Cyber Security Auditing Guide

EXPOSURE DRAFT

DECEMBER 2023

Issued in South Africa

First Edition (Exposure Draft), December 2023

Glossary of Abbreviations

- Dos – Denial of Service
- FTP – File Transfer Protocol
- ICT – Information and Communications Technology
- IP – Internet Protocol
- ISP – Internet Service Providers

Table of Contents

1. PURPOSE

This audit guide aims to provide AFROSAI-E member SAIs with specific guidance and a reference model to facilitate the alignment of the coverage, methodology, and deliverables of a cybersecurity audit and risk assessment. With this guide, the users (managerial users, IT managers, system administrators and other technical and operational staff) can better understand cybersecurity risk assessment and audit. They should understand what preparations are required, which areas should be noted, and what results would be obtained.

Information Systems audits can be conducted as performance and/or compliance audits related to the specific subject matter of information systems or can be part of a larger audit engagement, which may comprise financial, compliance or performance audits. This guide takes cybersecurity as a specific subject matter of information systems that can be assessed within the SAI or another institution.

This document should be used with other security documents such as the Cybersecurity Technical Guide, Executive Guide and relevant procedures, where applicable.

2. DEFINITION OF TERMS

Information Security	A process of safeguarding information assets from unauthorised access, modification, use, disruption and destruction to ensure confidentiality, integrity, and availability of information.
Cybersecurity	Protection of cyberspace, including users, computers, servers, mobile devices, electronic systems, networks and data from malicious attacks.
Security Risk Assessment	An assessment involves identifying the risks in your company, your technology and your processes to verify that controls are in place to safeguard against security threats.
Cybersecurity audit	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.

Table 1: Definition of Terms

3. INFORMATION SECURITY MANAGEMENT

Information security is planning, implementing and continuously enhancing security controls and measures to protect information assets' confidentiality, integrity and availability, whether in storage, processing, or transmission. Information security management is a set of principles relating to planning, organising, directing, controlling, and applying 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.

3.1. Security Management Framework and Organisation

The *SAI may* establish and enforce departmental information security policies, standards, guidelines, and procedures according to business needs and government security requirements. The *SAI* may also define the organisation structure on information security and provide clear definitions and proper assignment of security accountability and responsibility to involved parties.

3.2. Governance, Risk Management and Compliance

The *SAI* may adopt a risk-based approach to identify, prioritise and address the security risks of information systems consistently and effectively. The *SAI* may perform security risk assessments for information systems and production applications periodically and when necessary. This will enable the SAI to identify risks and consequences associated with vulnerabilities. It may also provide a basis to establish a cost-effective security programme. The SAI may also regularly perform cybersecurity audits on information systems to ensure that current security measures comply with organisational information security policies, standards, and other contractual or legal requirements.

3.3. Security Operations

To protect information resources, the *SAI* should implement comprehensive security measures based on their business needs, covering different technological areas and adopt the principle of "Prevent, Detect, Respond and Recover". The principle is explained as follows:

- 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.
- Recovery measures restore the confidentiality, integrity and availability of information systems to their expected state.

3.4. Security Event and Incident Management

Security incidents might occur due to unforeseeable disruptive events. When security events give rise to a data security risk or compromise business continuity, the SAI may activate its standing incident management plan to identify, manage, record, and analyse security threats, attacks, or incidents in real time. The SAI should also prepare to communicate appropriately with relevant parties by sharing information on responses for security risks to subdue distrust or unnecessary speculation. When developing an incident management plan, the SAI should plan and prepare the right resources and establish the procedures to address necessary follow-up investigations.

3.5. Awareness Training and Capability Building

As information security is everyone's business, the SAI should continuously promote information security awareness throughout the organisation. To achieve this, the SAI may arrange sensitisation, training and education to ensure that all related parties understand the risks, observe the security regulations and requirements, and conform to security best practices.

3.6. Situational Awareness and Information Sharing

As the cyber threat landscape constantly changes, the SAI should also attend to current vulnerabilities, threat alerts, and important notices disseminated by the security industry. The security alerts on impending and actual threats should be disseminated to and shared with those responsible within the SAI so that timely mitigation measures can be taken. The SAI could use the cyber risk information sharing platform to receive and share information regarding security issues, vulnerabilities, and cyber threat intelligence.

4. SECURITY RISK ASSESSMENT AND AUDIT

4.1. Security Risk Assessment and Audit

Security risk assessment and audit is an ongoing process of cybersecurity practices to discover and correct security issues. They involve a series of activities shown in the figure below. They can be described as a cycle of iterative processes that require ongoing monitoring and control. Each process consists of different activities, some highlighted below as examples.

