CyberSecurity MALAYSIA

An agency under MOSTI

3rd Party Information Security Assessment Guideline

Nor'azuwa Muhamad Pahri
Noor Aida Idris

Securing Our Cyberspace

"But with that connection comes new threats: malicious hackers, criminals, industrial spies. These network predators regularly steal corporate assets and intellectual property, cause service breaks and system failures, sully corporate brands, and frighten customers."

(Bruce Schneier)

COPYRIGHT

REGISTERED OFFICE:

CyberSecurity Malaysia
Block A, Level 8, Mines Waterfront Business Park,
No 3, Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan, Selangor, Malaysia
Phone : +603 - 8992 6888
Fax : +603 - 8945 3205
http://www.cybersecurity.my

Printed in Malaysia

ACKNOWLEDGEMENT

CyberSecurity Malaysia wishes to thank the Panel of Reviewers who reviewed the drafts of this Guideline and contributed to its content.

External Reviewers

1. Abdul Aziz Hassan (Malayan Banking Berhad)
2. Abdul Rahman Mohamed (Malaysia Airlines)
3. Adnan Mohamad (Bank Negara Malaysia)
4. Azleyna Ariffin (Jaring Communications Sdn Bhd)
5. David Ng (Jaring Communications Sdn Bhd)
6. Dr Jamalul-lail Ab Manan (MIMOS Berhad)
7. Mahdi Mohd Ariffin (Bank Negara Malaysia)
8. Ong Ai Lin (PricewaterhouseCoopers)
9. Prof Dr Shahrin Sahib@Sahibuddin (Universiti Teknikal Malaysia Melaka)
10. Thaib Mustafa (Telekom Malaysia Berhad)
11. Ummi Kalsom Abdul Rahim (Securities Commission)
12. Yusfarizal Yusoff (Time dotCom Berhad)

Internal Reviewers

1. Adli Abd Wahid (Malaysian Computer Emergency Response Team)
2. Ida Rajemee Ramli (Security Management & Best Practices)
3. Maslina Daud (Security Management & Best Practices)
4. Nor Aza Ramli (Security Management & Best Practices)
5. Muralidharon (Security Management & Best Practices)
6. Raja Azrina Raja Othman (Chief Technology Officer)
7. Ruhama Mohd Zain (Security Assurance)
8. Suhairi Mohd Jawi@Said (Malaysian Computer Emergency Response Team)
9. Wan Roshaimi Wan Abdullah (Security Assurance)
10. Zahri Yunos (Chief Operating Officer)

Table of Contents

Executive Summary vi

1 Introduction 1
1.1 Objective 1
1.2 Scope 1
1.3 Target Audience 2
1.4 Document Structure 2

2 Terms & Definitions 3

3 Acronyms and Abbreviations 5

4 Overview 6
4.1 Information Security Assessment Process 6

5 Pre-Assessment 8
5.1 Roles & Responsibilities for Organisations 8
5.1.1 Develop Assessment Requirements 8
5.1.2 Plan and Allocate Resources 9
5.1.3 Evaluate 3rd Party Assessor 9
5.1.4 Develop Policies and Procedures 9
5.1.5 Prepare Documents and Records 9
5.1.6 Prepare Non-Disclosure Agreement 10
5.2 Roles & Responsibilities for 3rd Party Assessors 10
5.2.1 Develop Information Security Assessment Plan 10
5.2.2 Establish Team Members and Resources 10
5.2.3 Conduct Information Gathering 10

6 During Assessment 11
6.1 Roles & Responsibilities for Organisations 11
6.1.1 Ensure Key Personnel are Available 11
6.1.2 Hold Meetings 12
6.2 Roles & Responsibilities for 3rd Party Assessors 12
6.2.1 Conduct Assessment 12
6.2.2 Ensure Information and System Security 14
6.2.3 Produce Progress Report 14

7 Post Assessment 15
7.1 Roles & Responsibilities for Organisations 15
7.1.1 Review Assessment Report 15
7.1.2 Develop Remediation Action Plan 16
7.1.3 Information Security Requirements 16
7.2 Roles & Responsibilities for 3rd Party Assessors 16
7.2.1 Produce Assessment Report 16
7.2.2 Perform Clean-up 16

Appendix A Checklist of Organisation's Roles & Responsibilities I
Appendix B Checklist of 3rd Party Assessor's Roles & Responsibilities ... III
Appendix C Checklist for Security Controls V
References XIX

EXECUTIVE SUMMARY

Organisations today understand the need to periodically conduct information security assessment. The assessment is usually performed by an external service provider (i.e. 3rd party assessor) together with the organisations' team (e.g. internal audit department, risk management department, information technology department, etc). This assessment can assist organisations in understanding and staying alert for security risks and threats that may exist within their environment and even externally. These security risks, if left unmanaged, may present a negative impact to any organisation (e.g. financial, image, reputation, etc).

Hiring a competent 3rd party assessor leads to more cost-effective and impartial results from the assessment process. However, both organisations and 3rd party assessors need to prepare and understand their roles and responsibilities in the assessment. They need to cooperate to ensure the assessment is carried out smoothly and effectively.

This '3rd Party Information Security Assessment Guideline' provides guidance on roles and responsibilities that need to be carried out by both organisations and 3rd party assessors in information security assessment. The roles and responsibilities of both organisations and 3rd party assessors are discussed separately in each of the information security assessment process: pre-assessment, assessment, and the post-assessment phase.

In addition, three categories of security controls: Management, Technical and Operational are recommended for organisations in conducting the assessment. In the final section of this Guideline, a checklist for organisation's and 3rd party assessor's roles and responsibilities discussed ealier are provided for easy reference.

1

INTRODUCTION

Information security assessment is an activity when organisations assess the effectiveness of the security controls that they have implemented in their information systems. Results from the assessment provide organisations with the following:

- Evidence on the effectiveness of security controls implemented; and the effectiveness of the deployment.
- Information on the strengths and weaknesses of the organisations information systems.

