Ds should define clear and comprehensive selection criteria before starting the vendor selection process. This could include the vendor's qualifications, experience, reputation, and pricing.

- Vendor Qualifications: Vendors should be qualified to conduct security risk assessments. This could include certifications from recognised bodies in the field of IT security.
- Vendor Experience: The vendor's experience in conducting security risk assessments should be considered. This should include the number of assessments the vendor has conducted and the types of systems they have assessed.
- Vendor Reputation: The vendor's reputation in the IT security field should be evaluated. This could involve checking references, reviewing client testimonials, and researching the vendor's history.

B/Ds should use a standardised evaluation method, such as a scoring system or decision matrix, to objectively assess each vendor against the selection criteria. This helps to minimise bias and ensure a fair and transparent selection process.

B/Ds should consider the past performance of potential vendors, including their track record of delivering on time, staying within budget, and achieving the desired outcomes. References from previous experience can provide valuable insights into a vendor's reliability and performance.

B/Ds should conduct thorough due diligence on potential vendors. This includes verifying their professional qualifications, checking their financial stability, and ensuring they comply with all relevant regulations and standards.

4.4 Steps in the Security Risk Assessment Exercise

Security Risk Assessment at the system level involves several major activities and deliverables, as shown in Figure 4.1, including Risk Identification, Risk Analysis, Risk Evaluation, Risk Treatment and System Risk Registers.

For departmental level risk management, please refer to Practice Guide for IT Security Risk Management for more detail.

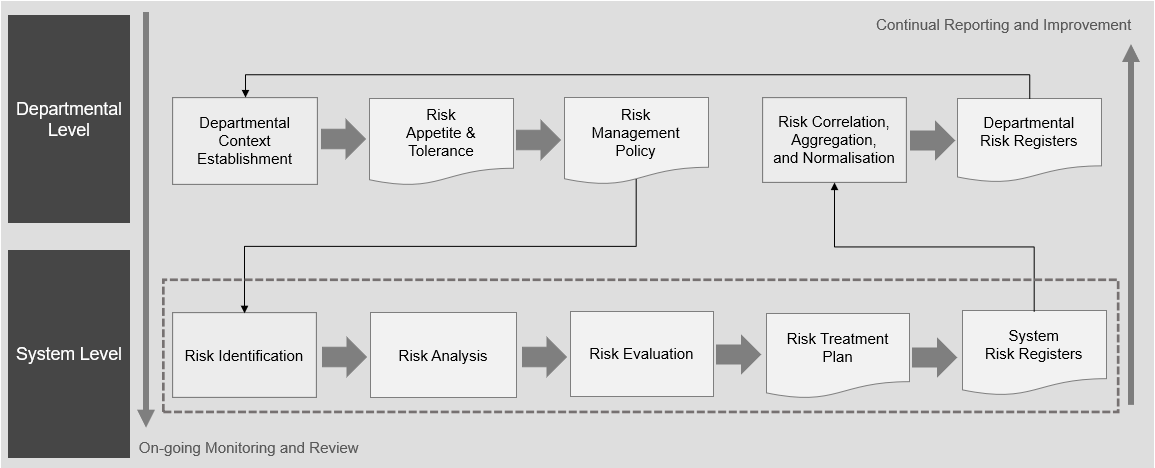

Figure 4.1 General Security Risk Assessment Steps

4.4.1 Risk Identification

Risks represent vulnerabilities exploited by threat in a system that could lead to a significant negative impact on B/D's operations, assets, or reputation. Threats might come from a range of sources, including individuals, groups, or even environmental conditions that could cause unauthorised access, destruction, modification of information, or denial of service. Vulnerabilities, on the other hand, are weaknesses or gaps in a security system that can be exploited by threats.

The impact is potential severity of damage of a threat exploiting a vulnerability alongside with the likelihood which is the probability. It can be tangible and intangible affecting the confidentiality, integrity, and availability of B/D's digital assets.

Figure 4.2 Risk is Defined as a Combination of Threat, Vulnerability and Impact

Risk identification is the process of finding, recognizing and describing risks. This involves the identification of risk sources and events. Risk identification aims to

generate a list of risks based on those events that can prevent, affect or delay the achievement of IT security objectives. Risk identification on every aspect should be performed, which includes, but is not limited to, the following:

- Human resource security.
- Asset management.
- Access control.
- Cryptography.
- Physical and environmental security.
- Operations security.
- Communications security.
- System acquisition, development and maintenance.
- Outsourcing security.
- IT security aspects of business continuity management.

This process can generally be divided into sub-processes. They are:

- Information Systems Identification
- Risk Scenario Identification

Each of these sub-processes is explained briefly in later sub-sections.

4.4.1.1 Information Systems Identification

B/Ds should identify all information systems within their purview, regardless of their funding sources. These systems, serving as supporting assets, encompass all components of the information system upon which business operations and processes are based. Before conducting the risk assessment, a comprehensive inventory of all assets within the B/D's information systems should be available. An accurate information system inventory ensures that all critical components are considered during risk identification and analysis.

B/Ds should also understand the value of each information system to the B/D based on their information system classification. Systems with higher classification typically have a higher value due to their criticality.

The objective is to understand the existing system and environment and identify the risks through analysis of the information / data collected.

Values of assets can be expressed in terms of:

- Tangible values such as replacement costs of IT facilities, hardware, software, system data, media, supplies, documentation, and IT staff supporting the systems.

- Intangible values such as goodwill and improved service quality.
- Information values, e.g. confidentiality, integrity and availability.
- Data classification of the information stored, processed, or transmitted by the asset.

The output of asset identification and valuation process is an inventory checklist of assets with their corresponding values, if any, in terms of their tangible values, intangible values, or information values in terms of confidentiality, integrity and availability. The more specific values the assets are needed, the more time is required to complete this process.

By default, all relevant information should be collected irrespective of storage format. Listed below are several kinds of information that are often collected.

- Security requirements and objectives.
- System or network architecture and infrastructure, such as a network diagram showing how the assets are configured and interconnected.
- Evidence or supporting documents indicating that the physical environment of computer rooms meets the physical security requirements according to the classification of data resided. Examples are certification/notification issued by Architectural Service Department or relevant results from last SRAA reports.
- Information available to the public or found in the web pages.
- Physical assets such as hardware equipment.
- Systems such as operating systems and network management systems.
- Contents such as databases and files.
- Applications and servers information.
- Networking details such as supported protocols and network services offered.
- Access control measures.
- Processes such as business process, computer operation process, network operation process, application operation process, etc.
- Identification and authentication mechanisms.
- Relevant statutory, regulatory and contractual requirements pertaining to minimum security control requirements.
- Policies and guidelines.
- Information system classification.

4.4.1.2 Risk Scenario Identificaiton

(i) Techniques for Identifying Risks

B/D shall use various techniques to identify uncertainties that may affect one or more objectives. The following factors and the relationship between these factors should be considered:

- Tangible and intangible sources of risk;
- Causes and events;
- Threats and opportunities;
- Vulnerabilities and capabilities;
- Changes in the external and internal context;
- Indicators of emerging risks;
- The nature and value of assets and resources;
- Consequences and their impact on objectives;
- Limitations of knowledge and reliability of information;
- Time-related factors;
- Biases, assumptions and beliefs of those involved.

There are two approaches commonly used to perform risk identification.

a) Event-based approach: identify strategic scenarios by considering risk sources and how they use or impact interested parties to reach those risk's desired objectives.

With an event-based approach, the underlying concept is that risks can be identified and assessed by evaluating events and consequences. Events and consequences can often be determined by discovering the concerns of top management, risk owners and the requirements identified in determining the context of the B/D.

For instance, consider a B/D that handles sensitive citizen data. A potential risk could be a data breach event, where unauthorised users gain access to this sensitive information. The source of this risk could be external hackers. The interested parties impacted could include citizens whose data is compromised and the B/D itself due to potential reputation damage and legal consequences.

b) Asset-based approach: identify operational scenarios detailed in terms of assets, threats and vulnerabilities.

With an asset-based approach, the underlying concept is that risks can be identified and assessed by inspecting assets, threats and vulnerabilities. An asset has value to the B/D and, therefore, requires protection. Assets should be identified, considering an information system consists of activities, processes, and information to be protected. A threat exploits a vulnerability of an asset to compromise the confidentially, integrity and/or availability of corresponding information.

Using the same B/D in a) as an example, an asset could be the database containing sensitive citizen data. A threat could be a phishing attack from cybercriminals aiming to gain unauthorised access to the database. The vulnerability could be an

insufficiently secure system or a lack of employee training on identifying phishing attempts. In this case, the confidentially, integrity, and availability of the information in the database could be compromised if the threat exploits the vulnerability. This example highlights the need for robust security measures and employee training to protect valuable assets from identified threats and vulnerabilities.

For each system, B/Ds shall identify and document risk scenarios in the risk assessment form, a critical output of the risk identification process. The risk list should include a detailed description of each risk, including the potential sources, the assets that could be affected, the threats that could exploit vulnerabilities, and the potential impact on the B/D's objectives.

B/Ds should leverage their understanding of the complexity and interdependencies of their individual systems and associated processes and resources in risk identification. B/Ds should consider all relevant risk sources for each system, including human, environment and technical risks.

B/Ds shall regularly update the risk list to account for new and changing risks. This includes tracking and documenting any changes in the B/D's internal and external context that could introduce new risks or modify existing ones for each system.

B/Ds shall assign a risk owner for each identified risk in each system. A risk owner is typically an individual or a role within a B/D with the knowledge, resources, and authority to manage the risk.

(ii) Assets/Threats/Vulnerabilities Mapping

IT security risk identification is an intricate process composed of four necessary inputs. The integration of these elements enables the practitioner to record each scenario as a description of a potential IT security risk.

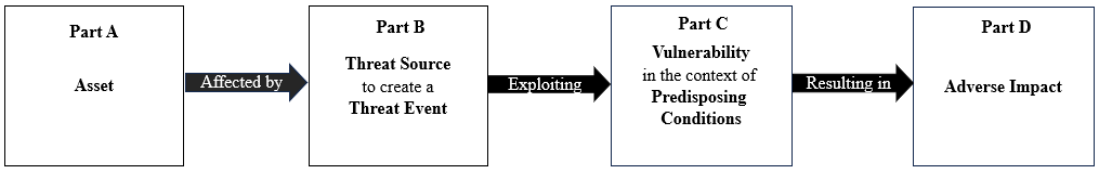

Figure 4.3 Input to Risk Scenario Identification

Part A – Identification of the B/D's relevant assets and their valuation. This is the starting point for understanding what needs to be protected within the B/D.

Part B – Determination of potential threats that might jeopardise the confidentiality, integrity, and availability of those assets. These threats could come from various sources and impact the B/D in diverse ways.

Part C – Consideration of vulnerabilities or other predisposing conditions of assets that make a threat event possible. These vulnerabilities are weaknesses that could be exploited by a threat to cause harm to an asset.

Part D – High-level evaluation of the potential consequences if the threat source (part B) exploits the weakness (part C) against the B/D's asset (part A). This will give an idea of the potential impact of a security incident.

To enhance the understanding of these four inputs, mapping threats to assets and vulnerabilities can help to identify their possible combinations. Each threat can be associated with a specific vulnerability or even multiple vulnerabilities. However, a critical point to consider is that unless a threat can exploit a vulnerability, it would not pose a risk to an asset.

The range of all possible combinations should be refined prior to performing risk results analysis. Some combinations may not make sense or are not feasible. This interrelationship of assets, threats, and vulnerabilities is critical to analysing security risks. Factors such as project scope, budget, and constraints may also affect the levels and magnitude of these mappings.

Through this comprehensive process, B/Ds can accurately identify relevant risk scenarios, enabling more informed decision making and more effective risk management strategies.

4.4.1.3 Threat Identification

A threat is a potential event or any circumstance with the potential to adversely impact the information assets, systems and networks, in terms of confidentiality, integrity and availability. Threat analysis may need to be occasionally revised to reflect any new potential threats to the information asset.

Examples of sources of threats are:

- Human errors.
- Disgruntled employees.
- Malicious or careless personnel.
- Misuse of systems and computer resources.
- Computer fraud.
- Theft.
- Industrial espionage.
- Environmental disasters.

Threat analysis is to identify the threats and to determine the likelihood of their occurrence and their potential to harm systems or assets. System errors or control logs can be a good source of data, which can be converted into threat event information and statistics. For each system, B/Ds shall identify a list of threats to their information systems by conducting a comprehensive threat identification. This task requires understanding who or what might threaten the B/D and how they might orchestrate an attack or compromise the B/D's assets.

Threats can be categorised into three main types:

- ***Social threats***: directly related to human factors, can be intentional or unintentional, such as human errors, results of omission or negligence, theft, fraud, misuse, damage, destruction, disclosure and modification of data.
- ***Technical threats***: caused by technical problems such as wrong processes, design flaws, breakage of communication paths like cabling.
- ***Environmental threat*s**: caused by environmental disasters such as fire, water damage, power supply, and earthquake.

In addition to these categories, continuous threat modelling is important, which involves regularly revisiting and updating threat models, especially following any changes in software, infrastructure, or the threat landscape. This ensures that the threat identification is up-to-date and relevant, effectively mitigating current and emerging threats.

Annex F shows some examples of threats.

Identifying and categorising relevant IT security threats is crucial for effective risk mitigation. To achieve this, B/Ds should develop a threat taxonomy that categorises and prioritises IT security threats based on their potential impact and likelihood.

A threat taxonomy is for organising and classifying different types of IT security threats. It helps B/Ds to understand the threat landscape clearly and enables them to prioritise their resources and efforts accordingly. The following are some suggested steps to be included when identifying and categorising IT security threats:

- ***Develop a Threat Taxonomy.*** B/Ds should create a process for organising and classifying different IT security threats, which include a wide range of threats such as malware, phishing attacks, Distributed Denial of Service (DDoS) attacks, insider threats, and advanced persistent threats (APTs). This provides a clear understanding of the threat landscape and enables resource prioritisation.

- ***Regularly Update and Refine.*** B/Ds should regularly review and update the threat taxonomy to adapt to the evolving threat landscape. In addition, B/Ds should stay informed about emerging threats, attack techniques, and vulnerabilities.

It is s also beneficial to consider various approaches to threat modelling, which can be used based on the specifics of the system and the threat landscape. These include asset-centric threat modelling, which focuses on system assets and the business impact of each asset's loss; attack-centric threat modelling, which looks at identifying the most likely successful threats against the system; and system-centric

threat modelling, which prioritises understanding the system being modelled before evaluating its threats.

B/Ds can enhance the threat identification process by utilising threat modelling. Threat modelling is a systematic process to identify, comprehend, and assess potential threats that could negatively impact a system or application. Threat modelling helps understand each system or application, identify viable threats, categorise them, and prioritise them based on risk. It aids in comprehending the attack surface, potential attack vectors, and the security controls that can mitigate these threats. Alongside the use of mnemonics such as cyber kill chains, the development of attack trees and publicly available knowledge bases of threat information, such as MITRE Adversarial Tactics, Techniques, and Common Knowledge ("MITRE ATT&CK"), can contribute to the threat identification.