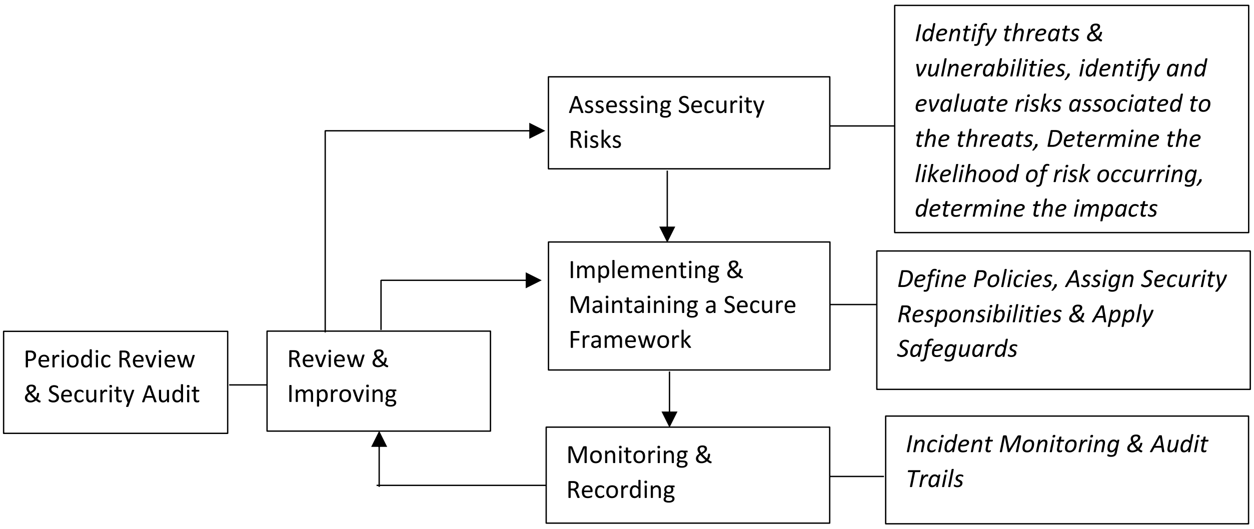
Assessing Security Risks
Identify threats & vulnerabilities, identify and evaluate risks associated to the threats, Determine the likelihood of risk occurring, determine the impacts
Implementing & Maintaining a Secure Framework
Define Policies, Assign Security Responsibilities & Apply Safeguards
Periodic Review & Security Audit
Review & Improving
Monitoring & Recording
Incident Monitoring & Audit Trails

Figure 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 programme.

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 the implementation of a secure framework, there is also the need for constant monitoring and recording so that proper arrangements can be made for tackling a security incident. Monitoring and recording may include day-to-day operations such as user access attempts (successful and failed) and activities while using a resource or information.

Cyclic compliance reviews and re-assessments follow this step (monitoring and recording) to ensure that security controls are properly implemented to meet users' security requirements and to cope with rapid technological and environmental changes. This model relies on continuous feedback and monitoring. The review can be done by conducting periodic cybersecurity audits to identify necessary enhancements.

4.2. Security Risk Assessment vs Cybersecurity Audit

Both the security risk assessment and the cybersecurity audit are ongoing processes but are different in terms of nature and function.

Security risk assessment is identifying, analysing and evaluating the security risks and determining 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 provides a basis for establishing a cost-effective security programme and implementing appropriate security protection and safeguards.

The security risk assessment is typically conducted at the beginning of the system development life cycle for a new information system. For an existing system, the assessments may be conducted continuously throughout the system development life cycle, including when major changes are made to the IT environment.

A cybersecurity audit is an audit on compliance with the security policy and standards to determine the overall state of the existing protection and verify whether the existing protection has been performed properly. The cybersecurity audit is an ongoing process to ensure that current security measures comply with organisational IT security policies, standards, and other contractual or legal requirements.

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

Security Risk Assessment	**Cybersecurity Audit**
The identification of threats 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 organisational 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 assessed against security policies, standards or other pre-defined criteria.
Conduct early in the system development life cycle for new information systems before the system is put into production.	Periodic review, ongoing process.
It can be a self-assessment or completed by an independent third party.	An independent third party must complete it.

Security Risk Assessment	Cybersecurity Audit
Key deliverables: risk register and risk mitigation measures.	**Key deliverable:** compliance checklist.

5. SECURITY RISK ASSESSMENT

Security risk assessment is identifying, analysing and evaluating the security risks and determining the mitigation measures to reduce the risks to an acceptable level. The assessment process of a system includes the identification and analysis of:

- all information assets of and processes related to the system
- threats that could affect the confidentiality, integrity or availability of the SAI information system
- system vulnerabilities and the associated threats
- potential impacts and risks from the threat activity
- protection requirements to mitigate identified 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 may 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 automated security assessment tools depending on the assessment scope, requirements, methodology, and international information security assessment standards and guides such as ISO 27005. After evaluating all collected information, a list of observed risk findings will be reported. Appropriate security measures will be determined, implemented and deployed for each reported risk. Due to the high demand for expert knowledge and experience in analysing the collected information and justifying security measures, a security risk assessment should be performed by qualified security person(s).

5.1. Benefits of Security Risk Assessment

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

5.2. Frequency and Type of Security Risk Assessment

5.2.1. Frequency of Security Risk Assessment

Security risk assessment is an ongoing activity. For a new information system, the assessment should be conducted early in the system development life cycle to identify security risks and implement appropriate security controls early. An existing system may be conducted at least [organisation-defined frequency] or when major changes are made to explore the risks in the information systems. A security risk assessment can only give a snapshot of the risks of the information systems at a particular time. For mission-critical information systems, it is recommended to conduct a security risk assessment more frequently.