Information security assessment can be carried out by a 3rd party assessor together with cooperation from organisations (system owners' information and system owners). The 3rd party assessor provides impartial results when conducting the information security assessment and may provide the best recommendations in mitigating the identified risks.

When hiring a 3rd party assessor to carry out the assessment, organisations need to ensure that the confidentiality, integrity and availability of the information at hand is preserved during the assessment.

Prerequisite: It is essential for organisations to perform internal audit prior to engaging a 3rd party assessor to carry out the assessment.

1.1 OBJECTIVE

The 3rd Party Information Security Assessment Guideline provides recommendations on roles and responsibilities of both organisations and 3rd party assessors before, during and after the information security assessment that is to be conducted by a 3rd party assessor. It is imperative to note that this Guideline does not address the overall management of the information security assessment itself.

This Guideline provides recommendations and guidance only; as such there are no penalties imposed on organisations that do not follow them. It is not intended to replace any existing information security standards or guidelines produced by standards organisations or regulators.

The use of this Guideline can differ according to the size, nature and complexity of an organisation, as well as the objective and scope of the information security assessment to be carried out.

1.2 SCOPE

The Guideline focuses on roles and responsibilities for organisations and 3rd party assessors in the three phases of information security assessment.

- Pre-Assessment
- During-Assessment
- Post-Assessment

The roles and responsibilities recommended in this Guideline are directly related to information security only. The Guideline mainly uses ISO/IEC 27001:2005 for reference; other standards and guidelines can and may be used as and when necessary.

Furthermore, an organisation may have additional or specific roles and responsibilities that they need to carry out (e.g. banking industries have specific duties they need to perform and relevant Acts that they have to adhere to). These additional roles and responsibilities are not within the scope of this guideline.

1.3 TARGET AUDIENCE

This Guideline is recommended to the following audience:

- Organisations (e.g. public, private and Critical National Information Infrastructure (CNII) sectors), that wish to carry out information security assessments using the services of 3rd party assessors.
- 3rd party assessors who performs information security assessments for other organisations.
- Information security personnel who are responsible in monitoring information security assessments.
- Individuals who are an internal and/or external auditors, information security officers or security consultants who performs information security assessments.

1.4 DOCUMENT STRUCTURE

This Guideline is structured as follows:

- Section 1 introduces objective, scope, and the target audience of the Guideline.
- Section 2 defines Terms and Definitions used in the Guideline.
- Section 3 lists the Acronyms and Abbreviations used in the Guideline.
- Section 4 provides an overview and description of the Information Security Assessment Processes.
- Section 5 provides roles and responsibilities for organisations and 3rd party assessors in the 'Pre-assessment Phase'.
- Section 5 provides roles and responsibilities for organisations and 3rd party assessors during the 'Assessment Phase'.
- Section 6 provides roles and responsibilities for organisations and 3rd party assessors in the 'Post-assessment Phase'.
- Appendix A provides a checklist of roles and responsibilities (discussed earlier) for organisations.
- Appendix A provides a checklist of roles and responsibilities (discussed earlier) for organisations.
- Appendix B provides a checklist of roles and responsibilities (discussed earlier) for 3rd party assessors.
- Appendix C provides a checklist of security controls requirements.

2

TERMS & DEFINITIONS

For the purpose of this guideline, the following terms and definitions apply.

2.1
3rd PARTY ASSESSOR
An external party, who is independent from the organisation who conducts information security assessment.

2.2
ASSET
Anything that has value to the organisation [1].

2.3
ATTACKER / CRACKER
Someone who breaks into someone else's computer system, often on a network; bypasses passwords or licenses in computer programs; or in other ways intentionally breaches computer security. The reason is for profit, malicious purpose, or because the challenge is there [2].

2.4
COMPUTING RELATED EQUIPMENT
Computer, network, telecommunications and peripheral equipments that support the information processing activities of an organisation. Examples of computing related equipments are computers, PDAs, thumbdrives, printers, video cameras, game consoles and multimedia devices.

2.5
FIREWALL
A firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks. The term also implies the security policy that is used with the programs [3].

2.6
INFORMATION SECURITY
Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved [4].

2.7
INFORMATION SECURITY ASSESSMENT
The testing and/or evaluation of the management, operational and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system [5].

1 ISO/IEC 27001:2005 – Information Security Management Systems
2 http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211852,00.html
3 http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212125,00.html
4 ISO/IEC 27001:2005 – Information Security Management Systems
5 NISTIR 7328 Security Assessment Provider Requirements and Customer Responsibilities

2.8
INFORMATION AND COMMUNICATION TECHNOLOGIES (ICT) SYSTEM

A set up consisting of hardware, software and firmware of computing related equipment and the people who use them. ICT system includes any computing related equipment or other electronic information handling systems and associated equipment or interconnected systems that are used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data/information.

2.9
MALICIOUS CODE

A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim [6].

2.10
ORGANISATION

Public or private registered entity that uses the services of a 3rd party assessor to conduct security assessments.

2.11
PATCH

A piece of software designed to update or fix problems with a computer program or its supporting data. This includes fixing bugs, replacing graphics and improving the usability or the performance of a particular machine.

2.12
THREAT

A probable impending danger or warning of impending danger which vulnerability may be exploited to cause harm to an organisation.

2.13
VIRTUAL PRIVATE NETWORK (VPN)

A means by which certain authorised individuals (such as remote employees) can gain secure access to an organisation's Intranet by means of extranet (a part of the internal network that is accessible via the Internet) [7].

2.14
VULNERABILITY

A weakness in an ICT system which allows an attacker to violate the integrity of the ICT system.