The threat identification for each system should cover the following:

- Incorporating threat modelling to understand the system, identify and categorise threats, and determine viable attack vectors and mitigation strategies.
- Identifying possible threats to the B/D and the threat actor's objectives.
- Gaining insights into how these threats might compromise the B/D's valuable assets.
- Correlating the analysis and identification of threats to the context established in the first step.
- Developing an understanding of potential attack methodologies and techniques that threats might employ.
- Documenting the threat analysis.

B/Ds should initially understand and define the system. This could be a comprehensive network architecture, an application, or a software component. B/Ds should record the system details, including its purpose, users, functionality, and the data it processes and stores.

B/Ds should create a system diagram illustrating all the components and their interactions, including all data flows, entry points, exit points, and trust boundaries. The system diagram can demonstrate how data moves through the system and where potential vulnerabilities may lurk.

B/Ds can identify the potential threat by utilising the system diagram. B/Ds can use methods like STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege), for example. B/Ds should consider how the system could be compromised for each component or data flow in the diagram.

While STRIDE is a widely used method for threat modelling, there are additional frameworks that can further enhance the threat identification process. These include methodologies such as PASTA (Process for Attack Simulation and Threat Analysis), Trike, VAST (Visual, Agile, and Simple Threat modelling), and CVSS (Common

Vulnerability Scoring System). Each of these provides a unique perspective on threat modelling and can be selected based on the specific needs of B/Ds.

B/Ds can effectively utilise threat modelling to identify potential threats to their systems in a risk assessment. This shift from a reactive stance to a proactive approach helps B/Ds stay prepared and resilient against evolving IT security threats.

Annex G shows an example of a threat modelling form.

4.4.1.4 Vulnerability Identification

Vulnerability is a weakness in operational, technical and other security controls and procedures that could be exploited by a threat, allowing assets to be compromised. Examples are the interception of data transmission and the unauthorised access of information by third parties. Vulnerability analysis is to identify and analyse the vulnerabilities of the system and environment. It is important to systematically measure these vulnerabilities, including thoroughly evaluating all security controls, procedures, and mechanisms.

Annex H shows some examples of vulnerabilities.

The context and characteristics of each vulnerability should be understood and documented. This includes the conditions for the vulnerability to be exploited and the potential impacts if the vulnerability were to be exploited.

Each vulnerability can be assigned a level or degree (e.g. high, medium, low) to indicate its importance. Key and critical assets must first be identified. The level of vulnerability can be determined based on several factors, including the ease of exploitation, the potential impact, and the existence of mitigating controls.

Vulnerability identification will concentrate on identifying vulnerabilities across the B/D's assets, systems, and networks. This process may involve the use of various tools and techniques, as well as the expertise of personnel in identifying weak points, such as insecure configurations, outdated software, and policy shortcomings.

Moreover, it's important to consider non-technical vulnerabilities that could be exploited, such as policy weaknesses, lack of user awareness, and inadequate physical security measures.

B/Ds shall identify their systems' vulnerabilities in a list of vulnerabilities for each system, which can exist in people, processes, places, and technology, and threat actors may exploit these vulnerabilities to achieve their aims and objectives.

The vulnerability identification for each system should cover the following:

- Identifying potential weaknesses in the B/D's defences that threat actors could exploit.
- Identifying vulnerability in terms of the ease by which it could be exploited, how widespread it is across the B/D and systems, and how easy it is for a threat actor to know or assume that it affects the B/D's systems and services.
- Conducting a thorough review of the system's configurations, hardware, software, and network infrastructure to uncover potential vulnerabilities.

Once vulnerabilities are identified, they should be documented and regularly reviewed to ensure that the B/D's understanding of its vulnerabilities remains current. This will also help to prioritise remediation efforts and allocate resources more effectively.

B/Ds should stay updated with the latest threat intelligence and security trends relevant to the B/D's industry and technology landscape. This information can help identify emerging threats, new attack vectors, and vulnerabilities that should be considered during the risk assessment. Regularly review and incorporate relevant threat intelligence sources into the risk assessment process.

In general, there are two common types of vulnerability identification appraoches:

- General Control Review
- System Review

4.4.1.4.1 General Control Review

This method is to identify any potential risks or threats in general controls being put in place for the current environment by examining the systems manually through interviews, site visits, documentation review, and observations, etc.

This may include but not be limited to the following:

- Departmental IT security organisation, in particular staff roles and responsibilities.
- Management responsibilities.
- IT security policies.
- Human resource security, including security awareness training.
- Asset management.
- Access control, such as password policy, access privileges.
- Cryptography.
- Physical and environmental security.
- Operations security.
- Communications security.

- System acquisition, development and maintenance.
- Outsourcing security.
- Security incident management.
- IT security aspects of business continuity management.
- Compliance.

The following methods can be considered in collecting the information:

- Site Visits: visit to the data centres, computer rooms, and office environment should be arranged to identify physical security risks. In addition, assessment team should record down on-site observations about system operations and end user behaviours (e.g. the use of password-protected screensaver) in order to verify if relevant security policies are followed accordingly.
- Group Discussions: group discussions or workshops can be facilitated by the assessment team to gather information about the existing security environment (controls and risks) of the B/D or information systems. The discussion can be any format and topic, depending on the target information to be gathered.
- Multi-level Interviews: on-site interviews with key persons or representatives at different levels may also be conducted to verify previously obtained information, and to improve the accuracy and completeness of the collected information.
- Questionnaires: questionnaires or checklists are effective tools to identify the potential risks. Questionnaires can be customised and developed by the security consultants to tailor for the environment.

For example, multi-level interviews may involve different categories of staff such as:

- Senior management: who decides strategies such as scope and objective of the assessment.
- Line management: who needs to understand the main business processes and procedures that would be affected by the strategic security changes.
- Human resources personnel: who need to identify specific controls for hiring, terminations and transfers of staff related to systems security and usage rights.
- Operational and technical personnel: who provide technical and operational information.

Annex A provides some guidance on general control review checklist.

Supporting evidence serves as the foundation for verifying the implementation and effectiveness of security controls and is indispensable for a comprehensive and reliable assessment. **Annex E** provides a sample list of documented information as supporting evidence.

During the security risk assessment, B/Ds are responsible for presenting evidence that corresponds with each evaluated control or criterion. This compilation of

evidence should be organised to correspond with the assessment's outcomes, showcasing the operational status and efficiency of the security controls.

Assessors are tasked with meticulously reviewing the evidence based on several key factors: relevance to the security controls, the accuracy of the information provided, the completeness of the evidence for each control, and the consistency of the evidence with the overall security objectives. The goal is to ensure that the evidence not only aligns with the assessment criteria but also convincingly demonstrates the controls' actual performance.

Should the evidence provided be deemed inadequate or fail to meet the necessary standards, B/Ds may be subject to further inquiry or be asked to submit additional evidence. It is crucial for B/Ds to recognise that incomplete or subpar evidence could cast doubts on the security controls' effectiveness and put the credibility of the security risk assessment.

A well-documented and transparent collection of supporting evidence significantly enhances the integrity and value of the security risk assessment or security audit. By presenting detailed and precise evidence, B/Ds affirm their dedication to maintaining solid security practices.

For a streamlined and effective assessment process, B/Ds should endeavour to provide evidence that is both clear and easily interpretable. Well-maintained documentation, logs, and test results not only expedite the assessment process but also contribute to a more profound understanding of the security controls in place. Likewise, assessors should maintain clear, detailed records of their assessment activities and conclusions. These practices ensure a robust, transparent, and effective assessment process.

4.4.1.4.2 System Review

This system review is to identify any vulnerabilities and weaknesses of network or systems. It will focus on operating system, administration and security monitoring tools in different platforms.

Examples are:

- System files or logs.
- Running processes.
- Access control files.
- User listing.
- Configuration settings.
- Security patch level.
- Encryption or authentication tools.
- Network management tools.
- Logging or intrusion detection tools.

Assessment team should also spot if there is any abnormal activity such as intrusion attempt.

To collectively gather the above information more efficiently and comprehensively, automated scripts and/or tools can be tailored to run on the target host to extract specific information about the system. Such information will be useful in the later stage of risk analysis.

After performing the review, the identified risks and recommendations should be documented and addressed in the design stage or other phases appropriately.

Technical vulnerability tests such as vulnerability scanning, penetration testing, configuration review and source code scanning should be performed to identify the vulnerabilities and weaknesses of network or systems when necessary. Before conducting the vulnerability scanning and/or penetration testing, the assessment team should agree with the B/D on the scope, possible impact and fallback/recovery procedure. This should be based on the Business Continuity Plan and Disaster Recovery Plan if Tier 2 or above information systems are involved.

Vulnerability scanning at network, hosts and systems should be performed to cover at least the following where appropriate:

- Network level probing/scanning and discovery.
- Host vulnerability tests and discovery.
- System/application (including web system/application) scanning.

The assessment team should review whether patches or compensating measures have been applied for all applicable known vulnerabilities including but not limited to all relevant security alerts issued by the Government Computer Emergency Response Team Hong Kong (GovCERT.HK).

4.4.2 Risk Analysis

4.4.2.1 Impact and Likelihood Assessment

Given the assets, threats and vulnerabilities, it is now possible to assess the impact and likelihood.

(i) Impact Assessment

Impact assessment, (or impact analysis or consequence assessment) is to estimate the degree of the overall harm or loss that could occur. Examples of impact are on revenues, profits, cost, service levels and government's reputation, damage to the confidentiality, integrity and availability of the concerned system. It is necessary to consider about the level of risk that could be tolerated and how, what and when the assets could be affected by such risks. The more severe the consequences of a threat, the higher the risk.

For each risk scenario identified, B/Ds shall identify potential consequences if the event occurs and document them in the risk assessment form.

B/Ds shall define the risk impact criteria. This involves establishing the varying levels of potential consequences, such as low, medium and high. Each level should be defined regarding the potential damage to B/D operations, financial loss, regulatory implications, or any other relevant impact measures.

B/Ds shall analyse the potential consequences for each risk scenario identified, considering what could happen if there is a loss of confidentiality, integrity, or availability of the relevant information. This should be performed from the bottom up, starting with the most basic security consequences.

For each potential consequence, B/Ds should estimate the impact of time or data due to the event due to interrupting or disturbing operations. These estimations should align with the predefined risk impact criteria.

(ii) Likelihood Assessment

Likelihood assessment is to estimate the frequency of a threat happening, i.e. the probability of occurrence. It is necessary to observe the circumstances that will affect the likelihood of the risk occurring. In general, the likelihood of a threat exploiting a system’s vulnerability can be measured in terms of different circumstances such as its accessibility and its number of authorised users. The accessibility of a system can be affected by many factors such as physical access control, system configuration, network type, network topology and network interfaces. The system with Internet connection is more likely to have its vulnerabilities exploited than an internal system. Also, the former one may

have a large number of authorised users (i.e. the public) than the latter internal system, which has limited number of users. A system with one user is clearly less likely to be exploited than a system with several hundreds or thousands of users. As more people can gain access to the system, it is more difficult to ensure that each individual user performs only those functions he or she is permitted to do. Normally, the likelihood of vulnerabilities exploited increases with the number of authorised users.

The likelihood can be expressed in terms of the frequency of occurrence such as once in a day, once in a month and once in a year. The greater the likelihood of a threat happening, the higher the risk. For example, if there had been a well-known vulnerability in application software, the likelihood of an intentional social threat exploiting this vulnerability is high. If the systems affected is critical, then the impact is also high. As a result, the risk of this threat is high.

B/Ds shall analyse the likelihood of each risk scenario identified and document it in the risk assessment form.

B/Ds shall define the risk likelihood criteria. This involves establishing the various levels of likelihood or probability of risk occurrence, such as low, medium and high. Each category should be defined in terms of frequency or potential recurrence of the risk event.

This should be performed considering the frequency of risk sources or how easily particular vulnerabilities can be exploited. The analysis should start from the ground level, considering the most basic likelihood elements.

For each likelihood measure, B/Ds should estimate the potential or recurring instances that could happen due to the event in the context of the identified risk scenario. This estimation should consider the effectiveness of existing controls and their ability to mitigate the identified weaknesses. These estimations should be in line with the predefined risk likelihood criteria.

For each identified risk, determine its impact and likelihood to give an overall estimated level of risk. Assumptions should be clearly defined when making the estimation.

Furthermore, B/Ds can refer to the assurance model in "Risk Assessment Reference Framework for Electronic Authentication" in analysing the risks relating to the registration and authentication process of the electronic service, including government-to-citizen (G2C) and government-to-employee (G2E) applications.

Techniques for Estimating Impact and Likelihood

- Improving Estimation Based on Knowledge of Prior Events

Information about previous risk events may be helpful when estimating the future impact and likelihood of those. For example, risk owners should consult IT security incident reports, industry literature, or their current IT service providers to describe loss events within a given sector or over a particular time frame. To determine the impact and likelihood of a IT security breach, the IT service provider or IT security insurance provider can be asked to provide details regarding previous breaches, their duration, the nature of data compromised, and the corrective measures taken.

- Three-Point Estimation

  The three-point estimation is useful to estimate the impact and likelihood of a risk scenario because it considers the judgement of available subject matter experts (SMEs). For example, to determine the impact of a successful phishing attack, the risk estimator could poll an SME regarding:

  - The most optimistic (or best case) estimate (O),
  - A most likely estimate (M), and
  - A pessimistic (or worst-case) estimate (P).

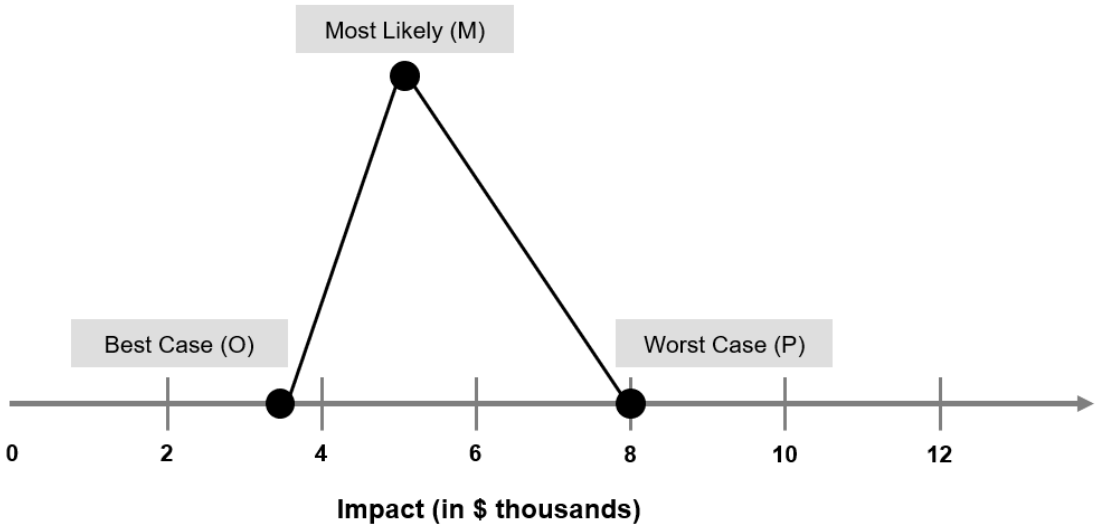

Figure 4.4 Example Three-Point Estimate Graph (Triangle Distribution)

The three datapoints can be categorised as **O**ptimistic ($35,000), **P**essimistic ($80,000), and **M**ost likely ($50,000).
The Estimated Value ("EV") is calculated by a simple average of the three numbers (called a "Triangular Distribution"):

$$EV = \frac{\text{P (\$80,000)} + \text{M (\$50,000)} + \text{O (\$35,000)}}{3} = \$55{,}000$$

In this attack scenario, if the estimator believes that the "pessimistic" and "optimistic" values are too different and that the "most likely" estimate is a better predictor, the estimator can give greater weight (perhaps four times as much) to the "most likely" value.

$$EV\text{^} = \frac{\text{P (\$80,000)} + \text{4M (\$50,000)} + \text{O (\$35,000)}}{6} = \$52{,}500$$

Although impact was used in this example, three-point estimating can also be used in determining likelihood.