5.2.2. Type 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 policy requirements and resources.

- ***High-level Assessment***: This assessment emphasises the analysis of organisational security posture and overall infrastructure or design of a system in a more strategic and systematic approach. In such assessment, SAIs with many information systems are looking for a high-level risk analysis of their information systems rather than a detailed and technical control review. It can also be applied to a system at the planning phase to identify risks or review general security controls before designing it.
- ***Comprehensive Assessment:*** This assessment is typically conducted periodically for the security assurance of an organisation’s information systems. It can be used to evaluate the risks of a particular system in an SAI and to provide recommendations for improvement. General control review, system review, and vulnerability identification will be conducted during the information gathering stage. A verification process should be followed to ensure all recommended remedies are properly implemented.
- ***Pre-production Assessment:*** Similar to the works performed in a “Comprehensive Assessment”, this assessment is commonly conducted on a new information system before it is rolled out or after a major functional change. For a new information system, *SAIs* should conduct a security review in the design stage of the system, which serves as a checkpoint to ensure necessary security requirements are identified and incorporated in the system design stage or other phases appropriately. The pre-production security risk assessment should verify the follow-up actions of the security review to ensure necessary security measures and controls are implemented in the system properly before going live.

5.3. Steps on Security Risk Assessment

Security risk assessment may involve several activities, as shown in the figure below. The typical steps may include Planning, Information Gathering, Risk Evaluation, Identifying and Selecting Safeguards and Monitoring and Implementation.

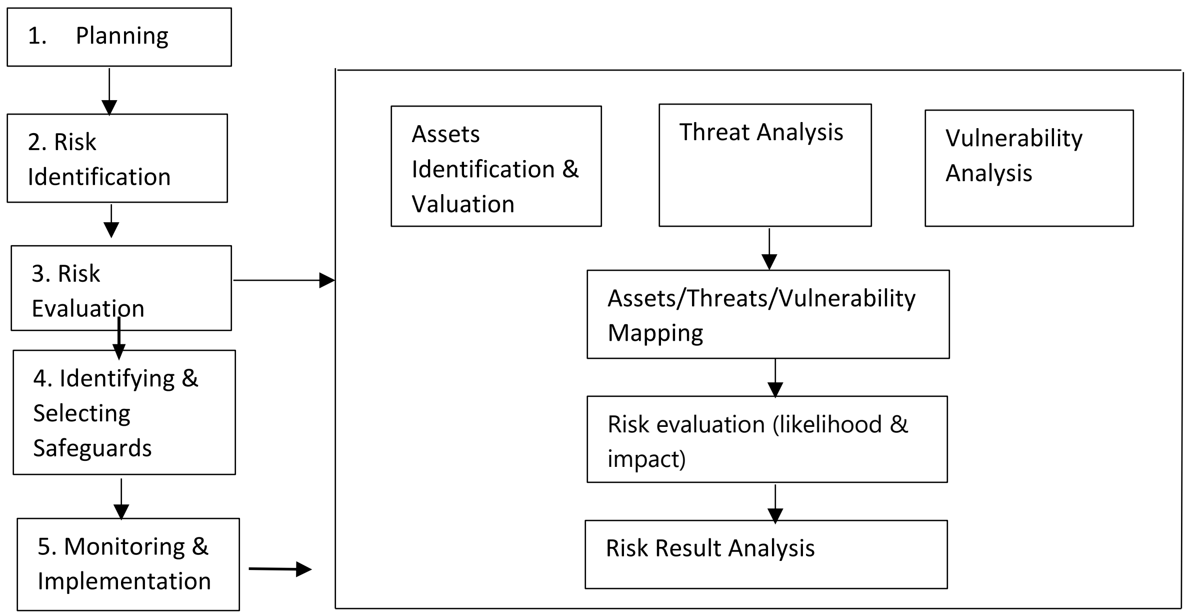
1. Planning
2. Risk Identification
3. Risk Evaluation
4. Identifying & Selecting Safeguards
5. Monitoring & Implementation
Assets Identification & Valuation
Threat Analysis
Vulnerability Analysis
Assets/Threats/Vulnerability Mapping
Risk evaluation (likelihood & impact)
Risk Result Analysis

Figure 2: Steps on Security Risk Assessment

5.3.1. 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, application, and security incident handling teams, 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. Below are several major items that may be defined first.

- Project scopes and objectives
- Background information
- Constraints
- Roles and responsibilities of stakeholders
- Approach and methodology
- Project size and schedule
- Data and tools protection

5.3.1.1 Project Scopes and Objectives

The project scopes and objectives can influence the style of analysis and types of deliverables of the security risk assessment. The scope of a security risk assessment may cover the connection of the internal network with the internet, the security protection for a computer centre, or even the information security of the whole organisation. Thus, the corresponding objectives may want to identify the security requirements, such as protection when connecting to the internet and potentially risky areas in a computer room, or assess the organisation's overall information security level. 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 SAI.

5.3.1.2 Background Information

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

5.3.1.3 Constraints

Constraints like time, budget, cost, technology, and other restrictions may also be considered. This may affect the project schedule and the available resources to support the assessment. For example, assessing during non-peak office hours or even during non-office hours may be necessary.

5.3.1.4 Stakeholders

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

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

5.3.1.5 Approach and Methodology

The assessment approach or methodology analyses the relationships among assets, threats, vulnerabilities and other elements. Numerous methodologies can be classified into two main types: quantitative and qualitative analysis. To be more helpful, 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.