6 NIST SP800-83 Guide to Malware Incident Prevention and Handling
7 NIST SP 800-48 Wireless Network Security 802.11, Bluetooth and Handheld Devices

3

ACRONYMS AND ABBREVIATIONS

CISO	Chief Information Security Officer
CNII	Critical National Information Infrastructure
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardization
IT	Information Technology
NDA	Non Disclosure Agreement
SDLC	Software Development Life Cycle
UAT	User Acceptance Test
VPN	Virtual Private Network

4

OVERVIEW

The need for organisations to periodically conduct information security assessment of their environment is driven by two factors [8]:

- The increasing level of threats from internal users and external hackers who wish to gain unauthorised access to the organisation's confidential and/or sensitive information.
- The growing commercial imperatives for compliance with data security, accessibility and retention standards.

Benefits of information security assessments include:

1. Identify gaps in organisational security controls, policies and processes.
2. Discover the risks of external and internal security threats to organisations and provide detailed recommendations to mitigate them.
3. Improve organisations overall security posture and productivity based on recognised business needs.
4. Understand clearly the security issues and requirements within organisations information systems or applications before they are exploited.
5. Provide secure extension for business applications especially critical and core business applications.
6. Increase trust and confidence in the organisations systems and applications by ensuring the secure availability of their information systems or applications for their customers.

4.1 Information Security Assessment Process

Conducting an information security assessment requires a process that must be followed closely by organisations and 3rd party assessors. By following this process, organisations are able to determine the effectiveness of the implemented security controls.

The information security assessment process consists of three (3) phases, namely:

(a) Pre-Assessment

This is the first phase in information security assessment. It prepares organisations for the actual assessments conducted by 3rd party assessors. In this phase, organisations develop requirements for the assessment, plan and establish sufficient resources, and ensure all documents and records related to information security assessment are in order.

(b) During-Assessment

Once preparation for assessment is completed, 3rd party assessors together with organisation will conduct information security assessments as agreed in the scope of work and information security assessment plan. In this phase, organisations evaluate threats and vulnerabilities within the assets of the organisations information systems and to validate whether all implemented security controls are either adequate, completely secure or have met an acceptable level of risk.

(c) Post-Assessment

This is the last phase of information security assessment. In this phase, organisations receive assessment reports based on the conducted assessments. They should develop a remediable action plan and update their security requirements.

8 Security Audits – Eurokom Communication Solutions

The figure below describes an overall information security assessment process. It provides an overview of roles and responsibilities for organisations and 3rd party assessors in an information security assessment.

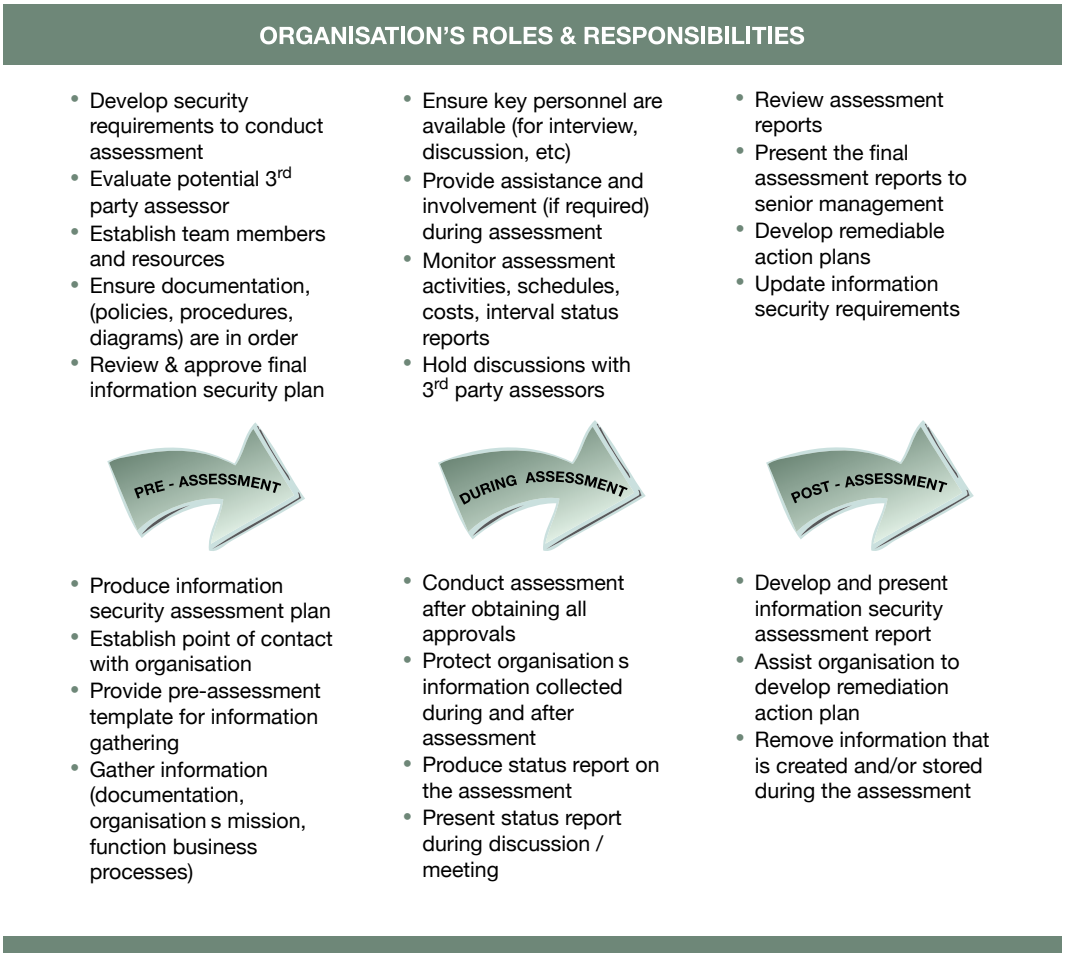

Figure 1: Roles and Responsibilities in an Information Security Assessment

The next 3 sections- section 4, 5 and 6 will provide further explanations on organisations and 3rd party assessors roles and responsibilities in pre-assessment, assessment and post-assessment phases.