(iii) Existing Control Identification

Upon completion of the likelihood and impact assessments, the next critical phase is the existing control identification. B/D shall identify all existing controls currently in place for each information system. This step involves identifying and evaluating current controls that aim to manage, mitigate, or eliminate the identified risks.

Step 1: Cataloguing Existing Controls

The initial phase of this step involves enumerating all the existing controls within the system. These controls can be broadly segregated into three categories:

Technical Controls: These mechanisms, often hardware or software, are implemented to safeguard systems and data. Firewalls, encryption techniques, antimalware software, and access controls are some examples of technical controls.

Physical Controls: These are tangible measures implemented to protect the B/D's assets and premises. They can range from security measures like CCTV cameras and access-controlled doors to environmental controls like fire suppression systems or secure disposal methods for physical data.

Administrative Controls: These are the policies, procedures, and training programs that govern the B/D's approach to information security. Examples of administrative controls include incident response plans, employee security training or awareness programs, data privacy policies, and disaster recovery plans.

Step 2: Evaluation of Control Effectiveness

An evaluation of each control's effectiveness is carried out upon identifying controls. B/Ds should understand the impact each control has on identified risks. This involves analysing how the control reduces the possibility of a threat successfully exploiting a vulnerability or diminishes the potential impact should the threat materialise. The effectiveness evaluation gives a clear understanding of the role each control plays in risk reduction.

All existing controls and their effectiveness shall be documented. This documentation should also include any dependencies between controls and the risks they mitigate.

4.4.2.2 Risk Results Analysis

B/Ds shall choose the suitable methodology for analysing identified risks. Risk results can be analysed using different methods and ways: Qualitative and Quantitative Methods, and Matrix Approach. The methodology selection should be made considering the form of output most useful to B/D, the relevant stakeholders and the available, reliable data. The fundamental objective of the risk analysis process is to determine the risks associated with each identified threat and vulnerability.

(i) Qualitative and Quantitative Methods

Qualitative method is to use descriptive, word scales or rankings of significance/severity based on experience and judgement. Examples are past experience, market research, industry practice and standards, surveys, interviews and specialists'/experts' judgements. This method requires a subjective assignment of categories, e.g. levelling using high, medium or low, ordinal ranking from 1 to 5, or degree of importance from least to most significant etc. Qualitative measure is more subjective in nature.

For instance, the value of an asset can be expressed in terms of degree of importance, e.g. least significant, significant and most significant.

Quantitative method is to use numerical information to arrive at percentages or numerical values. An example is the cost/benefit analysis. But this method requires more time and resources than the qualitative method, as every possible element (i.e. asset, threat or vulnerability) has to be categorised and considered.

For example, the value of an asset can also be expressed in terms of monetary value such as the purchase costs or maintenance costs. Threat frequency can be expressed in terms of rate of occurrence, e.g. once a month or once every year.

Normally, a qualitative method is used for initial screening while a quantitative method is used for more detailed and specific analysis on some critical elements and for further analysis on high-risk areas.

(ii) Matrix Approach

A matrix approach can be used to document and estimate the three major needs of security protection: confidentiality, integrity and availability in three different levels of severity (high, medium, low). The risk level can be ranked based on the criticality of each risk elements. Risk interpretation should better be limited to the most significant risks so as to reduce the overall effort and complexity.

Table 4.1 shows a sample Risk Ranking Matrix of a particular threat on a particular function or asset. For the Impact and Likelihood and System Tier columns, a value is assigned to each entry indicating the status (3-high, 2-medium and 1-low). As the risk level is the multiplication of the Impact's and the Likelihood's and the Information System Tier's values, it will thus have a value ranging from 1 to 27 (18 – 27: high, 9 – 17: medium, 1 – 8: low). With this matrix, it is possible to classify overall risk level of each information system.

System	**Impact (High, Medium, Low)**	**Likelihood (High, Medium, Low)**	**System (Tier 1-3)**	**Risk Level = Impact x Likelihood x System Tier (High, Medium, Low)**	**Risk Rating (1-8: low; 9-17: medium; 18-27: high)**
A	3	2	3	***18***	***High***
B	3	1	3	***9***	***Medium***
C	2	1	2	***4***	***Low***

Table 4.1 A Sample of Risk Ranking Matrix

The following example demonstrates another methodology to determine the risk rating.

There are different risk matrices for each tier of the system. In Table 4.2, Information System A of Tier 1, having a medium likelihood of a security breach and high impact, is categorised as a 'High Risk' according to the Tier 1 information system's risk matrix.

	High Impact	**Medium Impact**	**Low Impact**
High Likelihood	High Risk	Medium Risk	Low Risk
Medium Likelihood	Medium Risk	Low Risk	Low Risk
Low Likelihood	Low Risk	Low Risk	Low Risk

Table 4.2 A Sample of Tier 1 Information System Risk Ranking Matrix

In Table 4.3, Information System B of Tier 2, having a low likelihood of a security breach and medium impact, falls into the 'Low Risk' category, according to the Tier 2 information system's risk matrix.

	High Impact	**Medium Impact**	**Low Impact**
High Likelihood	High Risk	High Risk	Medium Risk
Medium Likelihood	High Risk	Medium Risk	Low Risk
Low Likelihood	Medium Risk	Low Risk	Low Risk

Table 4.3 A Sample of Tier 2 Information System Risk Ranking Matrix

In Table 4.4, Information System C of Tier 3, having a low likelihood of a security breach and high impact, is categorised as a 'High Risk' according to the Tier 3 information system's risk matrix.

	High Impact	**Medium Impact**	**Low Impact**
High Likelihood	High Risk	High Risk	High Risk
Medium Likelihood	High Risk	Medium Risk	Medium Risk
Low Likelihood	High Risk	Medium Risk	Low Risk

Table 4.4 A Sample of Tier 3 System Risk Ranking Matrix

Remarks for Table 4.1, Table 4.2, Table 4.3, Table 4.4:

- High Impact: Most significant: major loss and seriously damaging the organisation; severe, catastrophic, or serious long-term damage/disruption.
  e.g. DoS, unauthorised access to system.
- Medium Impact: Significant: medium loss which would be detrimental to the organisation; serious short-term, or limited long-term damage/disruption.
  e.g. intruder may gather system critical information to gain unauthorised access or launch further attacks.
- Low Impact: Least significant: low loss which would cause little or no damaging to the organisation; limited and short-term damage/disruption.
  e.g. intruder may gain non-critical information for processing.
- High Likelihood: Expected to occur in most circumstances.
- Medium Likelihood: Should occur occasionally.
- Low Likelihood: Could occur at specific time or in exceptional circumstances.
- High Risk Level: A low tolerance to risk exposures, i.e. requiring the highest security protection.
- Medium Risk Level: A medium tolerance to risk exposures.
- Low Risk Level: A high tolerance to risk exposures.
- Overall Result: Equal to the highest security risk level in various risk categories.

This matrix can be further extended by classifying sub-categories for risk exposures and with more weighted, numerical values for risk levels.

B/Ds shall determine the level of risk for each risk scenario, which is a combination of the assessed likelihood and impact. B/Ds shall also consider the system criticality tier in risk level determination. This ensures that the risk level accurately reflects the risk rating of each risk scenario, as well as the criticality of the affected system within the B/Ds.

4.4.3 Risk Evaluation

The purpose of risk evaluation is to support decisions. Risk evaluation involves comparing the risk analysis results with the established risk criteria to determine where additional action is required. This can lead to a decision to:

- do nothing further;
- consider risk treatment options;
- undertake further analysis to understand the risk better;
- Maintain existing controls;
- reconsider objectives.

The outcome of risk evaluation should be recorded, communicated and then validated at appropriate levels within the B/D.

4.4.3.1 Comparing the Results of Risk Analysis with the Risk Criteria

Once the risks have been identified and impact and likelihood values assigned, B/Ds should apply their risk acceptance criteria to determine whether or not the risks can be accepted. If they cannot be accepted, they should be prioritised for treatment.

B/Ds should compare the assessed risks with the criteria defined during the context establishment to evaluate risks.

The criteria for accepting risk can be a value above which the risks are deemed unacceptable.

Risk Level	Acceptable
High Risk	No
Medium Risk	Yes, with DITSO approval
Low Risk	Yes, with the system owner's approval

Table 4.2 Risk Acceptance Criteria Example

For example, in Table 4.3, all risks with low or medium levels would be considered acceptable by the B/D with corresponding approval, and all risks with high levels would be considered unacceptable.

Risk evaluation decisions should be based on comparing assessed risk with defined acceptance criteria, ideally taking into account the degree of confidence in the assessment. In some cases, such as the frequent occurrence of relatively low impact events, it can be helpful to consider their cumulative impact over some timescale of interest rather than the risk of each event considered individually, as this can provide a more realistic representation of overall risks.

There can be uncertainties in defining the boundary between those risks that require treatment and those that do not. Under certain circumstances, using a single level as the acceptable level of risk that divides risks that require treatment from those which do not is not always appropriate. In some cases, it can be more effective to include an element of flexibility into the criteria by incorporating additional parameters such as cost and effectiveness of possible controls.

The levels of risk can be validated based on consensus among risk owners and business and technical specialists. Risk owners must understand the risks they are accountable for that accord with objective assessment results. Consequently, any disparity between assessed levels of risk and those perceived by risk owners should be investigated to determine which better approximates reality.

4.4.3.2 Prioritising the Analysed Risk for Risk Treatment

Risk evaluation uses the understanding of risk obtained by risk analysis to make proposals for deciding the next step. Those should refer to:

- whether a risk treatment is required;
- priorities for risk treatment considering assessed levels of risks.

B/Ds shall prioritise these risks based on their assessed levels, considering the risk's potential impact and likelihood of occurrence. This process includes a comprehensive review of all identified risks from the preceding stages, aiming to arrange them in order of priority risk management based on the B/D's risk appetite and tolerance. Risk criteria used to prioritise risks should consider the objectives of the B/D, contractual, legal and regulatory requirements and the views of relevant interested parties. Prioritisation in the risk evaluation activity is mainly based on the acceptance criteria.

Each risk should then be given priority to indicate its significance and potential impact. Normally, the higher the security risk level, the higher priority should be given. In other words, higher priority risks are usually unacceptable and require more attention from management.

4.4.4 Risk Treatment

After reviewing the results of the security risk assessment, the risk owner should implement appropriate risk treatment to reduce the likelihood and impact of identified threats and vulnerabilities to an acceptable level.

The purpose of risk treatment is to select and implement options for addressing risks. Risk treatment involves an iterative process of:

- formulating and selecting risk treatment options;
- planning and implementing risk treatment;
- assessing the effectiveness of that treatment;
- deciding whether the remaining risk is acceptable;
- if not acceptable, further treatment is needed.

B/Ds shall choose and execute effective risk treatment options for managing identified risks following their risk appetite and tolerance.

4.4.4.1 Selecting Appropriate Risk Treatment Options

After the IT security risks are identified, analysis and prioritisation of risks should be performed, and B/Ds shall implement appropriate risk treatment options to safeguard their systems, including Risk Acceptance, Risk Reduction, Risk Avoidance, and Risk Transfer.

When	Options	Description	Action
• Risk falls within the predetermined risk tolerance range. • Usability or other factors outweigh security.	Risk Acceptance	To bear the liability	Making an informed decision to accept and do nothing (or nothing further) to treat, mitigate, modify or reduce an identified risk. This decision should be only considered when the cost of treating a risk might outweigh the cost of any impact that might be realised or the risk is tolerable in the context of the risk appetite for taking risk in pursuit of its objectives and priorities.

• It is a high risk and cannot be accepted.	Risk Reduction	To reduce the impact or the likelihood, or both	Implementing, managing and maintaining technical and non-technical controls that are aimed at either reducing the likelihood of an IT security risk occurring or reducing the impact if one does occur (to make an IT security risk acceptable or tolerable in the context of risk appetite.
• The risk is too high or costly to be reduced and unmanageable.	Risk Avoidance	To use alternative means or not to proceed with the task that would cause the risk.	Not pursuing or stopping the activity that led to a risk existing.
• Another party is willing to accept the risk. • Another party has greater control over the risk.	Risk Transfer	To shift the responsibility for the risk to the other party, either partially or fully	Transferring the impact or consequence of a risk being realised to someone else (e.g., insurance or outsourcing).

Table 4.2 Risk Treatment Options

When selecting risk treatment options, B/Ds should consider the value, perceptions and potential involvement of stakeholders and the most appropriate ways to communicate and consult with them. The application of risk treatment options does not need to be mutually exclusive. A risk owner is likely to apply a hybrid of multiple treatment options to achieve the desired effect. The goal of the risk owner is to evaluate the options that will best achieve the balance among value, risk, and resources.

For any of the options selected, recommendations on how to proceed with the selected option have to be made to management. Besides, safeguards and security controls have to be suggested if it is decided to reduce risk.

If no treatment options are available or treatment options do not sufficiently modify the risk, the risk should be recorded and kept under ongoing review.

Risk owners and other stakeholders should be aware of the nature and extent of the remaining risk after risk treatment. The remaining risk should be documented and subjected to monitoring, review and further treatment where appropriate.

4.4.4.2 Preparing and Implementing Risk Treatment Plans

The purpose of risk treatment plans is to specify how the chosen treatment options will be implemented so that arrangements are understood by those involved, and progress against the plan can be monitored. The treatment plan should identify how risk treatment should be implemented.

The information provided in the treatment plan should include:

- the rationale for the selection of the treatment options, including the expected benefits to be gained;
- those who are accountable and responsible for approving and implementing the plan;
- the proposed actions;
- the resources required, including contingencies;
- the performance measures;
- the constraints;
- the required reporting and monitoring;
- when actions are expected to be undertaken and completed.

4.4.4.3 Residual Risk

After the implementation of risk treatment plans, residual risks may remain. These risks exist even after all planned treatment measures have been applied. It is important to manage and document these residual risks in the risk register appropriately to ensure that they do not exceed the B/D's risk tolerance:

- Regularly monitor and review residual risks. This involves tracking changes in the risk landscape, reviewing the effectiveness of the risk treatment measures, and updating risk information accordingly.

- If a residual risk is deemed too high according to the B/D's risk tolerance, further risk treatment measures should be considered. This could include additional risk mitigation strategies or, in some cases, the decision to accept the risk if it is within the acceptable threshold but still requires monitoring.

4.4.4.4 Common Types of Safeguards

Safeguards can be quick fixes for problems found on existing system configurations or planned enhancements. Safeguards can be technical or procedural controls.