5.3.1.6 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.

5.3.1.7 Data and Tools Protection

Throughout the stages of security risk assessment, a tremendous amount of data and system configurations will be collected; some may contain sensitive information. Therefore, the assessment team should store all collected data securely. File encryption tools and a lockable cabinet/room may 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 damage to the information systems. These tools should also be removed immediately after use unless there is proper control to protect them from unauthorised access. Examples of assessment tools include, but are not limited to – Tenable Nessus, Kali Linux, ArcSight, Nipper or any other internally developed cybersecurity audit workpapers).

A security risk assessment report will be compiled at the end of the assessment process to document all the risk findings. Any unauthorised access to such information, especially before rectification, may pose immediate threats to the SAI. Hence, the assessment team must enforce proper protection on the security risk assessment report during and after documentation. Senior management may also be reminded to treat the security risk assessment report in strict confidence. Lastly, the assessment team may return all requested data or documents to the SAI.

5.3.2. Risk Identification

The objective is to understand the existing environment and identify the risks by analysing the information collected.

By default, all relevant information should be collected irrespective of storage format. Below are several kinds of information that may be collected.

- Security requirements and objectives.
- System or network architecture and infrastructure, such as a network diagram showing how the assets are configured and interconnected.
- Information available to the public or found on 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 about minimum security control requirements.
- Documented or informal policies and guidelines.

In general, there are two common types of information collection methods:

- General control review
- System review

5.3.2.1. General Control Review

This method identifies 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 reviews, and observations.

This may include, but is not limited to, the following:

- Organisational IT security function, in particular, staff roles and responsibilities
- Management responsibilities
- IT security policies
- Human resource security, including security awareness and training
- Asset management
- Access control, such as password policy, access privileges
- Cryptography, including data encryption techniques
- 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

The following methods can be considered in collecting the information:

- **Site Visits**: Visits to the data centre, computer rooms, and office environment should be arranged to identify physical security risks. In addition, the assessment team should record on-site observations about system operations and end-user behaviours (e.g., using a password-protected screensaver) to verify if relevant security policies are followed accordingly.

- **Group Discussions:** The assessment team can facilitate group discussions or workshops to gather information about the information systems' security environment (controls and risks). 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 improve the collected information's accuracy and completeness.
- **Questionnaires:** Questionnaires or checklists are effective tools for identifying potential risks. The assessment team can customise and develop questionnaires tailored to the environment.

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

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

Using site visit and questionnaire methods may not be applicable or feasible for a high-level or design-phase assessment. Hence, the security assessment team should focus on information collected from group discussions and multi-level interviews.

5.3.2.2. System Review

This review is to identify any vulnerabilities and weaknesses of the network or systems. It will focus on operating systems, administration, and 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

The assessment team should also spot if there is any abnormal activity, such as an intrusion attempt.

To 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.

Technical vulnerability tests such as vulnerability scanning and penetration testing should be performed to identify the vulnerabilities and weaknesses of networks or systems when necessary. Before conducting the vulnerability scanning and/or penetration testing, the assessment team should agree with the SAI on the scope, possible impact and fallback/recovery procedure. If mission-critical systems are involved, this should be based on the Business Continuity and Disaster Recovery Plan.

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. Web penetration testing may be performed for internet-facing web applications processing classified information, websites with input fields or mission-critical systems.

5.3.3. Risk Analysis

NIST SP 1800-21C defines risk as identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Risk analysis 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

In general, this process may be divided into several sub-processes. They are:

- Asset Identification and Valuation

- Threat Analysis
- Vulnerability Analysis
- Risk Identification
- Impact and Likelihood Assessment
- Risk Results Analysis

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

5.3.3.1. Asset Identification and Valuation

All assets included within the scope of security risk assessment, both tangible and intangible, such as information, services, reputation, hardware and software, communications, interfaces, physical assets, supporting utilities, personnel and access control measures, must be identified.

Asset valuation approaches may differ and depend on the analysis method adopted. The value of an asset can be expressed in terms of:

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

The output checklist may include the following items:

- Name and type of the information assets.
- Physical location of the assets.
- Storage media and retention period before information stored/processed is destroyed.
- Nature of information stored/processed such as backup or original copy.
- Indicators showing the importance/values of the assets, such as the sensitivity levels, operation needs or criticality.
- Incoming/outgoing information flow, such as information transmission mode via email, dial-up modems or other telecommunication links.
- Software installed.
- Development and maintenance costs.
- Values of each identified asset.

5.3.3.2. Threat Analysis

A threat is a potential event or circumstance that can adversely impact the information assets, systems and networks regarding confidentiality, integrity and availability. Threat analysis may need to be occasionally revised to reflect any new potential threats to the information asset. Threat analysis is used to identify the threats and determine the likelihood of their occurrence and potential to harm information assets. System errors or control logs can be a good source of data, which can be converted into threat event information and statistics.

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 threat: caused by technical problems such as wrong processes, design flaws, and breakage of communication paths like cabling.
- Environmental threats: caused by environmental disasters such as fire, water damage, power supply, and earthquake.