5

PRE-ASSESSMENT

Pre-assessment phase is the first phase in information security assessment. It entails planning and preparation for information security assessments to be carried out by both organisations and 3rd party assessors.

The process flow of activities to be carried out during the pre-assessment phase with respect to roles and responsibilities of both organisations and 3rd party assessors is depicted in Diagram 1 below.

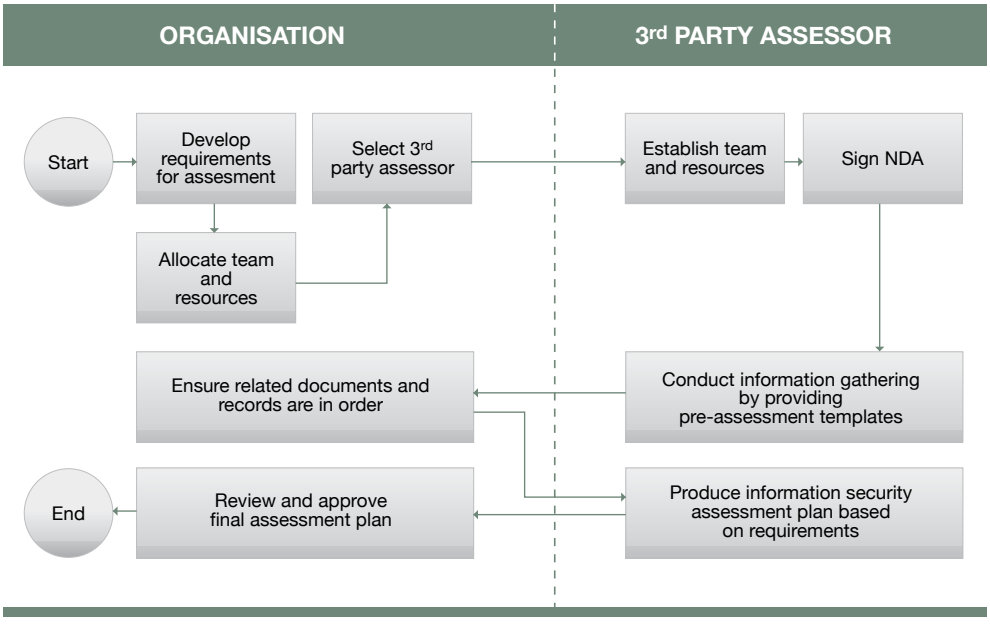

Diagram 1: Pre-assessment Phase

5.1 Roles & Responsibilities for Organisations

Roles and responsibilities for organisations in the pre-assessment phase should include, but not limited to, the following:

5.1.1 Develop Assessment Requirements

Organisations should plan and develop security requirements for information security assessment. The requirements should be in line with objective and scope of work of the assessment. The requirements should be also in line with the organisation's business functions, processes, compliance, regulatory, security policies and procedure requirements. Organisations should identify the areas to be assessed (e.g. network security architecture, web applications, physical security) and state the objectives to be achieved.

5.1.2 Plan and Allocate Resources

An organisation shall identify and allocate, based on the identified scope of work, a team and other resources (e.g. time, equipments, etc) for the assessment. The team should compromise representatives (and/or key personnel who have authority in decision making) from various departments within the organisation such as:

- Internal Audit Department
- Risk Management Department
- Human Resource Department
- Information Technology Department
- Administration Department
- Finance Department

The team should be notified on the impending information security assessment. A team leader shall be appointed to lead and manage the assessment as well as communicating with the 3rd party assessor's assessment team.

In planning for the assessment, organisations should also determine the suitable time (e.g. after UAT), duration (e.g. 5 days) and frequency (e.g. annually) for conducting the planned assessment.

5.1.3 Evaluate 3rd Party Assessor

Before acquiring services from a 3rd party assessor to conduct information security assessment, organisations should evaluate the agreed criterias and capabilities of the 3rd party assessor in a selection process.

Criteria in selecting a 3rd party assessor should include, but not limited, to the following:

1) 3rd party assessor is certified in Information Security Management System (in accordance to ISO/IEC 27001: 2005).
2) 3rd party assessor is willing to comply with the organisation's security policies & procedures.
3) 3rd party assessor has undergone and passed vetting procedure (for the employees who are involved in the assessment team), and registered with the Ministry of Finance (if applicable).
4) 3rd party assessor has certified personnel in information security area and forms a quality team that consists of subject matter experts in information security (organisations should check the accuracy of 3rd party assessor's qualifications).

5.1.4 Develop Policies and Procedures

Organisation should ensure relevant policies and procedures are in order prior to the assessment. The policies and procedures need to be developed and reviewed periodically to ensure their effectiveness. Examples of policies and procedures that should be developed are organisational information security policy, physical security policy, access control policy, information classification, labelling and handling policy, and network security policy.

5.1.5 Prepare Documents and Records

Organisations should ensure documents and records related to information security assessments are in order and readily accessible. A 3rd party assessor needs to evaluate and review various types of information security-related documents and records during the assessment. If all documentations are in place, the assessment can be conducted in a timely and effective manner. Examples of documents and records related to information security are:
Information system diagrams

- Internal audit reports
- Risk assessment reports
- Information security incident management response plans
- Business continuity plans

5.1.6 Prepare Non-Disclosure Agreement

Organisations should prepare a Non-Disclosure Agreement (NDA) for 3rd party assessors. They should ensure that the appointed 3rd party assessor signs the NDA before performing the assessment to ensure that the 3rd party assessor does not disclose any information relevant to the assessment activities. The NDA should be signed with the 3rd party assessor as well as with employees who are involved in the assessment.