In general, safeguards can be classified into three common types:

- Barriers: keep unauthorised parties completely away from accessing critical resources.
- Hardening: make unauthorised parties difficult to gain access to critical resources.
- Monitoring: help to detect and respond to an attack promptly and correctly.

Examples of safeguards:

- Develop/enhance the departmental IT security policy, guidelines or procedures to ensure effective security.
- Re-configure operating systems, network components and devices to cater for the weaknesses identified during the security risk assessment.
- Implement password control procedures or authentication mechanism to ensure strong passwords.
- Implement encryption or authentication technology to protect data transmission.
- Enhance physical security protection.
- Develop security incident handling and reporting procedures.
- Develop staff awareness and training programs to ensure compliance with security requirements.

4.4.4.5 Major Steps of Identifying & Selecting Safeguards

The selection of appropriate security safeguards is not simple. It requires knowledge and technical skills on the system. The cost of managing risks needs to commensurate with the risk exposure. That is, the cost of reducing risk on a specific asset should not exceed the total value of that asset.

Listed below are several major steps of identifying and selecting safeguards:

- Select appropriate safeguards for each targeted vulnerability.
- Identify the costs associated with each safeguard such as the development, implementation and maintenance costs.
- Match safeguard/vulnerability pairs to all threats, i.e. develop a relationship between these measures and the threats.

- Determine and quantify the impact of the safeguard, i.e. the extent of risk that can be reduced after applying the selected safeguards.

Different combinations of physical, managerial, procedural, operational and technical based safeguards may be required. An analysis may be required to determine the optimal combinations for different circumstances.

A single safeguard may reduce risk for a number of threats. Several numbers of safeguards may act to reduce risk for only one threat. Hence, the integration of all safeguards shows the overall gross risk reduction benefit as a whole.

The effects of using different safeguards should be tested before implementation. Hence, this selection process may need to be performed several times to see how the proposed changes affect the risk results.

However, there are also other factors that have to be considered other than those identified in security risk assessment.

For example,

- Organisational factors like department's goals and objectives.
- Relevant statutory, regulatory and contractual requirements.
- Cultural factors such as social custom, beliefs, working styles.
- Quality requirements such as safety, reliability, system performance.
- Time constraints.
- Supporting services and functions.
- Technical, procedural and operational requirements and controls.
- Existing technology available in the market.

4.4.5 Monitoring and Implementation

Risk assessment results should be properly documented. This enables the security risk assessment process to be audited. This also facilitates on-going monitoring and reviewing.

Re-assessment should be conducted whenever necessary. It is essential to keep track of the changing environment and the changing priority of the identified risks and their impact. Security audit is one of the ways to review the implementation of security measures.

Roles and responsibilities of related personnel such as operators, system developers, network administrators, information owners, IT security officers and users should be clearly defined, reviewed and assigned to support the safeguard implementation.

Management should commit resources and provide support to monitoring and controlling the implementation.

The findings from the assessment should be transferred and documented in the system risk register. This ensures that all identified risks and their corresponding mitigation strategies are accounted for in a centralised and accessible location.

Establishing system level risk registers for each system is an essential practice for effective IT security risk management. These risks can then be documented in the system level risk register, providing a detailed picture of the unique risk landscape for that particular system.

B/Ds shall maintain system risk registers for their systems. This register shall document at least all identified risks, their potential impacts, the likelihood of occurrence, and the corresponding risk treatment option. It serves as a comprehensive record of the B/D's risk landscape at the system level, enabling effective monitoring, management, and communication of risks.

It's important to keep the system level risk register up to date, reflecting any changes in the system's risk landscape as well as the progress of risk treatment activities. This will ensure that the register remains a useful and accurate tool for understanding and managing system-specific risks.

A key part of effectively maintaining and utilising a system level risk register involves risk communication. It is importance to effectively communicate the information in the system risk register to DITSO, the risk owner and the system owner. This includes sharing the register with them in system security risk management. Clear and concise communication about risks and their risk treatment option is crucial. Transparent communication can foster a broader understanding of risks and promote collaborative efforts towards risk management.

ID	Priority	Risk Description	Risk Category	Impact	Likelihood	System Tier	Risk Rating	Risk Treatment Option	Risk Treatment Description	Risk Owner	Target Completion Date	Status
1												
2												
3												

Figure 4.5 Example of Risk Register Template

4.5 Deliverables

At different stages of security risk assessment, there may be different deliverables. A list of deliverables is shown below in Table 4.4. **Annex B** gives some examples of the contents of these deliverables for reference.

Item	Deliverables	Brief Description
1	Security Risk Assessment Report	A report which shows the results of security risk assessment with identified assets, threats, vulnerabilities, impacts and recommendations for enhancement or remediation
2	Risk Treatment Plan	A structured approach to managing and reducing risks identified from systems
3	System Risk Register	A system-based central repository for recording identified risks, their likelihood, impact, and associated treatment plans

Table 4.3 List of Deliverables

5. Security Audit

Security Audit is an audit on the level of compliance with the security policy or standards as a basis to determine the overall state of the existing protection and to verify whether the existing protection has been performed properly. It targets at finding out whether the current environment is securely protected in accordance with the defined security policy. It should be performed periodically to ensure the compliance of the security policies and effective implementation of security measures.

A security audit will require security policy and standards, audit checklists and an inventory list, which may cover different areas such as web application, network architecture, wireless communication, etc. **Annex C** lists different sample audit areas. **Annex D** provides a sample audit checklist under different security areas. **Annex E** provides a sample list of documented information as supporting evidence. Security audit may also involve the use of different auditing tools and different review techniques in order to reveal the security non-compliance and loopholes. After the audit process, an audit report will be prepared to highlight the conformance and gaps between the current protection and the requirements specified in the security policies and guidelines.

The selection of auditors and conduct of audits shall ensure objectivity and impartiality of the audit process. As a general principle, auditors shall not audit their own work. System related documentation could be reviewed by the security auditor for any insufficiency or non-conformance.

B/Ds should select an independent auditor not involved in the B/D's daily operations or system development processes. This ensures the auditor can offer an unbiased assessment of the system's security posture. The selected auditor should possess relevant professional qualifications, such as Certified Information Security Professional (CISP), Certified Information Systems Auditor (CISA) or Certified Information Systems Security Professional (CISSP). These certifications indicate that the auditor has the necessary knowledge and experience to conduct thorough and effective security audits.

The major objectives of a security audit are to:

- Check for compliance against the government security requirements based on objective evidence and inspection with existing security policy, standards, guidelines and procedures.
- Identify the inadequacies and examine the effectiveness of the existing policy, standards, guidelines and procedures.
- Identify and review relevant statutory, regulatory and contractual requirements.
- Identify, analyse and understand the existing vulnerabilities.

- Review existing security controls on operational, administrative and managerial issues, ensure effective implementation of security measures and compliance to minimum security standards.
- Provide recommendations and corrective actions for improvements.

5.1 Timing of Audit

Security audit is an on-going activity, and is not a one-off event. There are different scenarios when a security audit should be performed. The exact timing depends on your system requirements and resources.

- New Installation/Enhancement Audits: prior to implementation or major enhancements, in order to ensure conformance to existing policies and guidelines and meet the configuration standard.
- Regular Audits: conduct audits periodically, e.g. once a year, either manually or automatically using security-related tools in order to assure the minimum set of controls are implemented to detect and handle security loopholes or vulnerabilities.
- Sample Audits: to perform random checks in order to reflect the actual practice.
- Nightly or Non-Office Hour Audits: to reduce the auditing risks by performing during non-office hours or at night.

5.2 Auditing Tools

There are many automated tools which can help to find vulnerabilities. The choice of auditing tools depends on the security needs and the workload impact of monitoring.

For instance, some security scanning tools can check for any existing vulnerabilities on the network (network-based) or on specific hosts (host-based) through scanning and launching simulated attacks. Results are then shown in reports for further analysis.

These commercially available tools may be used together with security auditors' own developed tools. Latest tools used in the hacker community may also be used by security auditors to simulate the emerging attack activities.

Manual review techniques such as social engineering attacks and auditing checklists may be applied for non-technical reviews on all levels of security awareness within the organisation.

5.3 Auditing Steps

In general, a security audit can be divided into the following steps:

- Planning.
- Collecting audit data.
- Performing audit tests.
- Reporting for audit results.
- Protecting audit data and tools.
- Making enhancements and follow-up.

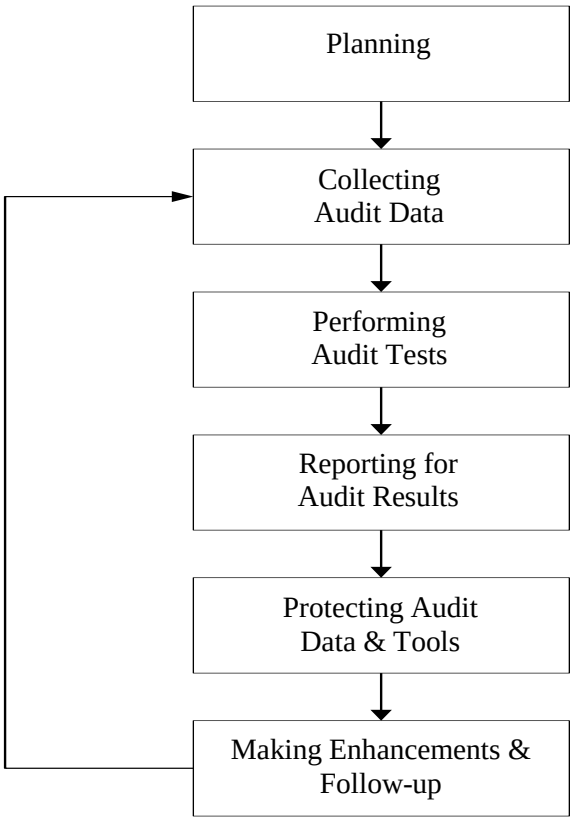

Figure 5.1 General Audit Steps

5.3.1 Planning

Planning helps to determine and select effective and efficient methods for performing the audit and obtaining all necessary information. The required time for planning depends on the nature, extent and complexity of the audit.

5.3.1.1 Project Scope and Objectives

Audit scope and objectives should be clearly defined and established. User requirements should be identified and agreed with security auditors before proceeding.

Examples of security audit scope are:

- Internet security
- General security of an internal network
- Tier 2 information systems
- Hosts security
- Network server's security such as web servers, email servers etc.
- Network components and devices such as firewalls, routers etc.
- General security of a computer room
- Network services such as directory services, mailing services, remote access services
- System documentation and records

Some audit objectives are listed below for reference:

- To ensure compliance with the system security policy and procedures with supporting evidence.
- To examine and analyse the safeguards of the system and the operational environment.
- To assess the technical and non-technical implementation of the security design.
- To validate lack of, proper or improper integration and operation of all security features.

5.3.1.2 Constraints

The period allowed for auditing should be adequate and sufficient enough to complete all tests. Sometimes the systems or networks have to be off-line or not in live production when performing the audit. Possible service interruption may occur. Backup and recovery of existing configuration and information must be performed before starting the security audit.

5.3.1.3 Roles and Responsibilities

Similar to conducting a security risk assessment, the roles and responsibilities of all parties involved should be carefully and clearly defined. Typical members involved can be referenced to "Section 4.3.1.4. Roles and Responsibilities of Stakeholders".

In particular, the security auditors, after their appointment, should plan for pre-audit by:

- Identifying and verifying the current environment via documentation, interviews, meetings and manual review.
- Identifying the significant areas or operations that are related to the audit.
- Identifying the general controls that may have effects on the audit.
- Identifying and estimating the resources required such as the auditing tools and manpower.
- Identifying any special or additional processing for the audit.

A security audit must be properly controlled and authorised before proceeding. A communication channel must be established between B/Ds and the security auditors.

On the other hand, there are two major areas that should be considered beforehand:

- Independence of Security Auditors

  It is required to consider whether the appointed security auditor is appropriate for the nature of the planned security audit. An independent and trusted party should be chosen to ensure a true, fair and objective view. The hiring of internal or external security auditors should be carefully planned, especially when dealing with classified information. The selection of auditors shall ensure objectivity. Auditors shall not audit their own work.

  Security audit is an ongoing process in discovering and correcting security issues. Same security auditor should be avoided to be engaging for a prolonged period so as to avoid the degradation of independence as well as to avoid the blind spots of the security review due to repetitive audits with the same approaches.

- Staffing

  The audit should be performed by auditors with sufficient skills and experience accompanied by system administrators. Roles, responsibilities and accountabilities of each involved party should be clearly defined and assigned.

5.3.2 Collecting Audit Data

It is required to determine how much and what type of information to be captured, and how to filter, store, access and review the audit data and logs.

The amount of data collected depends on the audit scope, objectives and data availability.

Careful planning is required for data collection. Such collection shall be in accordance with the government rules and regulations, and shall not create or initiate other potential security threats and vulnerabilities. All necessary data shall be collected, properly stored and protected from unauthorised access.

Audit data can be collected and stored in different ways. For example,

- Log files such as system start up and shut down information, logon and logout attempts, commands executed, access violations, accounts and password changes.
- Record such as audit trails, journals, summaries, detailed reports for all transactions, statistics reports or exception reports.
- Storage media such as optical disks.

Apart from electronic data collection, some physical or manual events should also be recorded and collected for future reference.

Examples are:

- Computer equipment repair and maintenance activities such as date, time, supporting vendor information and the activity's description.
- Change control and administration events such as configuration changes, installation of new software, data conversion or patches updating.
- Physical site visits by external parties such as security auditors or guests.
- Policy and procedures changes.
- Operation logs.
- Security incident records.

In general, the audit data collection steps may follow information gathering techniques as those in a security risk assessment. However, instead of assessing the risk exposures in the environment, the objective of a security audit is to review existing security controls on operational, administrative and managerial issues, and ensure compliance to established security standards. Audit data, or evidence, is collected to support whether proper security controls are in place and enforced appropriately.

5.3.3 Performing Audit Tests

After thorough planning and data collection, security auditors may perform:

- A general review on the existing security policies, standards or guidelines according to the defined scope of audit.
- A general review on the security configurations.
- Technical investigation by using different automated tools for diagnostic review and/or penetration tests.

Depending on the audit scope, different systems or network may be involved in a security audit. **Annex C** provides the purposes and coverages of different sample audit areas.

5.3.4 Reporting for Audit Results

A security audit report is required upon completion of audit work. Security auditors should analyse the auditing results and provide a report, which reflects the current security status. Performing further analysis on reports generated from scanning tools is necessary to remove non-applicable findings and false positives. The severity level may need to be adjusted in accordance with B/Ds' environment.

This audit report must be comprehensible by different readers such as IT management, executive management, related system administrators and owners, and the auditing and controlling sections.

See also **Annex B** for the suggested contents of a security audit report.

5.3.5 Protecting Audit Data & Tools

Throughout the stages of the security audit, it is essential to safeguard the audit data and tools.

Audit data and all documents relating to the audit shall be classified to an appropriate level and protected according to their classification.

The auditing tools should be properly maintained, controlled and monitored to avoid misuse. Such tools should only be used by the security auditors in a controlled manner. These tools should also be removed immediately after use unless proper control has been made to protect them from unauthorised access.

Security auditors shall also return all audit information to corresponding B/Ds after completing their audit services. The arrangement shall be agreed with security auditors in advance before their appointment.