5.3.3.3. Vulnerability Analysis

Vulnerability is a weakness in operational, technical and other security controls and procedures that could be exploited by a threat, allowing information assets to be compromised. Examples are the interception of data transmission and the unauthorised access to information by third parties. Vulnerability analysis is to identify and analyse the vulnerabilities of the system and environment. It is important to measure these vulnerabilities systematically. Each vulnerability can be assigned a level or degree (e.g., critical, high, medium, low) to indicate the extent of the vulnerability. Critical assets must first be identified. Vulnerability identification will concentrate on identifying vulnerabilities, with the assistance of automated tools or programs, over the network using one of the following methods:

i.) Vulnerability Scanning

The assessment team can perform vulnerability scans using an automated tool to identify known vulnerabilities on the target hosts or network devices. Like an anti-malware solution, scanning tools are installed on the assessment team's computer and require regular updating of the vulnerability signature files before use. Based on user requirements, a single or group of hosts/networks will be scanned for known vulnerable services (e.g., the system allows anonymous File Transfer Protocol (FTP), mail relaying) to identify any vulnerability.

For web or mobile applications, vulnerability scanning should be performed to discover security vulnerabilities before they are exploited before penetration testing.

ii.) Penetration Testing

Penetration testing can be performed internally or externally. It involves a manual process supplemented with automated tools, which may be installed on a portable computer, to scan the network or system to create a network map of connected workstations and servers and to identify vulnerabilities from either inside or outside the network and system under study by attempting to penetrate them. Penetration testing may also involve user interviews and hacking techniques to test the system or network. The level of details and hacking types must be thoroughly planned and agreed upon before proceeding. Hacking may stop after gaining access to a particular system or further in-depth analysis of the penetrated system. Legal matters should be settled beforehand when dealing with external ethical hacking. Typical steps of penetration testing are depicted in the figure below:

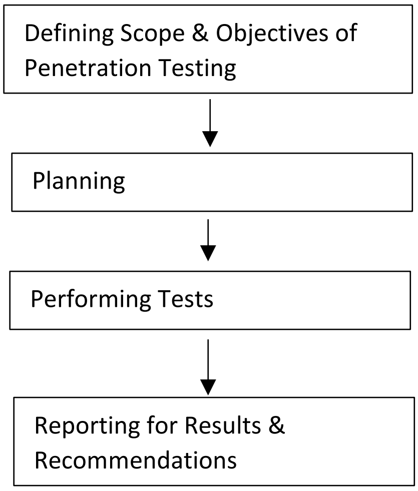
Defining Scope & Objectives of Penetration Testing
Planning
Performing Tests
Reporting for Results & Recommendations

Figure 3: Typical Steps of a Penetration Test

Before conducting penetration testing, SAIs should consider the following security concerns:

- The scopes and objectives must be clearly defined; machines/systems outside must be identified.
- The person conducting the penetration test should discuss and agree with the system owner on the suitability and impact of intrusive attacks and denial of service (DoS) attacks.
- The person conducting the penetration test shall sign a non-disclosure agreement to protect the privacy or confidentiality of the data in the system.
- Only acquire the service from service providers with good credibility and track record.
- Consider conducting background and qualification checks on the service providers to see if they possess the necessary experience and expertise.
- The latest full system backup of the target systems must be available because the penetration tests may impact the integrity of the data in the target system.
- Clearly define the "capture-the-flag" situation, such as placing a file in a designated directory, acquiring the password of some testing accounts, accessing designated web pages which should have proper access control, etc. Production data shall never be modified or deleted.
- Provide a contact list to the service providers for emergency contact, such as system owners and IT administrators. The staff will be the contact points for the vendor to report any emergency that arises

during the tests.

- Inform and alert the security monitoring service provider before the penetration testing unless it is intended to assess the effectiveness of the monitoring capability of the service provider.
- The machines' source Internet Protocol (IP) addresses will be tested to determine if an attack is genuine by examining and comparing the intrusion detection/prevention system logs.
- Consider arranging the penetration tests to be conducted at non-peak working hours.
- Ensure the service provider will not modify any user data even if the service provider can successfully access the user data.

5.3.3.4. Assets/Threats/Vulnerabilities Mapping

Mapping threats to assets and vulnerabilities can help identify their possible combinations. Each threat can be associated with specific or multiple vulnerabilities. Unless a threat can exploit a vulnerability, it would not be a risk to an asset. All possible combinations' ranges should be reduced before performing risk results analysis. Some combinations may not make sense or are not feasible. This interrelationship of assets, threats and vulnerabilities is critical to studying security risks. Factors like project scope, budget and constraints may also affect the levels and magnitude of mappings.

5.3.3.5. Risk Evaluation (Likelihood and Impact)

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

i.) Impact Assessment

Impact assessment (or impact analysis or consequence assessment) is used to estimate the degree of the overall harm or loss that could occur. Examples of impact are loss of revenue, loss of audit data, unauthorised access or leakage to audit reports, and damage to SAI. The more severe the consequences of a threat, the higher the risk.

ii.) Likelihood Assessment

Likelihood assessment is used 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 possibility of a threat exploiting a system's vulnerability can be measured in different events, 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. A system with an internet connection is more likely to have its vulnerabilities exploited than an internal system. Also, the former may have more authorised users (i.e., the public) than the latter's internal system, which has limited users. Typically, the likelihood of vulnerabilities being exploited increases with the number of authorised users. The likelihood can be expressed in terms of the frequency of occurrence, such as once a day, once a month, and once a year. The greater the likelihood of a threat happening, the higher the risk. For each identified risk, determine its impact and likelihood to give an overall estimated level of risk.