5.2 Roles & Responsibilities for 3rd Party Assessors

Roles and responsibilities for 3rd party assessors in pre-assessment phase include, but not limited to, the following:

5.2.1 Develop Information Security Assessment Plan

The assessment plan is a plan that the 3rd party assessors should develop for conducting an information security assessment. The plan should be in line with an organisation's requirements. 3rd party assessors should develop this plan after understanding on the objective and scope of work for the assessment. The plan should cover a detailed roadmap of how 3rd party assessors are going to conduct the assessment based on the agreed scope of work and schedule.

Organisations meanwhile should review and approve the information security assessment plans before the assessment begins. This is important to ensure that the plan is consistent with the information security assessment objectives, scope of work, and timeline with regards to the resources allocated for the assessment.

5.2.2 Establish Team Members and Resources

3rd party assessors should provide sufficient resources in their assessment team to ensure the assessment can be completed in time. They should provide the team members background including their relevant knowledge, skills, experience and certifications (either professional certifications or product or technology specific certifications) on information security assessment methods and procedures. The knowledge requirements needed for assessments will vary based on the type of assessment and assessment environment. However, the selected assessment teams should have sufficient knowledge from experience or training in the following areas [9]:

- Information technology specific to the information system and the technologies functions
- Software specifications (e.g., functional specification, high-level design, low-level design, and source code)
- Information system architecture (i.e., components and their interactions)
- Testing and assessment tools
- Information technology security concepts, principles, analysis methods, and practices
- System Development Life Cycle (SDLC) phases and the security considerations in each phase
- Information security roles and responsibilities
- Security assessment reporting guidelines

In addition the team should establish an effective communication mechanism to minimise ambiguities or misunderstandings. Consistent communications should be carried out during weekly/bi-weekly/ monthly meetings throughout the three phases of assessment.

5.2.3 Conduct Information Gathering

3rd party assessors should provide pre-assessment template forms which will be used to gather information required in performing the assessment. The form is to be filled out by organisations. 3rd party assessor should acquire relevant documents and records from the organisations in question during this phase. They should understand them, as well as the organisations operations and structure of environment systems under the agreed scope of work prior to conducting the assessment.

9 NISTIR 7328 – Security Assessment Provider Requirements and Customer Responsibilities

6

DURING ASSESSMENT

In this phase, information security assessment is conducted based on the agreed scope of assessment and the information security assessment plan. The 3rd party assessors are responsible to perform the assessment; however organisations should oversee and/or assist 3rd party assessors (if required) with the assessment.

The process flow of activities to be carried out during the assessment phase with respect to roles and responsibilities of both organisations and 3rd party assessors is depicted in Diagram 2 below.

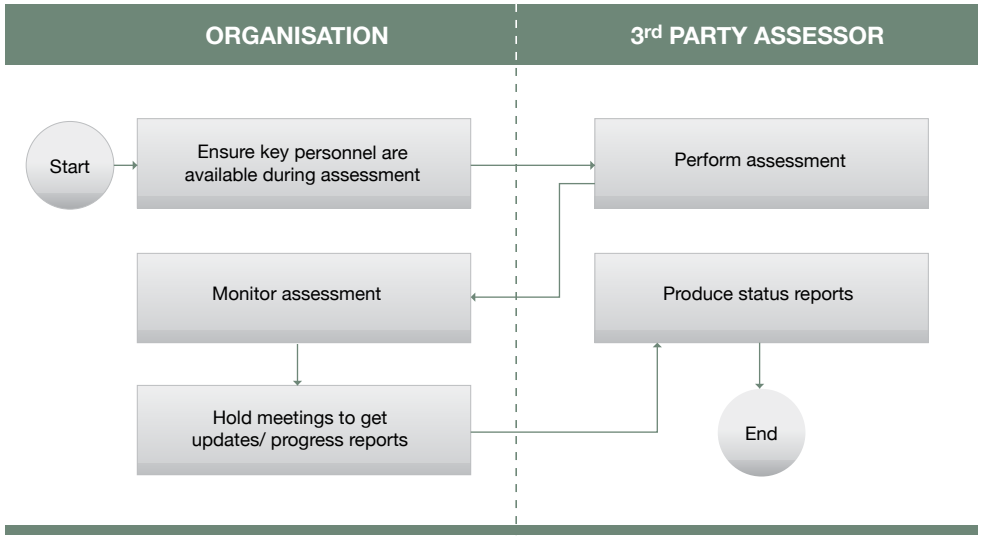

Diagram 2: During Assessment Phase

6.1 Roles and Responsibilities of Organisations

Roles and responsibilities for organisations during an assessment include, but not limited to, the following:

6.1.1 Ensure Key Personnel are Available

Organisations should ensure the availability of identified team members and they are able to provide assistance to 3rd party assessors during the assessment. 3rd party assessors may need to interview key personnel (who have decision-making authority) and/or information/system owners (other than identified team member) during the assessment. Hence, the team leader should identify and inform these individuals, the time and place as agreed with the 3rd party assessors.

In addition, organisations should be prepared should any administrative issues arise during the assessment. This includes providing an escort while 3rd party assessors conduct the assessment and appropriate office equipment to the 3rd party assessors (if they are working in the organisations premises).

6.1.2 Hold Meetings

Organisations should ensure the team to closely monitor the assessment activities. This monitoring shall include all aspects of activities listed in the information security assessment plan. In addition, the team leader (and/or with team members) should hold regular meetings to receive progress reports and resolve any issues pertaining to assessment activities. The minutes of meeting/discussion should be produced within three working (3) days after the meeting.

6.2 Roles & Responsibilities for 3rd Party Assessors

Roles and responsibilities for 3rd party assessors during assessment include, but are not limited, to the following:

6.2.1 Conduct Assessment

3rd party assessors should conduct the assessment based on the agreed scope of work and assessment plan. 3rd party assessors should only start the assessment after obtaining approvals from the relevant organisations.