5.3.6 Making Enhancements and Follow-up

If corrective actions are required, resources should be allocated to ensure that the enhancements could be performed at the earliest opportunity. Management of the system should be notified of any non-conformance. Details of follow-up can be referred in the later section.

6. Service Pre-requisites & Common Activities

6.1 Assumptions and Limitations

In conducting a security risk assessment or audit, a few assumptions have been made.

- There are limited time and resources.
- It is intended to mitigate and manage security risks as comprehensive as possible.

6.2 Client Responsibilities

When performing security risk assessment or audit by an external party, B/Ds should observe and be responsible for the following activities:

- Conduct background checks and qualification checks on supporting vendor and security consultants / auditors, to ensure that they possess necessary experience and expertise.
- Prepare an agreement for supporting vendor to sign, including but are not limited to the disclaimer of liability, the service details, and statement of non-disclosure, before starting any assessment or auditing activities. This is especially important when deciding to perform external penetration testing such as war dialling or hacking into the internal network from the Internet.
- Assign staff to be the primary and/or secondary points of contact for the vendor.
- Provide contact lists to vendor for both office and non-office hours whenever necessary.
- Be cooperative and open-minded. Acknowledge the results and develop plans for improvement if there are security needs.
- Allow physical and logical access only to the systems, network or computer equipment, which are necessary to perform the evaluations, and protect all assets that may be affected by this service.
- Obtain formal notification from the vendor about the level of impact or damage on the network, services or systems during the testing, so that recovery scheme and appropriate incident handling procedure could be ready before proceeding.
- Provide response to enquiries from security consultants / auditors within a reasonable time span.
- Provide sufficient office space and office equipment for the vendor to perform their service; a restricted area is preferred.
- Provide all necessary documentation about the specific area under assessment and audit such as logging policy or log review procedures, e.g. records of access log checking.
- Hold regular meetings with vendor for project control and review.

- Apply changes or enhancements at the earliest convenience after assessing the risk involved with fallback procedure ready, especially those that were at very high risks.

6.3 Service Pre-requisites

The following pre-requisites should be met:

- Provide all necessary documented information, either formal or informal, such as network diagrams, operation manual, user access control lists, security policy, standards, guidelines, and procedures. Please refer to **Annex E** for a sample list of documented information as supporting evidence.
- Provide personnel support related to the areas under study, including Internet usage, firewall configuration, network and system management, security needs and requirements, etc.
- Arrange guided site visit to gather more information for the assessment and audit.
- Choose independent third party to conduct security audit.

6.4 Responsibilities of Security Consultant / Auditors

In performing security risk assessment or audit for a B/D, the security consultants / auditors should:

- Possess the necessary skills and expertise.
- Understand the impact of every tool and estimate impact to the B/D.
- Obtain proper written authorisation from other necessary parties such as Internet Service Provider (ISP) and police, especially when performing hacking tests.
- Document every test regardless of whether it is successful.
- Ensure that the report reflects B/D's security policy and operational needs.
- Exercise good judgment in reporting immediately any significant security risk findings and non-conformance to the B/D.

6.5 Examples of Common Activities

Item	List of Activities	Description
1	Introductory Meeting	Agree on service scope, goals, and deliverables.
2	Project Planning	Develop a mutually agreeable delivery schedule and duration of service.
3	Preparation of Checklist	Prepare a checklist and have it agreed upon by the B/D.
4	Preparation of Fallback/Recovery Procedures for Technical Vulnerability Tests (such as vulnerability scanning, penetration testing, etc.)	Prepare fallback/recovery procedures before technical vulnerability tests and penetration tests.
5	Asset Identification and Valuation	Identify and evaluate assets in the agreed scope.
6	Security Risk Assessment	
	Risk Identification	Identify and document potential risks that could impact a system.
	Risk Analysis	Perform impact and likelihood assessment to determine the risk result.
	Risk Evaluation	Compare the result of the risk analysis with the established risk criteria to determine where additional action is required.
	Delivery of Security Risk Assessment Report, Risk Treatment Plan, and System Risk Register	Produce the security risk assessment report, risk treatment plan, and system risk register to state the findings and follow-up actions.
	Presentation of Security Risk Assessment Report, Risk Treatment Plan, and System Risk Register	Present the results and findings to management.
7	Security Audit	
	Compliance Check	Conduct compliance checking by documentation review, site visits, multi-level interviews, group discussion, surveys, etc. against S17 and departmental security policy or policies that are relevant and within the scope of security audit.
	Delivery of Security Audit Report	Produce the security audit report.
	Presentation of Security Audit Results	Present the results and findings to management.

Item	List of Activities	Description
8	Safeguard Data and Results	After completion of security risk assessment and security audit, all data collected and testing results & tools should be safeguarded.
9	Follow-up Actions	
	Development of Follow-up Plan	Develop a follow-up plan on recommendations with implementation schedule.
	Safeguard Implementation Review	Review the security status after implementation of safeguards.
	Delivery of Verification Report	Produce the verification report to conclude the finalised result of each finding.
10	Closure	
	Presentation of Verification Results	Present the results to management to close the project.

Table 6.1 Examples of Common Activities

7. Follow-Up of Security Risk Assessment & Audit

7.1 Importance of Follow-Up

The benefit of security risk assessment and audit is not in the recommendations made, but in their effective implementation. When a recommendation is made, the management is basically responsible for implementing it. If management has made the decision of not implementing a recommendation, they have to bear the associated security risk and non-conformance. Adequate reasons should be provided to support the decision.

There are three major areas of concern with regard to recommendations made in the security risk assessment and audit:

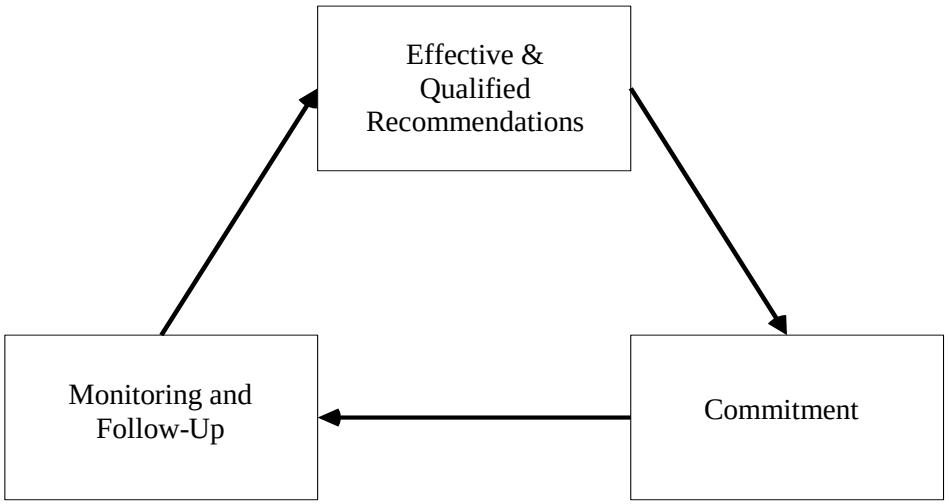

Figure 7.1 Follow-Up Actions on Recommendations

7.2 Effective & Qualified Recommendations

Security consultants / auditors are required to produce effective and qualified recommendations, which should possess the following characteristics:

- Specific and clear, readily understandable and identifiable
- Convincing and persuasive with sufficient evidence
- Significant
- Feasible and practical

In addition, the recommendations should be able to deal with the actual causes of problems, and should propose the best alternatives with supporting evidence and justifications. All these recommendations must be submitted to management which, in turn, has the authority to approve and enforce the recommendations.

7.3 Commitment

Individual and departmental commitment is important for implementation of the recommendations. Security consultants / auditors, staff and management may have different interests, emphasis and priority given to the recommendations.

7.3.1 Security Consultants / Auditors

Security consultants / auditors are those who first introduce the recommendations for improvement. They should:

- have confidence on their recommendations and if followed, there would be desirable improvements;
- understand the B/D's environment and its constraints such as time, resources and culture; and
- communicate through an appropriate and effective channel to give their recommendations.

7.3.2 Staff

Staff are specifically referred to those who would be directly or indirectly affected by the recommendations. They may need to provide support for implementing the recommendations, or they are actually the users who may have to change their daily operation procedures. They should be:

- encouraged and motivated to co-operate with the security consultants / auditors;
- given sufficient time and resources to perform the enhancements; and
- assured that they would benefit from the recommendations.

7.3.3 Management

Management plays an important role in enforcing the enhancements. They should:

- be proactive rather than reactive on security matters;
- provide sufficient support throughout the assessment or audit process;
- allocate sufficient resources for making the enhancements;
- understand that follow-up is a valuable and significant responsibility;
- encourage prompt enhancements with adequate planning, control and communication; and
- promote staff security awareness and training.

7.4 Monitoring and Follow-Up

Monitoring and follow-up consists of three major steps:

- Set up an effective monitoring and follow-up system.
- Identify recommendations and develop follow-up plan.
- Perform active monitoring and reporting.

7.4.1 Set Up Monitoring and Follow-up System

Management should set up a monitoring and follow-up system to follow up the recommendations. Besides those responsible for the security risk assessment or audit, management may assign additional staff to oversee the overall effectiveness of the monitoring system.

Management is responsible for providing adequate support, overall guidance and direction. It can establish scope, objectives and functions of the monitoring system. In addition, basic rules and guidelines can be set up as a general reference for performing security assessment monitoring and follow-up.

7.4.2 Identify Recommendations & Develop Follow-up Plans

To perform effective and prompt enhancements, the following have to be done:

- Identify key, significant and critical recommendations in which additional monitoring and maximum effort should be used.
- Develop a follow-up plan for all recommendations; this may include implementation plan, estimated time, action lists, results verification procedures and methods.
- Report and emphasise on key recommendations and highlight the follow-up process.
- Follow up all recommendations according to the plan.

7.4.3 Perform Active Monitoring & Reporting

Proactively monitoring and reporting the progress and status of actions, and taking follow-up actions on all recommendations are required until implementation is completed.

7.4.3.1 Progress & Status of Actions

There are different progress and status of actions:

- Actions not yet started or taken
- Completed actions.
- Actions being undertaken with a target completion date.
- Reasons for actions not being taken.
- Alternative actions if different from recommendations.

7.4.3.2 Follow-Up Actions

Some follow-up actions are suggested for considerations:

- Review the implementation plans, documentation and time frames for planned actions.
- Find and document the underlying reasons why the action was not taken.
- Establish additional steps or tasks to handle the technical, operational or managerial difficulties.
- Find and implement alternative recommendations due to unexpected environmental or requirement changes.

- Determine the "closing" of recommendations when they are proved to be successfully implemented and tested, to be no longer valid, or to be unsuccessful even after further actions.
- Assess the effectiveness of the corrective actions.
- Report accomplishment, status and progress to management.
- Escalate to management whenever applicable, especially when implementation of key recommendations is inadequate, delayed, or not taken.

*** ENDS ***

Annex A: Guidance on General Control Review Checklist

Depending on the scope of security risk assessment, there are many different areas that may need to be evaluated before security risks can be identified. Please note that the provided checklist below is not exhaustive and intended for reference purposes only. B/Ds or security consultants should customise their own checklists according to the specific project scope and objectives.

General Control Checklist	Testing Methods	Supporting Evidence	Implemented? (Y/N/NA)	Effective? (Y/N/NA)
Rules & Policy				
• Are there any appropriate security policy, guidelines or procedures established? • Do the existing security policy/procedures/guidelines adequately state what are allowed or not allowed to do? • Are staff and users informed of their obligation with regard to the relevant laws, security policy and procedures before giving access rights? • Are the security policy/guidelines/procedures readily available to users? • Are there any ongoing monitor and review on these security documents? • Is all the software used in the system complying with the existing intellectual property rights and licensing agreements? • Are all the rules and policy correctly followed and observed?	• Review security policies and procedures against systems/practices • Interview staff to check awareness and compliance with policies • Verify policies are accessible to all users	• Copies of security policies/procedures • Training/awareness records acknowledging policies • Meeting minutes reviewing policies		

General Control Checklist	Testing Methods	Supporting Evidence	Implemented? (Y/N/NA)	Effective? (Y/N/NA)
• Are these security documents regularly reviewed to address the threats emerged from new technologies?				
System Service Usage & Support				
• Does the system solely used for performing official duties and no massive violation in usage? • Are all the users adequately trained for using the systems/services offered to them? • Are there any written application and authorisation procedures for applying and granting the rights for using the service or system? • Do the service vendors provide a reliable supporting service? • Is appropriate protection given on the IT assets provided by service vendors? • Is the service vendor's performance properly monitored, controlled and reviewed?	• Review system logs to check for misuse • Interview users and check training records • Review application/authorisation records for services • Interview vendors and review contracts • Monitor vendor performance metrics	• System logs analysed for misuse patterns • Training records and curricula • Service application/approval records		

General Control Checklist	Testing Methods	Supporting Evidence	Implemented? (Y/N/NA)	Effective? (Y/N/NA)
System/Network Integrity				
• Is it forbidden for users to have a connection or gain access to the service or system by themselves? e.g. Internet connection • Are all hosts and workstations configured to prevent active contents or applets? • Are system logs or error logs been kept for an appropriate period of time? • Are all logs, with both logical and physical control, protected from unauthorised access and modification? • Is there any protection in the system or network from the external side to gain access to it? • Is there any classified data being sent without encryption across the network? • Are there digital certificates technology been used? If then, which service or application are they being used for?	• Conduct network scans to check for open ports/services • Review system configs to verify protection settings • Review logs on systems to check required fields and retention • Review logs and verify protection from unauthorised access	• Network/system configuration documentation • Log analysis reports on integrity checks • Network scans/vulnerability assessments		
Intrusion Detection & Monitoring				
• Is there any security incident response/handling procedure? • Do all the related parties understand and follow this procedure, at least the part	• Review incident response procedure and records	• Incident response procedure document • Past incident tickets and resolutions		

General Control Checklist	Testing Methods	Supporting Evidence	Implemented? (Y/N/NA)	Effective? (Y/N/NA)
which they are supposed to be responsible and affected by? • Has the security incident response/handling procedure stated any immediate actions should be performed in case suspicious activity occurred? • Are there any audit trail/logs, reports or alerts produced if there are any suspicious activities? • Is there any periodic or regular review on this procedure? • Are there sufficient reports to facilitate monitoring of users' activities, e.g. user identity, user log in/log out, connection date/time, services used, type of data sent/received, access rights given, usage of email, Internet, printer and removable media, computer equipment allocated for the users etc.? • Are the users' activity monitoring reports generated and reviewed regularly? • Are there any security breaches happened in the past? What was the recent/latest security breach? How was it handled? • Is there any dedicated staff for monitoring the service/network?	• Interview stakeholders and verify understanding of procedures • Scan for logs/alerts of suspected intrusions • Review monitoring reports over time	• Monitoring reports and alert logs		

General Control Checklist	Testing Methods	Supporting Evidence	Implemented? (Y/N/NA)	Effective? (Y/N/NA)
• Is there any contingency plan? Have they been tested and trial run before? Have these plans been regularly reviewed and tested to cater for the system/network changes? • Is there any detection and monitoring mechanism for emerging threats such as Denial of Service (DoS), Distributed DoS, Advanced Persistent Threat (APT) and Ransomware? • Are there any measures to mitigate the prevailing cyber security threats?				