5.3.3.6. Risk Results Analysis

Risk results can be analysed using qualitative and quantitative methods and a matrix approach.

i.) Qualitative and Quantitative Methods

The qualitative method uses descriptive word scales or rankings of significance/severity based on experience and judgement. This method requires a subjective assignment of categories, e.g., levelling using high, medium or low, ordinal ranking from 1 to 5, degree of importance from least to most significant, etc. The qualitative measure is more subjective in nature. The quantitative method uses numerical information to arrive at percentages or numerical values. An example is the cost/benefit analysis. For example, the value of an asset can also be expressed in terms of monetary value, such as purchase costs or maintenance costs. Threat frequency can be expressed in terms of rate of occurrence, e.g., once a month or yearly. Normally, a qualitative method is used for initial screening, while a quantitative method is used for a more detailed and specific analysis of some critical elements and further analysis of high risk areas.

ii.) Matrix Approach

A matrix approach can be used to document and estimate the three significant needs of security protection: confidentiality, integrity, and availability, at three different levels of severity (high, medium, and low). The risk level can be ranked based on the criticality of each risk element.

Sample of Risk Ranking Matrix

Risk Categories	Impact (High, Medium, Low)	Likelihood (High, Medium, Low)	Risk Level (Impact x Likelihood)
Confidentiality	3	2	6
Integrity	3	1	3
Availability	2	1	2
Overall	3	2	6

Table 2: Sample of a Risk Ranking Matrix

Notes for Impact: Sample of Risk Ranking Matrix

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 the system
Medium Impact:	Significant: medium loss which would be detrimental to the organisation; short-term severe 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 damage to the organisation; limited and short-term damage/disruption, e.g. intruder may gain non-critical information for processing

Table 3: Notes for Impact: Sample of Risk Ranking Matrix

Notes for likelihood: Sample of Risk Ranking Matrix

High Likelihood:	Expected to occur in most circumstances
Medium Likelihood:	Should occur occasionally
Low Likelihood:	Could occur at a 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

Table 4: Notes for likelihood: Sample of Risk Ranking Matrix

This matrix can be further extended by classifying sub-categories for risk exposures and with more weighted numerical values for risk levels. Once the risk level is identified, a list of technical, operational and administrative requirements can be produced for each asset. This provides a basis for making decisions to accept, reduce, avoid or transfer the risk, as risks cannot be removed entirely, as shown in the table below.

When	Options	Description
Consequences/likelihood are low. Usability or other factors outweigh security.	Accept risk	To bear the liability.
It is high risk and cannot be accepted.	Reduce risk	To reduce the consequences or the likelihood of both.
The risks are too high or costly to be reduced and unmanageable.	Avoid risk	To use alternative means or not to proceed with the task that would cause the risk.
Another party is willing to accept the risk. Another party has greater control over the risk.	Transfer risk	To shift the responsibility for the risk to the other party, either partially or fully.

Table 5: Sample of Decision to Accept, Reduce, Avoid or Transfer Risk

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

5.3.4. Identifying and Selecting Safeguards

After reviewing the security risk assessment results, safeguards may be identified and evaluated for effectiveness. The security assessment team would recommend possible safeguards to reduce the likelihood and impact of identified threats and vulnerabilities to an acceptable level.

5.3.4.1. Common Types of Safeguards

Safeguards can be quick fixes or preventive solutions for problems found in 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: makes it difficult for unauthorised parties to gain access to critical resources.
- Monitoring: help 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 address the weaknesses identified during the security risk assessment.
- Implement password control procedures or authentication mechanisms 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 programmes to ensure compliance with security requirements.

5.3.4.2. Major Steps of Identifying & Selecting Safeguards

Below are several major steps for 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.

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.

Other factors that may be considered other than those identified in security risk assessment are:

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

5.3.5. Monitoring and Implementation

Risk assessment results should be appropriately documented. This enables the security risk assessment process to be audited. This also facilitates ongoing monitoring and reviewing.

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

Roles and responsibilities of related personnel should be clearly defined, reviewed and assigned to support the safeguard implementation. Management should commit resources and provide support to monitor and control the implementation.

5.4. Common Security Risk Assessment Tasks

Some of the common tasks that will be performed in security risk assessment are:

- Identify business needs and changes to requirements that may affect overall information systems and security direction.
- Identify and document all relevant statutory, regulatory and contractual requirements applicable to the operations of each information system.
- Analyse assets, threats, vulnerabilities, their impacts and likelihood.
- Assess physical protection applied to computing equipment and other network components.
- Conduct technical and procedural review and analysis of the network architecture, protocols and

components.

- Review and check the configuration, implementation and usage of remote access systems, servers, firewalls, external network connections, and client internet connections.
- Review password and other authentication mechanisms.
- Review the current level of security awareness and staff commitment within the organisation.
- Review agreements involving services or products from vendors and contractors.
- Develop practical technical recommendations to address the vulnerabilities identified and reduce the security risk level.