It is recommended that 3rd party assessors conduct information security assessment which covers security controls in three aspects: management, technical and operational control. Security controls for organisations are essential to protect the confidentiality, integrity and availability of their information and information systems. These three controls need to be implemented together to ensure information security is preserved in three different perspectives listed below:

(a) Management Controls

Management controls focus on the management of risks and the management of information system security [10]. These should be taken and supported by the senior management of an organisation. Commitment from the senior management will ensure the controls are implemented effectively.

Management controls include risk management, policies and procedures, and internal audits:

(1) **Risk Assessment**

Risk assessment is a process of identifying, quantifying and prioritising risks against the set criteria for risk acceptance and objectives relevant to the organisation [11]. The information security risk assessment should have a clear defined scope in order to be effective and should include relationships with risk assessment in other areas (if any). Risk assessment should be conducted periodically or when there are any changes concerning an organisations information systems.

(2) **Policies and Procedures**

Policies and procedures related to information security should be developed, approved and communicated to all employees. These policies and procedures need to be reviewed periodically in ensuring their relevance and effectiveness.

(3) **Internal Audits**

Internal audits, sometimes called first-party audits, is a systematic, independent and documented process (usually) conducted by organisations themselves. This is done in the quest to obtain audit evidence and evaluating it objectively to determine the extent to which an audit criteria is fulfilled [12]. Internal audits should be planned (e.g. scope, frequency, methodology, criteria) and conducted periodically (or when organisations' information systems experience any major changes).

10 NIST FIPS Pub 200 Minimum Security Requirements for Federal Information and Information Systems
11 ISO/IEC 27001:2005 Information Security Management Systems - Requirements
12 ISO 19011:2002 Guidelines for Quality and/or Environmental Management Systems Auditing

(b) Technical Controls

Technical controls are security controls which are primarily implemented and executed through mechanisms contained in computing related equipments (hardware, software, or firmware components of the system) [13]. Organisations should implement technical controls via a comprehensive Defense-In-Depth (see Figure 2 below) approach which provide protection of multiple layers (i.e. network, communication, system/server, application, data).

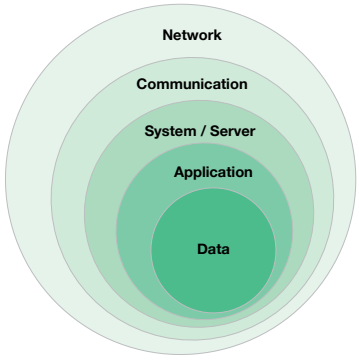

Figure 2: Five Layers in Defense-In-Depth approach

(1) **Network security**

Securing an organisations network layer should be done by securing the network architecture and design, securing network authentication and access control and securing all network devices.

(2) **Communication security**

Securing an organisations communication layer should be done by providing boundary protection (Internet-LAN-WAN-DMZ), providing remote, modem wireless and mobile protection, and providing malicious code protection.

(3) **System/server security**

Securing an organisations system/server should be done by securing all the operating systems, configuring identification and authentication, configuring and reviewing access controls, and protecting audit logs of the system/server.

(4) **Application security**

Securing an organisation's applications should be done by configuring identification and authentication, configuring and reviewing access control, ensuring information security during software development life cycle (SDLC), securing configurations and source codes of the application.

(5) **Database security**

Securing an organisations data should be done by configuring identification and authentication, configuring and reviewing access controls, and securing configurations of the database.

(c) Operational Controls

Operational controls are security controls that are primarily implemented and executed by people (as opposed to systems) [14]. These controls are controls that should be implemented by organisations continuously throughout the year. Organisations should implement operational controls which include, but not limited to, physical and environmental security, human resources security, information security incident management, and business continuity management.

13 NIST FIPS Pub 200 Minimum Security Requirements for Federal Information and Information Systems
14 NIST FIPS PUB 200 Minimum Security Requirements for Federal Information and Information Systems

(d) Physical and environmental security

Physical and environmental security helps organisations to prevent unauthorised physical access, damage and interference to an organisations' premises and information systems [16]. Organisations should implement physical and environmental security which consists of multiple controls such as biometric system, picture identification badges, gated facilities, guards and locked cabinets.

(e) Human resources security

Human resources security helps organisations to ensure that all employees, and external parties (e.g. contractors, third party users) understand their responsibilities (related to information security), aware of information security threats and are equipped to support organisational policies and procedures in reducing the risk of human error. This can be done by doing background verification of employees and external parties, providing job descriptions (i.e. define roles and responsibilities) of the employees, producing terms and conditions of employment to employees, and developing employees termination procedures.

(f) Information security incident management

The objective of managing information security incidents is to ensure a consistent and effective approach is applied when organisations face with such incidents. Organisations can implement this by establishing a procedure to ensure all information security incidents in organisations are reported, investigated and mitigated, and identifying mechanisms to monitor and learn from all the incidents.

(1) **Security training and awareness**

Security training and awareness aims to ensure organisations employees are competent to carry out required information security tasks associated with their jobs. Organisations should conduct regular security training and awareness to all employees and external parties (identified group and where relevant only).

(2) **Business continuity management**

Business continuity management is a management process that safeguards the interest of its key stakeholders, reputation, brand and value-creating activities by identifying potential impacts that threaten organisations and provides a framework for building resilience and capability for an effective response. To ensure the continuity and availability of critical business functions during a disaster, organisations should develop a business continuity management plan, and test the plan periodically.

Please refer to A*ppendix C: Security Controls Requirements* for a checklist of the three (management, technical and operational) security controls.

6.2.2 Ensure Information and System Security

3rd party assessors should be responsible to protect an organisations information collected before, during and after the information security assessment. This information includes the organisation's customers information and results of the assessment (i.e. vulnerabilities of the organisation's system or network).