General Control Checklist	Testing Methods	Supporting Evidence	Implemented? (Y/N/NA)	Effective? (Y/N/NA)
Physical Security				
• Are there any evidence or documents indicating that the computer rooms fulfill the physical security requirements according to the classification of data resided? Examples of the evidence or supporting documents include certification/notification issued by Architectural Service Department or relevant results from last SRAA reports. • Are all critical network components, e.g. firewalls, servers, routers and hubs located in a restricted or secured area? • Are there any environmental controls on the area where the network components are located to protect them from fire, power failure or irregular supply, flooding? • Are all the backups properly kept in a secure place? • Is there any access control on the network components such as with sign in and sign out logbook, control on the keys of the door of the computer room?	• Physically inspect security controls of computer rooms • Verify environment/access controls of critical assets • Check storage security of backups	• Facility access logs and records • Equipment inventories against physical checks • Environment monitoring records		
Change Control Management				
• Are the roles and responsibilities of the system administrators, users and operators	• Interview staff and check role/responsibility documentation	• Change request/approval documentation		

General Control Checklist	Testing Methods	Supporting Evidence	Implemented? (Y/N/NA)	Effective? (Y/N/NA)
clearly defined and assigned for accessing the system/network? • Have all the changes to configuration been formally approved, thoroughly tested and documented prior to implementation? • Is there any protection and access control on the configuration documentation to prevent unauthorised access? • Have all latest patches been applied to operating system and software? • Is there any logical access control on administration work both locally and remotely, if any? • Is there any dedicated staff assigned responsible for daily monitoring, administration and configuration? • Is there any training provided for the staff to perform the necessary system/network configuration function? • Do all the configurations fully backup both locally and remotely? Have all the backup media been securely protected?	• Review change records and verify testing/approvals • Attempt to access config docs to check for unauthorised access • Monitor systems to verify latest patches/configurations	• Testing plans and results • Configuration backups and version control		
Security Risk Assessment & Audit				
• Have there been any security risk assessments and security audit performed? • When, and what did each security risk assessment and security audit do?	• Review past risk assessment and audit reports	• Prior risk assessment/audit reports		

General Control Checklist	Testing Methods	Supporting Evidence	Implemented? (Y/N/NA)	Effective? (Y/N/NA)
• What were the major security risks identified? • Have there been any follow-up plans to implement the recommendations? • And, had they all been satisfactorily resolved? If not, why? • Have the unresolved follow-up plans been informed to the management? • Have the assessment and audit results been properly stored and saved up?	• Interview management on remediation of issues identified • Verify documentation of past assessments is maintained	• Remediation tracking documentation • Risk assessment methodology descriptions		

General Control Checklist	Testing Methods	Supporting Evidence	Implemented? (Y/N/NA)	Effective? (Y/N/NA)
Protection Against Malware				
• Are there any standard malware detection and repair measures or tools being used? Have they been installed in all hosts and servers? • Is there any standard or guidelines on how to use these malware detection and repair measures or tools? • Are all workstations and hosts installed with the latest malware definitions as well as updated with the corresponding detection and repair engines? • Are malware definitions kept up-to-date? At what time intervals will they be updated or distributed to users? • Have users been regularly informed about the latest malware definitions available? • Are the tools capable of checking any email macro viruses, compressed files, email attachments, memory resident data etc.? • Is there any supporting team to handle malware attacks? • If malware is detected, is it all investigated and followed up?	• Scan systems to verify anti-malware tools and definitions • Review update policies and procedures • Confirm staff awareness of updates • Simulate malware on systems to test detection capabilities	• Anti-malware deployment/update records • Malware detection test records • Helpdesk tickets on malware incidents		
Education & Training				

General Control Checklist	Testing Methods	Supporting Evidence	Implemented? (Y/N/NA)	Effective? (Y/N/NA)
• Are there any training or seminars about IT security? • Are there any periodic announcement or updates to users about changes on IT security technology, policy or news? • Are all supported staff having sufficient training to ensure proper network/system configuration, administration and monitoring?	• Review training records and materials • Interview staff to verify understanding from training • Check for refresher/awareness mechanisms in place	• Training materials, calendars and attendance • Email communications on updates/awareness • Staff interviews and qualifications		

Annex B: Sample Contents of Deliverables

B.1 Security Risk Assessment Report

A security risk assessment report should include but not limited to the following:

- Introduction/Background information.
- Executive summary.
- Assessment scope, objectives, methodology, time frame and assumptions for what are and are not covered.
- Current environment or system description with network diagrams, if any.
- Security requirements.
- Risk assessment team.
- Summary of findings and recommendations.
- Risk analysis results (recorded in the risk assessment form), including identified assets, threats, vulnerabilities and their impact, likelihood and risk levels with appropriate reasons.
- Recommended safeguards with cost/benefit analysis if more than one alternative, e.g. install defensive mechanisms or enhance existing security policy and procedures, etc.
- Conclusions
- Annexes to include completed general control checklist, vulnerability scanning report, penetration testing report, asset identification and valuation results, etc.

Sample Risk Assessment Form:

System	Threat	Vulnerability	Existing Control	Risk Description	Likelihood	Impact	System Tier	Risk Rating

- System: The system name.
- Threat: A threat is a potential event or any circumstance with the potential to adversely impact the information assets, systems and networks, in terms of confidentiality, integrity and availability.
- Vulnerability: Vulnerability is a weakness in operational, technical and other security controls and procedures that could be exploited by a threat, allowing assets to be compromised. Examples are the interception of data transmission and the unauthorised access of information by third parties.
- Existing Control: Existing controls currently in place for the information system.
- Risk Description: A brief explanation of the IT security risk scenario (potentially) impacting the system or B/D. Risk descriptions are often written in a cause-and-effect format, such as “if X occurs, then Y happens”.

- Impact: Analysis of this scenario's potential benefits or consequences if no additional response is provided. This may also be considered the initial assessment of the first iteration of the risk cycle.
- Likelihood: An estimation of the probability, before any risk response, that this scenario will occur. This may also be considered the initial assessment of the first iteration of the risk cycle.
- System Tier: The level of system criticality tier.
- Risk Rating: A calculation determined by the combination of impact, likelihood and other factors (e.g., system criticality).

B.2 Risk Treatment Plan

Risk Description	Risk Rating	Risk Treatment Option	Risk Treatment Measure	Risk Owner	Target Completion Date	Residual Risk Rating

- Risk Description: A brief explanation of the IT security risk scenario (potentially) impacting the system or B/D. Risk descriptions are often written in a cause-and-effect format, such as "if X occurs, then Y happens".
- Risk Rating: A calculation determined by the combination of impact, likelihood and other factors (e.g., system criticality).
- Risk Treatment Option: The risk treatment option (e.g. acceptance, reduction, avoidance, transfer) for handling the identified risk.
- Risk Treatment Description: A brief description of the risk treatment. For example, "Implement software management application XYZ to ensure that software platforms and applications are inventoried" or "Develop and implement a process to ensure the timely receipt of threat intelligence from [name of specific information sharing forums and sources]".
- Risk Owner: The designated individual or business unit responsible and accountable for ensuring that the risk is maintained in accordance with relevant requirements.
- Target Completion Date: The target completion date for risk treatment.
- Residual Risk Rating: A measure of the remaining level of risk after applying a risk treatment option. It helps assess the effectiveness of the chosen mitigation measures and guides resource allocation and decision-making.

B.3 System Risk Register

ID	Priority	Risk Description	Risk Category	Impact	Likelihood	System Tier	Risk Rating	Risk Treatment Option	Risk Treatment Description	Risk Owner	Target Completion Date	Status
1												
2												
3												
Continually Communicate, Learn and Update												

- ID (Risk Identifier): A sequential numeric identifier referring to a risk in the risk register.
- Priority: A relative indicator of the criticality of this entry in the risk register, either expressed in ordinal value (e.g., 1, 2, 3) or reference to a given scale (e.g., high, moderate, low).
- Risk Description: A brief explanation of the IT security risk scenario (potentially) impacting the system or B/D. Risk descriptions are often written in a cause-and-effect format, such as "if X occurs, then Y happens".
- Risk Category: Risk category groupings, such as by security and privacy control families (e.g., Access Control, Supply Chain Risk Management, such as those recorded in NIST SP 800-53). Categories could be any taxonomy that helps aggregate risk information and supports the integration of IT security risk registers for decision support.
- Impact: Analysis of this scenario's potential benefits or consequences if no additional response is provided. This may also be considered the initial assessment of the first iteration of the risk cycle.
- Likelihood: An estimation of the probability, before any risk response, that this scenario will occur. This may also be considered the initial assessment of the first iteration of the risk cycle.
- System Tier: The level of system criticality tier.
- Risk Rating: A calculation determined by the combination of impact, likelihood and other factors (e.g., system criticality).
- Risk Treatment Option: The risk treatment option for handling the identified risk.
- Risk Treatment Description: A brief description of the risk treatment. For example, "Implement software management application XYZ to ensure that software platforms and applications are inventoried" or "Develop and implement a process to ensure the timely receipt of threat intelligence from [name of specific information sharing forums and sources]".
- Risk Owner: The designated individual or business unit responsible and accountable for ensuring that the risk is maintained in accordance with relevant requirements.
- Target Completion Date: The target completion date for risk treatment.
- Status: A field for tracking the current condition of the risk and any next activities. The status could be a simple indicator (e.g., open, closed, pending, waived, transferred) or

provide a more detailed explanation (e.g., "risk accepted pending review by the Jan. 24 quarterly risk committee meeting"). Risk status should be a consistent set of indicators that helps aggregate risk information and supports the integration of IT security risk registers for decision support.

B.5 Security Audit Report

An audit report should include but not limited to the following information:

- Introduction/Background information.
- Executive summary.
- Audit scope, objectives, methodology, time frame, and assumptions and limitations.
- Description of current environment.
- Security requirements.
- Audit team.
- Declaration of security auditor's independence[1].
- Summary of findings.
- Details of tests and their results and findings.
- Recommendations and corrective actions based on the problem areas found, e.g. violation of security policy, misconfiguration, well-known and potential vulnerabilities, information leaks, unused services especially those default ones, and unused accounts and so on.
- Conclusions
- Annexes to include audit checklist, vulnerability scanning report, penetration testing report, etc.

[1] In case there is potential for impaired independence due to non-audit involvement, information about the non-audit role should be disclosed.

Annex C: Different Sample Audit Areas

C.1 Firewall

This audit area is to ensure that its firewall and associated systems have been properly configured to enforce the security policy with the minimal and optimal security protection. The firewall should be audited not only for its configuration, but also for its physical access control.

This audit area may cover the following:

- Physical access control to the firewall host.
- Firewall operating system version and patches.
- Firewall configuration and controls on Internet traffic such as rulebase and ports opened.
- Services permitted or disallowed to go through the firewall.
- Current architecture of Internet connection such as connections with routers, proxy servers, email servers and web servers.
- Connection with other third-party products for additional services such as malware detection and repair measure.
- Remote connection support and configuration.
- Administration and change control procedures.
- Access control list, if any.

The security audit report should summarise the firewall evaluation and recommendations in the firewall architecture, configuration, administration and operation.

C.2 Internal Network

The goal of this audit area is to discover any vulnerability that could be exploited by authorised internal users, and to identify any weaknesses and strengths in the controls of the internal systems and networks. The topology of internal network infrastructure may be reviewed as well.

The audit test usually includes an internal network scan to check for any security holes on specified times or pre-agreed periods. The scanning on critical hosts or workstations may be included.

This audit area would likely cover:

- Scanning of internal workstations, servers or networks to identify hosts, services and network configuration.
- Identifying vulnerabilities, protocol and configuration errors on operating systems, internal firewalls, routers, network components and infrastructure.
- Attempting intrusion of internal network and systems.
- Evaluating internal security related to access control and monitoring, administration and change control procedures and practices.
- Recommending measures to strengthen the network security.

C.3 External Network

The goal of this audit area is to identify security weaknesses of the systems and networks from outside such as the Internet. This helps to anticipate external attacks that might cause security breaches by scanning and launching attacks (i.e. hacking) from Internet to internal network at specified and pre-agreed time and locations.

The audit area would cover:

- Scanning internal servers for ports and services vulnerable to attack.
- Scanning external network gateways to identify ports, services and topology.
- Attempting to gather internal configuration information from external.
- Launching intrusion attacks to internal systems from external.

Agreements must be set up to clearly define the auditing scope and testing level details, e.g. which network segments/components or the acceptable severity of attack. The security auditor must commit to minimising disruption and avoiding damage to the systems and network.

C.4 Host Security

The purpose of this audit area is to assess the operating system level security of different computer platforms. Misconfiguration of the operating system may open up security loopholes that may not be known by the system administrators.

When considering the operating system security, accounts & password management, file system, networking workgroups, access permissions and auditing/logging are all common components that should not be omitted. Details are elaborated as follows:

Accounts and Password Management

- Password control policy such as password minimum or maximum length.
- User profiles, privileges and permissions.
- Default user or administration accounts.
- Group accounts.
- Account policy such as account lockout, account validity period.

File System

- System files protection and access permissions.
- Files access control lists.
- Network File System (NFS) usage.

Networking Workgroups

- Domain and trust relationships.
- Workgroups.
- Shared directories.
- Replicated directories.
- Remote access control.

Access Permissions

- Default directory permission.
- Shared workstation permission.
- Shared printer permission.
- Registry permission.
- Shared file permission.

Auditing/Logging

- Event logs/system logs/error logs auditing.
- File and directory auditing.
- Registry auditing.
- Printer/removable media log auditing.
- Alerts.
- Accounting and audit trail protections.

C.5 Internet Security

This audit area is to identify security weaknesses of the systems and networks in connection with the Internet. It is a combination of the internal network and external network audit areas with focus on the Internet gateway.

This audit area includes, but not limited to, the following items:

- Firewall and routers configuration.
- Security controls on host servers such as web servers, mail servers, authentication servers.
- Host, system and network security administration, and the control policy and procedures.
- Physical security of the Internet gateway network components and servers.
- Network security in Internet gateway segment and interfaces with internal network.
- Capacity of defending DoS or DDoS attacks from external to the internal Internet gateway.
- Compromise of the internal network components.

C.6 Remote Access

The audit area deals with vulnerabilities associated with remote access services via communication links such as dial-up connections and broadband connections (e.g. VPN, TLS VPN, etc.) This audit area may involve the following activities:

- Use automatic dialling/connection software to identify remote access users.
- Review security and configuration of remote access servers and the network where they are located.
- Conduct site visits to review the physical controls and location of modems or remote connection devices.
- Establish a remote access control policy or procedure.

Remote access without controls may open up a backdoor to external side. The problem is how to establish a secure connection.

The following may be identified and reviewed under this audit area:

- Applications/services requiring remote access and their security requirements.
- Any existing policies and procedures pertaining to remote access.
- Existing remote access connections such as using modems, remote access servers, modem pool connections, or broadband connections.

- Current remote access control methods.
- Current shortcomings and recommendations to improve the situation.