5.5. Deliverables

Some deliverables at different stages of security risk assessment may include:

Item	Tasks	Deliverables	Brief Description
1.	Security requirement identification	Security requirement report	A report shows the user security requirements on identified assets, threats, vulnerabilities, and impacts.
2.	Security risk assessment	Security risk assessment report	A report which shows the results of security risk assessment with identified assets, threats, vulnerabilities, impacts and recommendations for enhancement.
3.	Review existing security policies, guidelines and procedures	Gap assessment report	Gap assessment report on Information and Communications Technology (ICT) security policy, guidelines and procedures.

Table 6: Deliverables at Different Stages of Security Risk Assessment

6. CYBERSECURITY AUDIT

A cybersecurity audit is an audit on compliance with the security policy or standards to determine the overall state of the existing protection and verify whether the existing protection has been performed properly. It aims to determine whether the current environment is securely protected per the defined security policy. It should be performed periodically to ensure compliance with the security policies and effective implementation of security measures.

A cybersecurity audit will require security policy and standards, audit checklists and an inventory list, which may cover different areas such as web application, network architecture and wireless communication. Cybersecurity audits may also involve using different auditing tools and review techniques to reveal 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.

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 work.

The major objectives of a cybersecurity audit are to:

- Ensure compliance with security policies, standards, guidelines, procedures, laws, and regulations.
- Identify the inadequacies and examine the effectiveness of the existing policy, standards, guidelines and procedures.
- Identify compliance with the relevant statutory, regulatory, and contractual requirements.
- Review existing security controls on operational, administrative, and managerial issues to ensure effective implementation of security measures and compliance with minimum security standards.
- Identify and understand the existing vulnerabilities.

Provide recommendations and corrective actions for improvements.

6.1. Frequency and Timing of Audit

6.1.1. Audit Frequency

Cybersecurity audits should be conducted periodically to ensure compliance with security policies, guidelines, and procedures and to determine the minimum set of controls required to reduce risk to an acceptable level. It should be noted that a cybersecurity audit only gives a snapshot of the vulnerabilities revealed at a particular point in time.

6.1.2. Audit Timing

There are different scenarios when a cybersecurity audit should be performed. The exact timing depends on your system requirements and resources. These include:

- New Installation/Enhancement Audits: before implementation or significant enhancements, to ensure conformance to existing policies and guidelines and meet the configuration standard.
- Regular Audits: conduct audits periodically, e.g., once a year, manually or automatically, using security-related tools to ensure the minimum set of controls are implemented to detect and handle security loopholes or vulnerabilities.
- Random Audits: performing random checks 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.

6.2. Auditing Tools

Many automated tools can help 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 specific hosts (host-based) by scanning and launching simulated attacks. The commercially available tools may be used with cybersecurity auditors' developed tools. Manual review techniques such as social engineering attacks and auditing checklists may be applied for non-technical reviews on all security awareness levels within the organisation.

6.3. Auditing Steps

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

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

6.3.1. 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.

6.3.1.1. Project Scopes and Objectives

Audit scope and objectives should be clearly defined and established. User requirements should be identified and agreed between the parties before proceeding. Examples of cybersecurity audit scope are:

- Internet security
- General security of an internal network
- Mission-critical systems
- Hosts security
- Network server 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

Some examples of audit objectives are listed below for reference:

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

6.3.1.2. Constraints

The period allowed for auditing should be adequate to complete all tests. Sometimes, the information systems or networks must be offline or not in live production when performing the audit. Possible service interruption may occur. Before starting the cybersecurity audit, backup and recovery of existing configuration and information must be performed.

6.3.1.3. Roles and Responsibilities

Similar to conducting a security risk assessment, the roles and responsibilities of all parties involved should be carefully defined. Typical members involved can be referenced in 5.3.1.4.

Cybersecurity audit planning should include the following:

- 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.
- Estimating and identifying the resources required, such as the auditing tools and manpower.
- Identifying any special resources that may be needed for the audit.

A cybersecurity audit must be properly controlled and authorised before proceeding. A communication channel should be established between the cybersecurity auditors and management. On the other hand, two major areas should be considered beforehand:

i.) Independence of Cybersecurity auditors

It is necessary to consider whether the appointed cybersecurity auditor is appropriate for the nature of the planned cybersecurity audit. An independent and trusted party should be chosen to ensure an accurate, fair and objective view. The conduct of audits shall ensure objectivity and impartiality of the audit process. Auditors shall not audit their work.

ii.) Staffing

The audit should be performed by auditors with sufficient skills and experience accompanied by system administrators. Each involved party's roles, responsibilities and accountabilities should be clearly defined and assigned.

6.3.2. Collecting Audit Data

It is required to determine how much and what type of information to capture and how to filter, store, access, and review the audit data and logs. The data collected depends on the audit scope, objectives and availability. Careful planning is required for data collection. Such collection shall be based on government rules and regulations and 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 include system start-up and shut-down information, logon and logout attempts, commands executed, access violations, accounts and password changes.
- Reports include audit trails, journals, summaries, detailed reports for all transactions, statistics reports or exception reports.
- Storage media such as optical discs.

Apart from electronic data collection, some physical files should be collected for future reference.