To do this, 3rd party assessors should limit the sharing of confidential information to identified personnel. Those that need to know the information only (i.e. need-to-know basis). Another example is via understanding organisation's information classification, labelling and handling policies and procedures. In addition, they need to protect the organisations' systems and assets during the assessment. 3rd party assessors should obtain approval from organisations if any test (destructive or non-destructive) needs to be done on their systems and assets.

6.2.3 Produce Progress Report

3rd party assessors should produce progress reports periodically or at planned interval times as agreed by organisations. In the report, they should highlight issues related to the assessment and compile their findings. They should also recommend specific actions (if any) in the reports. These reports can be presented to the organisations' team during discussions and/or meetings.

16 MS 1970:2007 Business Continuity Management - Framework

7

POST ASSESSMENT

The post-assessment phase produces assessment reports by incorporating results of the assessment activities with information provided during the pre-assessment phase. This report will be reviewed the organisation's team members prior to it being presented to the senior management. Based on the report, the organisation as a whole would then need to make remediable action plans to mitigate the identified risks and vulnerabilities identified during the assessment.

The process flow of activities to be carried out in the post-assessment phase with respect to roles and responsibilities of both organisations and 3rd party assessors is depicted in Diagram 3 below.

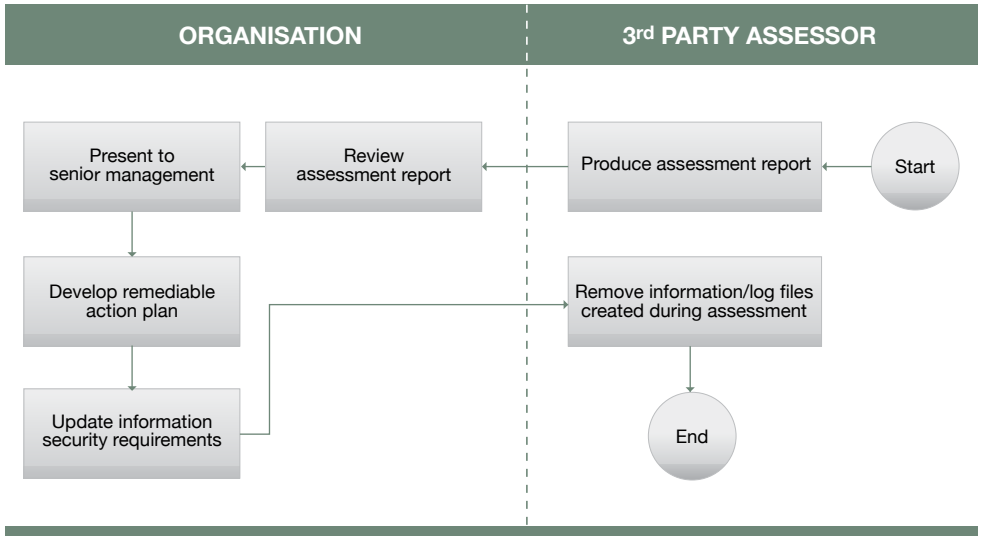

Diagram 3: Post-Assessment Phase

7.1 Roles & Responsibilities for Organisations

Roles and responsibilities for organisations in post-assessment phase include, but not limited, to the following:

7.1.1 Review Assessment Report

A security assessment report is a document that the 3rd party assessor team develops to report the results of the information security assessment. This report should be reviewed by organisations. Once the review is completed, it should be presented to the senior management. This is to ensure the findings of the assessment are made known to organisational officials and system owners so that appropriate steps can be planned to correct vulnerabilities and deficiencies identified during the assessment.

7.1.2 Develop Remediation Action Plan

Based on the information security assessment report, organisations should develop a remediable action plan. This plan is to ensure that each recommendation in the assessment report is addressed and rectified with specific, measurable, attainable, realistic, and tangible actions. It is recommended that any form of rectification to be carried out together with the vendor who supplied/supported the particular system, and advised by 3rd party assessors (if necessary).

7.1.3 Information Security Requirements

Information security requirements is a formal document that provides an overview of security requirements for organisations information systems. Requirements are usually derived from applicable laws, directives, policies, standards, instructions, regulations, procedures, or organisational mission/business case [17]. Organisation should update their information security requirements (including risk assessment plans) based on the assessment reports and remediable action plans.

7.2 Roles & Responsibilities for 3rd Party Assessors

Roles and responsibilities for 3rd party assessors in post-assessment phase include, but not limited, to the following:

7.2.1 Produce Assessment Report

3rd party assessors should incorporate findings from the assessments carried out and produce an information security assessment report. The report should contain the following [18]:

- Results and/or findings of the assessment (i.e., the determination of the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the intended security requirements for the system)
- Recommendations for correcting deficiencies in security controls and reducing or eliminating identified vulnerabilities (if any).

The report's format should include the following sections:

- Executive summary
- Objectives of assessment
- Scope of work
- Tools that have been used
- Dates and times of the actual on-site assessment on each area
- Every single output of assessment performed

7.2.2 Perform Clean-up

All testing data and log files that are created and/or stored on the organisations systems during the assessment should be removed. If this is for some reason not possible from a remote system, all these files (with their stated locations) should be mentioned in the assessment report so that organisations will be able to inform the respective system owners to remove them accordingly.

17 NISTIR 7328 – Security Assessment Provider Requirements and Customer Responsibilities
18 NISTIR 7328 – Security Assessment Provider Requirements and Customer Responsibilities

Appendix A

Checklist of Organisation's Roles & Responsibilities

The checklist below provides roles and responsibilities for organisations to use it to help them prepare for the information security assessment.

Table A1 below lists the roles and responsibilities in pre-assessment phase.