C.7 Wireless Communication

The audit area deals with vulnerabilities associated with wireless communication. This audit area should include, but not limited to:

- Assessing Service Set Identifier (SSID) naming as well as convention and other security configurations.
- Assessing current wireless encryption protocols and the strength of encryption cipher key and cipher algorithm, e.g. Wi-Fi Protected Access 3 (WPA3) supporting strong cryptography.
- Assessing the adoption of Virtual Private Network.
- Getting a list of access points and understanding their coverage.
- Identifying any unauthorised or rogue access points.
- Attempting to establish connection to the wireless communication.
- Attempting to gather internal system information through the wireless communication.
- Assessing if site survey is conducted and the coverage of wireless communication of the site.
- Assessing if the encryption key is properly protected at the client devices.

C.8 Phone Line

The goal of the audit area is to identify undocumented or uncontrolled modems connecting internal computers directly to the telephone network. This helps to eliminate any unauthorised or inappropriate modem connection and configuration to internal network and systems.

The audit area would cover:

- Assessing each modem entry point connected.
- Identifying any undocumented dial-up entry points.
- Attempting to establish connection to internal network.
- Attempting to gather internal system information through the connection.

C.9 Web / Mobile Application

The audit area deals with vulnerabilities associated with web / mobile applications. The following tests should be included in the audit area:

- Validating if security requirements are defined in early stage.
- Validating if security requirements specified in the functional specification document are met by the security controls implemented.
- Validating if malformed user inputs are handled or filtered.
- Assessing information leakage from error messages and meta data in the HTTP header for web application.
- Replaying security test cases prepared in the system acceptance test document for assuring proper security controls are maintained.
- Assessing the network and application architecture of the web / mobile application.
- Assessing if proper access control mechanisms are in place.
- Assessing the encryption mechanisms and protocols.
- Assessing the privilege of web / mobile application programs.

For best practices on web application security, please refer to Practice Guide for Website and Web Application Security.

C.10 Security Policy, Guidelines & Procedures

The objective is to review the existing security policy, guidelines and procedures. The review can focus on high-level / overall / organisation-wide security policy, or on specific systems, networks or components under concerns.

Listed below are some sample components under concerns:

- Remote access control.
- Internet access control, usage and monitoring.
- Internet email system.
- Operating system management.
- Password control policy.
- User account management.
- Network, systems or gateways administration.
- Change control practices.
- Network security practices.

Annex D: Sample Audit Checklist

Illustrated below are some examples of items to be checked in a security audit in compliance and best practice perspective. This checklist is not intended to cover all aspects, but rather acts as a preliminary reference. The auditor would customise the checklist based on the scope and environment of the audit, and may request B/Ds to provide the relevant records or documentations as supporting evidence.

Items to be checked	**Testing Methods**	**Supporting Evidence**	**Status** **(C= Compliance; NC = Non Compliance; NA = Not Applicable)**
Management Responsibilities			
• Departmental IT security organisational framework and the associated roles and responsibilities are defined. • Sufficient segregation of duties to avoid execution of all security functions of an information system by a single individual is applied. • Departmental budget covers the provision for necessary security safeguards and resources.	• Review documentation/records of IT security organisational structure, roles and responsibilities • Interview staff to verify roles and understand the segregation of duties • Review budget documentation to verify security is adequately funded	• Org charts, staff job descriptions, roles documentation • Budget plans highlighting security allocation	
IT Security Policies			
• Security policy is well documented and easy to understand. • Security policy is easily accessible by all involved parties.	• Review security policies and compare them to the implementation	• Copies of security policies and awareness materials • Policy implementation/compliance reports	

Items to be checked	Testing Methods	Supporting Evidence	Status (C= Compliance; NC = Non Compliance; NA = Not Applicable)
• Security policy is periodically reviewed, and updated with endorsement to reflect current environment. • Users are informed and commit to the security policy. • All rules stated in the security policy are implemented. • Security policy is approved, promulgated and enforced by the Head of B/D and the management.	• Interview staff to observe awareness and commitment to policies • Audit systems to verify the technical implementation of policies		
Human Resource Security			
• All staff are advised with acknowledgement of their IT security responsibilities upon being assigned a new post, and periodically throughout their term of employment. • All roles & responsibilities are clearly defined. • Adequate training on security is given to relevant parties. • Access to classified information higher than RESTRICTED is restricted to officers who have undergone appropriate integrity checking as stipulated by the Secretary for the Civil Service.	• Review records of security briefings for new and existing staff • Verify staff background/reference checks for handling classified data • Interview staff and management to verify training adequacy	• Staff on-boarding and training records • Background/reference checks, personnel files	

Items to be checked	Testing Methods	Supporting Evidence	Status (C= Compliance; NC = Non Compliance; NA = Not Applicable)
• Information security responsibilities and duties that remain valid after termination or change of employment has been defined and communicated to the staff.			
Asset Management			
• An inventory of information systems, hardware assets, software assets, valid warranties, service agreements and legal/contractual documents are properly owned, kept and maintained. • Computer resources and information are returned to the Government when a staff is transferred or ceases to provide services to the Government. • Information is properly classified and its storage media is labelled and handled according to government security requirements. • Proper security measures are in place to protect storage media with classified information against unauthorised access, misuse or physical damage. • All classified information is completely cleared or destroyed from storage media before disposal or re-use.	• Physically verify/inventory assets against records • Review documentation of returned assets from transferring/leaving staff • Inspect labelling/handling of classified media and storage	• Asset registry, purchasing/transfer records • Media labels/logs, storage access records	
Access Control			

Items to be checked	Testing Methods	Supporting Evidence	Status (C= Compliance; NC = Non Compliance; NA = Not Applicable)
• Personal Data (Privacy) Ordinance (Cap. 486) is observed when handling personal data. • User right assignment for various types of users on the system is documented and reviewed with appropriate segregation of duties. • There is a well-defined process to re-validate the user access right at the system and application level periodically. • User privileges and data access rights are clearly defined and reviewed periodically (e.g. at least once annually, preferably twice per year). • Records for access rights approval and review are maintained. • Each user is given with a unique user identity. • All users are granted with minimum privileges that are sufficient for carrying out their duties. • Users are informed about their privileges and access rights. • For distribution of user accounts and passwords, there are proper and secure procedures commensurate with the classification of information to be accessed.	• Audit system access rights against approvals and duties • Review password/authentication policies and configurations • Interview staff to verify password practices and remote access controls	• Access request/approval records • Password/remote access policies procedures • System access logs	

Items to be checked	Testing Methods	Supporting Evidence	Status (C= Compliance; NC = Non Compliance; NA = Not Applicable)

• Logs are properly kept for users' activities such as log in/out time, connection period, connection point, functions performed, etc.
• No unused accounts are found in the system/network.
• Administrators are also provided with user accounts.
• Administrator accounts are solely used for administration work.
• Users are classified into different categories with well-defined privileges for each category.
• There is a well-documented password policy for the system/network.
• Tier 2 information system follows the strong password policy.
• For strong password policy,
  o Last eight password selection(s) cannot be reused for renewal.
  o There is expiry period (3 – 6 months) on the password.
  o Maximum 5 trials are allowed for password attempts.
• No dictionary words, user names or obvious phrases are found in the password contents.			

Items to be checked	Testing Methods	Supporting Evidence	Status (C= Compliance; NC = Non Compliance; NA = Not Applicable)
• Users change the password regularly or immediately when their accounts are newly created. • No users write their passwords in labels or obvious place. • There are appropriate policies and procedures specifying the security requirement of using mobile computing and remote access. • There are control measures for remote access to the computers, application systems and data. • Multi-factor authentication is adopted for high risk access. • For remote access to the B/D's internal network via Virtual Private Network (VPN) connections or B/D's internal email systems via the Internet, multi-factor authentication is implemented. • Strong encryption and/or multi-factor authentication (for CONFIDENTAL data only) as well as inactive session timeout are in place over VPNs. • A formal usage policy and procedures is in place, and appropriate security measures shall be adopted to protect against the risks to IoT devices.			

Items to be checked	Testing Methods	Supporting Evidence	Status (C= Compliance; NC = Non Compliance; NA = Not Applicable)
Cryptography			
• Cryptographic keys through their whole life cycle including generating, storing, archiving, retrieving, distributing, retiring and destroying keys are properly managed.	• Review key management documentation and configurations • Conduct technical tests of encryption implementations	• Key management procedures/documentation • Encryption configuration files	
Physical and Environmental Security			
• There are evidence or supporting documents indicating that the physical security requirements of the computer rooms/server rooms/computer areas meets the requirements specified in the departmental IT security policy, government security requirements and other related standards. Examples include previous SRAA reports or certification/notification issued by Architectural Service Department. • All cables are tidy and properly labelled to assist maintenance and fault detection. • All under floor spaces, if any, are properly cleaned up. • The ceiling is regularly cleaned to avoid dust and dirt.	• Physically inspect security of computer rooms/facilities • Review service records for equipment like fire systems, temperature controls • Interview staff on physical security procedures	• Facility security assessments/certifications • Maintenance records, monitoring logs	

Items to be checked	Testing Methods	Supporting Evidence	Status (C= Compliance; NC = Non Compliance; NA = Not Applicable)
• Water detectors, if any, are fitted in the under floor space to detect flooding automatically. • Cables in ceiling voids are properly installed. • UPS are installed for necessary equipment. • UPS are capable to provide sufficient power supply for an expected period of time. • UPS are regularly tested. • UPS are located in a safe place. • Operators in a computer room are properly educated for the power supply control and power failure scenarios. • No inflammable equipment or materials are left in the computer room. • All automatic fire detection systems are operated in proper conditions with regular testing and inspection. • All automatic fire extinguishing systems installed are regularly tested and are in good conditions. • All water pipes passing through the room or under the floor, if any, are in good condition. • The room temperature and humidity is monitored and set in a way that fits for the computer equipment to be operated in good condition.			

Items to be checked	Testing Methods	Supporting Evidence	Status (C= Compliance; NC = Non Compliance; NA = Not Applicable)
• All keys of the doors in the computer room are properly issued, kept and recorded. • There are well-defined procedures for handling and distributing keys of the locks. • All personnel are trained and informed about the use of the fire extinguishers and other physical protection mechanism. • Smoking, food and drinks are not allowed inside the computer room. • Portable computers, mobile devices and other computer equipment, which are brought into the computer room, are controlled. • There are specially assigned staff responsible for arranging cleaning of the computer room. • There is regular inspection of equipment and facilities. • All visitors are authorised and identified before entering the computer room. • All visitors are accompanied with authorised staff at all times. • All visitors are provided with visitor labels when entering the room. • All visits are recorded. • There is proper access control to enter the computer room.			

Items to be checked	Testing Methods	Supporting Evidence	Status (C= Compliance; NC = Non Compliance; NA = Not Applicable)
• All entrances to computer room are controlled by locked doors. • Only authorised staff are allowed to enter the computer room with sign-in and sign-out processes. • All manuals and documents are not freely put aside and bookshelves are provided with filing and access controls. • Computer stationery held in a computer room is just sufficient for operation. No extra stock is held to avoid fire. • All computer stationery are properly kept and controlled. • There is procedure for issuing, authorising and recording computer stationery. • A proper inventory is kept and checked for all computer equipment. • Sample physically checking on the computer equipment against the inventory record is correct. • Mobile devices or removable media are secured when users have to leave their devices/media unattended. • IT equipment being taken away from sites is properly controlled.			

Items to be checked	Testing Methods	Supporting Evidence	Status (C= Compliance; NC = Non Compliance; NA = Not Applicable)
• Automatic re-authentication feature is used and enabled on all computers. • For IoT devices, security controls is enforced to protect the device against loss, theft and damage according to the classification of information being stored, processed and transmitted by the IoT devices.			
Operations Security			
• All software and files downloaded from the Internet are screened and verified with anti-malware solution. • There are procedures established and documented for backup and recovery. • Logs are kept for all backups and recovery taken including date/time, backup media used, taken by who, etc. • At least two backup copies are kept with one placed off-site. • There are well-defined retention periods and disposal procedures for backup media. • All backup media are properly labelled and locked in a safe place/area. • The place or cabinet where backup media is kept is always in lock.	• Monitor systems to verify anti-malware and patch management • Review logs, backup documentation and recovery tests • Observe administrators during activities to verify controls	• Patch/software update reports • Backup/DR test records and logs	

Items to be checked	Testing Methods	Supporting Evidence	Status (C= Compliance; NC = Non Compliance; NA = Not Applicable)
• There is proper transportation control for off-site storage. • Access to media is properly controlled and recorded. • An inventory is kept for all storage media. • Daily logs, e.g. system logs, error logs or user activity logs are properly kept, reviewed and analysed. • Logs of Approved Email System and Internet access service centrally provided by OGCIO or B/Ds are recorded. • Access to operating system utilities is restricted to authorised persons only. • No unused/suspicious services are running under the operating system account. • No unused user accounts are remained in the operating systems. • System logs are properly generated and reviewed on daily or regular basis. • The clocks of information systems are synchronised to a trusted time source. • Controls on changes to information systems are in place. Change records are maintained. • Patches are regularly applied to the operating systems to fix their known vulnerabilities.			