Examples are:

- Computer equipment repair and maintenance activities include 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 patch updates.
- Physical site visits by external parties such as cybersecurity auditors or guests.

- Procedures and policy changes.
- Operation logs.
- Security incident records.

The audit data collection steps may follow information gathering techniques similar to those in a security risk assessment. However, instead of assessing the risk exposures in the environment, the objective of a cybersecurity audit is to review existing security controls on operational, administrative and managerial issues and ensure compliance with established security standards. Audit data or evidence is collected to support whether security controls are enforced appropriately. For details on the data collection techniques, please refer to **Error! Reference source not found.**.

6.3.3. Performing Audit Tests

After thorough planning and data collection, cybersecurity auditors may perform the following:

- A general review of security policies or standards according to the defined scope.
- A general review of the security configurations.
- Conduct technical investigations using different tools for diagnostic review and/or penetration tests.

6.3.4. Reporting for Audit Results

A cybersecurity audit report is required upon completion of audit work. Cybersecurity auditors should analyse the auditing results and provide a report reflecting 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 by the SAIs' 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.

6.3.5. Protecting Audit Data and Tools

Safeguarding the audit data and tools throughout the cybersecurity audit stages is essential. Audit data and all physical documents relating to the audit shall also be classified appropriately and protected according to their classification.

The auditing tools should be properly maintained, controlled and monitored to avoid misuse. Cybersecurity auditors should only use such tools 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.

Cybersecurity auditors shall also return all audit information to corresponding owners after completing their audit services. The arrangement shall be agreed upon with cybersecurity auditors before their appointment.

6.3.6. Making Enhancements and Follow-up

If corrective actions are required, resources should be allocated to perform the enhancements immediately.

7. LIMITATIONS

In conducting a security risk assessment or audit, the cybersecurity auditor should know the potential limitations experienced during the exercise. These may include the fact that there may be limited resources, including time.

8. RESPONSIBILITIES

8.1. Responsibilities of the Auditees

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

- Conduct background and qualification checks on supporting SAIs and security consultants/auditors to ensure they possess the necessary experience and expertise.
- Prepare an agreement for SAI to sign, including but not limited to the disclaimer of liability, the service details, and the non-disclosure statement, before starting any assessment or auditing activities. This is especially important when deciding to perform external penetration testing.
- Assign staff to be the service provider's primary and/or secondary contact points.
- Provide contact lists to the service provider for both office and non-office hours.
- Be cooperative and open-minded. Acknowledge the results and develop improvement plans.
- Allow physical and logical access only to the systems, network or computer equipment necessary to perform the evaluations and protect all assets that may be affected.
- Obtain formal notification from the service provider about the impact or damage on the network, services or system during the testing so that the recovery scheme and appropriate incident handling procedure can be ready before proceeding.
- Respond to enquiries from security consultants/auditors within a reasonable time.
- Provide sufficient office space and equipment for the service provider to perform their service; a restricted area is preferred.
- Provide all necessary documentation about the specific area under assessment, such as logging policy or log review procedures.
- Hold regular meetings with the service provider for project control and review.
- Apply changes or enhancements at the earliest convenience after assessing the risk involved with the fallback procedure, especially those at very high risk.

8.2. Responsibilities of the Auditors

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

- Possess the necessary skills and expertise.
- Understand the impact of every tool and estimate its impact on the SAI or the government institution.
- Obtain proper written authorisation from other necessary parties such as Internet Service Providers (ISPs) and relevant government authorities, especially when performing hacking tests.
- Ensure that the report reflects SAI's security policy and operational needs.
- Exercise good judgement in reporting immediately any significant security risk findings to the SAI.
- Document every test conducted and the outcome.

9. 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 auditee.
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.
	Security risk assessment	
5.	General Control Review	Perform general control review by documentation review, site visits, multi-level interviews, group discussions, surveys, etc.
6.	System Review	Perform a system review to identify the system vulnerabilities. Perform vulnerability scanning and penetration testing where applicable.
7.	Risk and Impact Analysis	Identify assets, threats, vulnerabilities and their impacts.
	Safeguards Analysis	Identify and select alternative safeguards.
	Delivery of Security Risk Assessment Report	Produce the assessment report to state the findings and recommendations.

Item	List of Activities	Description
	Presentation of Security Risk Assessment Results	Present the results and findings to management.
	Cybersecurity audit	
8.	Compliance Check	Conduct compliance checking by documentation review, site visits, multi-level interviews, and group discussion surveys against the organisation's security policy or policies that are relevant and within the scope of the cybersecurity audit.
	Delivery of Cybersecurity audit Report	Produce the cybersecurity audit report.
	Presentation of Security Audit Results	Present the results and findings to management.
9.	Safeguard Data and Results	After completion, all data collected and
	Follow-up Actions	
10.	Development of Follow-up Plan	Develop a follow-up plan on recommendations with an implementation schedule.
11.	Safeguard Implementation Review	Review the security status after implementation of safeguards.

Table 7: Examples of Common Activities

10. FOLLOW-UP OF SECURITY RISK ASSESSMENT AND AUDIT

10.1. Importance of Follow-Up

The benefit of security risk assessment and audit is not in the recommendations but in their effective implementation. When a recommendation is made, the management is responsible for implementing it. If management has decided not to implement a recommendation, they have to bear the associated risk.