Items to be checked	Testing Methods	Supporting Evidence	Status (C= Compliance; NC = Non Compliance; NA = Not Applicable)
• An inventory record of hardware equipment and software packages (including the patch management system itself) and version numbers of those packages mostly used within the B/Ds is created and maintained. • Security risks of using end-of-support software are assessed and appropriate security measures to protect the information systems and related data are implemented by B/Ds.			
Communications Security			
• Network connected to Internet is protected by Firewall. • Intrusion detection strategy is implemented to detect abnormal activities on the network by installing a network intrusion detection system (NIDS) or network intrusion prevention system (NIPS) at critical nodes of the network. • Network segmentation/isolation is adopted and is a standard abided by all newly implemented systems or major enhancements and changes associated with the systems. • All remote access to the internal network is properly controlled with authentication and logs.	• Conduct network scans/tests and review firewall/IDS configurations • Verify encryption of critical transmissions • Review remote access authentication and logs	• Network diagrams, config files, rulesets • Encryption certificates/keys, VPN logs	

Items to be checked	Testing Methods	Supporting Evidence	Status (C= Compliance; NC = Non Compliance; NA = Not Applicable)
• Administration to network components is done by authorised staff only. • Controls are put on the use of network resources such as file sharing, printing, etc. to allow only authorised and authenticated users. • Upgrading on software located in the network is done by authorised persons only. • Policy is set up to control the proper use of the network and its resources. • Security protection, e.g. encryption, is used for information that is allowed to be transmitted and sent through the network. • Dedicated person is assigned to monitor the network performance and the daily operation. • All network user profiles are properly protected from unauthorised access. • Network configuration is documented and put in a secured place. • All network components are located in a secure area. • Proper security measures have been defined and implemented to ensure the security level of the departmental information system being			

Items to be checked	Testing Methods	Supporting Evidence	Status (C= Compliance; NC = Non Compliance; NA = Not Applicable)
connected with another information system under the control of another B/D or external party is not downgraded. • Agreement on the secure transfer of classified information between B/Ds and external parties are established and documented. • Wi-Fi infrastructure is reviewed to assess the impact of the vulnerability found in Wi-Fi communication standards and protocols periodically. • Resources records of Government's Internet domains is protected by prevailing security controls i.e. Domain Name System Security Extensions (DNSSEC). • HyperText Transfer Protocol Secure (HTTPS) is implemented for all Internet services, including informational websites.			
System Acquisition, Development and Maintenance			
• There are well-documented change control procedures. • Evaluation or estimation has been made on the effects of such change requests. • All changes are properly approved, recorded and tested before implementation.	• Review change control documentation and test changes • observe development/operations staff to verify practices	• Change requests, test plans/results • Source control/code quality tools logs	

Items to be checked	Testing Methods	Supporting Evidence	Status (C= Compliance; NC = Non Compliance; NA = Not Applicable)
• Adequate backups are performed before and after the changes. • Recovery procedures are defined before each change. • There are controls to ensure that no testing data/programs are resided in the production environment. • After applying to production environment, verification (e.g. manual review) has been made to assure that all changes were implemented as desired and planned. • There are proper access rights granted to allow only dedicated staff or administrator to amend the system/network's configuration. • The backup and recovery procedures have been revised to reflect the change if necessary. • Secure development environments for system development and integration efforts that cover the entire system development life cycle are established. • Version control mechanism is established to record changes to program source code over time during application development.	• Audit source code management and environments		

Items to be checked	Testing Methods	Supporting Evidence	Status (C= Compliance; NC = Non Compliance; NA = Not Applicable)
Outsourcing Security			
• Risks of utilising external services or facilities are identified and assessed. • Copy of signed confidentiality and non-disclosure agreement is properly managed. • All the government data in external services or facilities are cleared or destroyed according to the government security requirements at the expiry or termination of the service, or upon request of the government.	• Review third party contracts and due diligence performed • Verify return/destruction of data at contract end	• Contracts, due diligence documents • Data destruction certificates	
Security Incident Management			
• There is established incident monitoring and response mechanism, which has been tailored to specific operational needs, for each system. • There is predefined retention period of logs for tracing security incident when necessary. • Security incident response/handling procedure is periodically reviewed and drilled. (at least once every two years, preferably annually) • Should there be any security incidents, they are handled and escalated properly by staff, based on the established reporting channels.	• Review incident logs and reporting documentation • observe incident response to a test incident • Interview staff on procedure awareness and training	• Incident response procedure document • Past incident tickets and records	

Items to be checked	Testing Methods	Supporting Evidence	Status (C= Compliance; NC = Non Compliance; NA = Not Applicable)
• The latest version of the incident monitoring/response procedure is made available to the end users.			
IT Security Aspects of Business Continuity Management			
• Disaster recovery and emergency response plans are reviewed, drilled and updated according to documented frequency • Plans for emergency response and disaster recovery of Tier 2 or above information systems are fully documented, regularly tested and tied in with the Business Continuity Plan. • There is adequate resilience to meet the availability requirements of IT services and facilities.	• Review/observe testing of disaster recovery and business continuity plans • Verify system resilience and availability as defined in plans	• BC/DR plans, testing records, logs • System uptime/performance reports	
Compliance			
• Security policy should require that periodic security risk assessment and audit is performed. • The recommendations from the last security risk assessment and audit are followed up. • All relevant statutory, regulatory and contractual requirements to the system operation are identified and documented.	• Review documentation from past assessments/audits • Verify remediation of past issues and ongoing monitoring	• Previous audit/assessment reports • Remediation tracking documentation	

Items to be checked	Testing Methods	Supporting Evidence	Status (C= Compliance; NC = Non Compliance; NA = Not Applicable)
• Records to evidence compliance with security requirements and support audits of effective implementation of corresponding security measures are kept. • Selection of auditors and conduct of audits are objective and impartial. • Use of software and program for security risk assessment or audit is restricted and controlled. • Appropriate security measures are implemented throughout the whole data lifecycle for information system that involves personal data and a Personal Impact Analysis (PIA) shall be conducted if there has been any design change to the information system that has significant impact on personal data privacy.			

Annex E: Sample List of Documented Information as Supporting evidence

No.	Documented Evidence
1	IT Organisation Chart (with staff names & posts)
2	Structure of Information Security Organisation
3	Minutes for the Information Security Organisation meetings
4	Records of recent review or approval on departmental IT security policy, standards, guidelines and procedures
5	Records on recent distribution of department IT security policy with list of recipients
6	Policy on acceptable use of IT services and facilities
7	Records on recent distribution of policy in relation to acceptable use of IT services and facilities with list of recipients
8	Attendance list of awareness training
9	Materials of awareness training
10	Non-Disclosure Agreement signed by external service providers
11	Evidence on informing external service providers about their security responsibilities
12	Inspection records for equipment and communication facilities in the data centres or server rooms
13	Procedure for request and distribution of access keys, cards, passwords of the data centres or server rooms
14	Record of approval on requesting and distributing access keys, cards, passwords for entry to the data centres or server rooms
15	List of authorised persons to access the data centres or server rooms
16	Review records of the list of authorised persons to access the data centres or server rooms
17	Visitor access records for the data centres or server rooms
18	Inventory of information systems (with their system classifications), hardware assets (including notebooks, mobile devices and USB thumb drives), software assets (including desktop applications, mobile apps), valid warranties, service agreements, and legal/contractual documents.
19	Records of inventory check
20	Records on requesting IT equipment
21	User Account Maintenance Procedure
22	Records of approval for creation / modification of user account for access to internal network
23	Records of approval from DITSO for creation of shared user account for access to internal network
24	Account inventory list for shared user accounts with DITSO approval
25	Records on deactivation of user account for access to internal network
26	Record of handover and return of computer resources for staff resignation / termination / transfer
27	Review records of inactive user accounts for access to internal network
28	Review records on data access rights for user accounts

No.	Documented Evidence
29	Password policy or standards
30	Usage policies and procedures specifying the security requirements when using mobile computing and remote access
31	User acknowledgement on accepting their security responsibilities when using mobile devices and remote access
32	List of user accounts with remote access
33	Network diagram showing remote access points
34	Records of approval from DITSO for connection to internal network via privately-owned computer resources or IoT devices
35	Records of approval from Head of B/D for processing CONFIDENTIAL / RESTRICTED information in privately-owned computers or mobile devices
36	Certificates from external service providers on hard disk degaussing before disposal
37	Backup and restore policy or procedure
38	Records of review of backup activities
39	Records of restoration test of backup media
40	Transport log of backup media
41	Review records of logging on critical operations
42	Hardening guide for information systems and implementation records
43	Review records of system documentations
44	Upgrade plan with approval from the Head of B/D to implement encryption for RESTRICTED information not stored in mobile devices or removable media
45	Records of approval for broadband connections through stand-alone computers
46	Records of security patch evaluation and testing
47	Records of consultation for not applying a security patch
48	Records of request and approval for security patch installations
49	Records of computer equipment and software installation
50	Approved software list for user installation and its review record
51	Records of monitoring of software installed in end user workstations or mobile devices
52	Records of request and approval for installation of software not in the approved software list
53	Wireless security policy
54	Network diagram for wireless network
55	Policy on logging of activities of information systems
56	Review records on audit log for servers, network equipment, printer and removable media
57	Latest Security risk assessment report and follow-up action plan

No.	Documented Evidence
58	Documentation of relevant statutory, regulatory and contractual requirements applicable to the operations of information system. For example, contract, service level agreement (SLA), operational level agreement (OLA), etc.
59	Security audit report and follow-up action plan
60	Records of approval for running the software and programs (e.g. scanning tools) in the security risk assessment and / or security audit
61	Security incident response / handling procedure
62	Drill report on security incident response / handling
63	Records on recent distribution of security incident handling / reporting procedure with list of recipients
64	Latest Security incident report
65	Standard or policy for multi-factor authentication.

Annex F: Examples of Threats

Below are examples of threats. This table helps in identifying and documenting the threats which have the potential to adversely impact the information assets, systems and networks.

No.	Threat Description
1	Fire
2	Water
3	Pollution, harmful radiation
4	Major accident
5	Explosion
6	Dust, corrosion, freezing
7	Climatic phenomenon
8	Seismic phenomenon
9	Volcanic phenomenon
10	Meteorological phenomenon
11	Flood
12	Pandemic/epidemic phenomenon
13	Failure of a supply system
14	Failure of cooling or ventilation system
15	Loss of power supply
16	Failure of a telecommunications network
17	Failure of telecommunication equipment
18	Electromagnetic radiation
19	Thermal radiation
20	Electromagnetic pulses
21	Failure of device or system
22	Saturation of the information system
23	Violation of information system maintainability
24	Terror-attack, sabotage
25	Social Engineering
26	Interception of radiation of a device
27	Remote spying
28	Eavesdropping
29	Theft of media or documents
30	Theft of equipment
31	Theft of digital identity or credentials
32	Retrieval of recycled or discarded media

33	Disclosure of information
34	Data input from untrustworthy sources
35	Tampering with hardware
36	Tampering with software
37	Drive-by-exploits using web-based communication
38	Replay attack, man-in-the-middle attack
39	Unauthorized processing of personal data
40	Unauthorized entry to facilities
41	Unauthorized use of devices
42	Incorrect use of devices
43	Damaging devices or media
44	Fraudulent copying of software
45	Use of counterfeit or copied software
46	Corruption of data
47	Illegal processing of data
48	Sending or distributing of malware
49	Position detection
50	Error in use
51	Abuse of rights or permissions
52	Forging of rights or permissions
53	Denial of actions
54	Lack of staff
55	Lack of resources
56	Failure of service providers
57	Violation of laws or regulations

Annex G: Examples of Threat Modelling Form

The Threat Modelling Form is a tool used in the threat modelling activities. This form helps organise and document various elements related to threat scenarios.

Threat ID	Unique identifier assigned to identify each of the threat scenarios
Threat Scenario	Description of the threat scenarios
Threat Actor	Entities which may cause security impact.
Threat Action	Activities or tasks which Threat Actors will perform.
Impacted Entity	Potential victims of the threat scenario.

Here are a few basic examples as an illustrative reference.

Threat ID	TM001
Threat Scenario	Unauthorised Access to Confidential Data
Threat Actor	External Hackers
Threat Action	Exploiting system vulnerabilities, conducting phishing attacks
Impacted Entity	Citizen database, Financial records

Threat ID	TM002
Threat Scenario	Denial of Service (DoS) Attack
Threat Actor	Malicious External Actor
Threat Action	Flooding the network with excessive traffic, exploiting server weaknesses
Impacted Entity	Web application server, Network infrastructure

Threat ID	TM003
Threat Scenario	Insider Threat - Data Theft
Threat Actor	Disgruntled Employee
Threat Action	Unauthorised access to sensitive files, copying confidential information
Impacted Entity	Intellectual property, Employee records

Annex H: Examples of Vulnerabilities

Below are examples of vulnerabilities. This table helps in identifying and documenting various vulnerabilities that may exist within an information system or environment.

No.	Vulnerability Description
1	Insufficient maintenance/faulty installation of storage media
2	Insufficient periodic replacement schemes for equipment
3	Susceptibility to humidity, dust, soiling
4	Sensitivity to electromagnetic radiation
5	Insufficient configuration change control
6	Susceptibility to voltage variations
7	Susceptibility to temperature variations
8	Unprotected storage
9	Lack of care at disposal
10	Uncontrolled copying
11	No or insufficient software testing
12	Well-known flaws in the software
13	No “logout” when leaving the workstation
14	Disposal or reuse of storage media without proper erasure
15	Insufficient configuration of logs for audit trail’s purposes
16	Wrong allocation of access rights
17	Widely-distributed software
18	Applying application programs to the wrong data in terms of time
19	Complicated user interface
20	Insufficient or lack of documentation
21	Incorrect parameter set up
22	Incorrect dates
23	Insufficient identification and authentication mechanisms (e.g. for user authentication)
24	Unprotected password tables
25	Poor password management
26	Unnecessary services enabled
27	Immature or new software
28	Unclear or incomplete specifications for developers
29	Ineffective change control
30	Uncontrolled downloading and use of software
31	Lack of or incomplete back-up copies
32	Failure to produce management reports

33	Insufficient mechanisms for the proof of sending or receiving a message
34	Unprotected communication lines
35	Unprotected sensitive traffic
36	Poor joint cabling
37	Single point of failure
38	Ineffective or lack of mechanisms for identification and authentication of sender and receiver
39	Insecure network architecture
40	Transfer of passwords in clear
41	Inadequate network management (resilience of routing)
42	Unprotected public network connections
43	Absence of personnel
44	Inadequate recruitment procedures
45	Insufficient security training
46	Incorrect use of software and hardware
47	Poor security awareness
48	Insufficient or lack of monitoring mechanisms
49	Unsupervised work by outside or cleaning staff
50	Ineffective or lack of policies for the correct use of telecommunications media and messaging
51	Inadequate or careless use of physical access control to buildings and rooms
52	Location in an area susceptible to flood
53	Unstable power grid
54	Insufficient physical protection of the building, doors and windows
55	Formal procedure for user registration and de-registration not developed, or its implementation is ineffective
56	Formal process for access right review (supervision) not developed, or its implementation is ineffective
57	Insufficient provisions (concerning security) in contracts with customers and/or third parties
58	Procedure of monitoring of information processing facilities not developed, or its implementation is ineffective
59	Audits (supervision) not conducted on a regular basis
60	Procedures of risk identification and assessment not developed, or its implementation is ineffective
61	Insufficient or lack of fault reports recorded in administrator and operator logs
62	Inadequate service maintenance response
63	Insufficient or lack of Service Level Agreement
64	Change control procedure not developed, or its implementation is ineffective

65	Formal procedure for ISMS documentation control not developed, or its implementation is ineffective
66	Formal procedure for ISMS record supervision not developed, or its implementation is ineffective
67	Formal process for authorization of publicly available information not developed, or its implementation is ineffective
68	Improper allocation of information security responsibilities
69	Continuity plans do not exist, or are incomplete, or are outdated
70	E-mail usage policy not developed, or its implementation is ineffective
71	Procedures for introducing software into operational systems not developed, or their implementation is ineffective
72	Procedures for classified information handling not developed, or their implementation is ineffective
73	Information security responsibilities are not present in job descriptions
74	Insufficient or lack of provisions (concerning information security) in contracts with employees
75	Disciplinary process in case of information security incident not defined, or not functioning properly
76	Formal policy on mobile computer usage not developed, or its implementation is ineffective
77	Insufficient control of off-premise assets
78	Insufficient or lack of a "clear desk and clear screen" policy
79	Information processing facilities authorization not implemented or not functioning properly
80	Monitoring mechanisms for security breaches not properly implemented
81	Procedures for reporting security weaknesses not developed, or their implementation is ineffective
82	Procedures of provisions compliance with intellectual rights not developed, or their implementation is ineffective

B/Ds can make use of the table to aid vulnerability identification:

1. ***Review the Vulnerability Description column:*** Each row represents a specific vulnerability along with a brief description.
2. ***Assess B/D's information system or environment:*** Analyse B/D's information system, infrastructure, and processes to identify potential vulnerabilities that align with the descriptions provided in the table.
3. ***Match vulnerabilities to B/D's context:*** Identify vulnerabilities from the list that are relevant to B/D's information system or environment. Consider factors such as system configuration, software used, network setup, user practices, and physical security.
4. ***Document identified vulnerabilities:*** Create a list of vulnerabilities specific to B/D's system, mapping them to the corresponding numbers in the table. Include any additional details or context relevant to each vulnerability.