NO	ROLES & RESPONSIBILITIES	COMPLETED?		COMMENTS
		YES	NO	
1.	Establish the objectives and scope of work for information security assessment.			
2.	Allow sufficient time and resources for 3rd party assessors to gather requirements.			
3.	Allocate team members and resources (e.g. personnel, cost, time, etc) needed for the assessment (i.e. assisting 3rd party assessors).			
4.	Appoint a point-of-contact (or team leader) for managing communications with 3rd party assessors.			
5.	Evaluate criteria and capabilities of the 3rd party assessor.			
6.	Select an independent 3rd party assessor based on the evaluation.			
7.	Ensure all relevant policies, procedures, documents and records are in place and available for the assessment.			
8.	Fill-up pre-assessment templates provided by 3rd party assessor (to do information gathering).			
9.	Review the information security assessment plan provided by the 3rd party assessor and approve the plan prior to the assessment.			
10.	Ensure that a Non-Disclosure Agreement (NDA) has been signed by 3rd party assessor prior to the assessment.			

Table A1 : Pre-assessment Phase

Table A2 below lists the roles and responsibilities during the assessment.

NO	ROLES & RESPONSIBILITIES	COMPLETED?		COMMENTS
		YES	NO	
1.	Ensure key personnel are available during the assessment. Depending on the specific assessment, individuals in the following roles may be interviewed:			
(a)	Information system owners			
(b)	Information system security officer or CISO			
(c)	System/network administrator			
(d)	Database administrator			
(e)	Web administrator			
(f)	Executives that are responsible for specific security functions			
(g)	Head of departments/authorising officials			
(h)	Internal auditor			
(i)	Risk management personnel			
2.	Monitor the overall assessment process to ensure information security is intact.			
3.	Hold discussions/meetings with 3rd party assessor to receive updates and resolves any issues.			

Table A2 : Assessment Phase

Table A3 below lists the roles and responsibilities in post-assessment phase.

NO	ROLES & RESPONSIBILITIES	COMPLETED?		COMMENTS
		YES	NO	
1.	Review assessment reports produced by 3rd party assessors.			
2.	Present the final assessment report to senior management to ensure the findings are made known to organisational officials and system owners			
3.	Develop remediable action plans to address findings and recommendations that are highlighted in the assessment report.			
4.	Update information security requirements with findings from assessment reports and remediable action plans.			

Table A3: Post-assessment Phase

Appendix B

Checklist of 3rd Party Assessor's Roles & Responsibilities

The checklist for 3rd party assessor's roles and responsibilities can be used by both organisations and 3rd party assessors. It is a complete guide for organisations to evaluate a 3rd party assessor and also demonstrate to them on how to manage information security assessments. It is also to be used by 3rd party assessors to demonstrate their information security assessment practices to a particular organisation.

Table B1 below lists the roles and responsibilities in pre-assessment phase.

NO	ROLES & RESPONSIBILITIES	COMPLETED?		COMMENTS
		YES	NO	
1.	Allocate team members and sufficient resources to conduct the assessment.			
2.	Provide the team's background including relevant knowledge, skills, and certifications (either professional certifications or product or technology specific certifications) for verification.			
3.	Establish effective communication mechanism with organisation's point-of-contact (or team leader).			
4.	Understand scope of work for conducting information security assessment provided by organisation.			
5.	Understand organisation's structure of information system under scope of work of the information security assessment.			
6.	Participate in initial orientation meetings.			
7.	Acquire relevant documents and records for information gathering.			
8.	Provide pre-assessment templates to organisation in order to do information gathering.			
9.	Develop information security assessment plans and submit to organisation for approval.			

Table B1 : Pre-assessment Phase

Table B2 below lists the roles and responsibilities in assessment phase.

NO	ROLES & RESPONSIBILITIES	COMPLETED		COMMENTS
		YES	NO	
1.	Conduct assessment after obtaining approval.			
2.	Protect organisation's information collected during and after the information security assessment.			
3.	Produce status report periodically or at planned interval time as agreed with the organisation.			
4.	Present status report during discussion / meeting with the organisation's point-of-contact (or team member).			

Table B2 : Assessment Phase

Table B3 below lists the roles and responsibilities in post-assessment phase.

NO	ROLES & RESPONSIBILITIES	COMPLETED		COMMENTS
		YES	NO	
1.	Produce assessment reports that incorporate findings of the conducted assessment and recommendations for correcting current countermeasures (if any).			
2.	Assist organisation in producing remediable action plans.			
3.	Conduct clean-up by removing data/log files that is created and/or stored on the organisation's systems.			

Table B3 : Post-assessment Phase

Appendix C

Checklist for Security Controls

The checklist for security controls provides tasks for three major security controls stages: Management, Technical and Operational. These stages were discussed earlier in the Guideline. This checklist is a guide to 3rd party assessors when conducting an information security assessment for any organisation.

Table C1 below lists all tasks that should be executed when conducting information security assessment in management control

NO	SECURITY CONTROLS	COMPLETED?	VALIDATED?	COMMENTS
1	**Risk Assessment**			
(a)	Scope and strategy for risk assessment approach and methodology is defined and endorsed by organisation's senior management.			
(b)	Risk assessment is performed based on the defined scope and methodology.			
(c)	Risk assessment report is produced.			
(d)	Risk assessment report is presented to senior management.			
(e)	Risk assessment is performed periodically and/or when significant changes occur in the organisation's systems.			
2	**Policies & Procedures**			
(a)	Policies and procedures related to information security are developed.			
(b)	The policies and procedures are endorsed by senior management.			
(c)	The policies and procedures are communicated to all employees.			
(d)	The policies and procedures are reviewed periodically or at planned intervals.			
3	**Internal Audits**			
(a)	Internal audit requirements and activities (including checks on operational systems) are carefully planned.			
(b)	Internal audits are conducted periodically (e.g. annually, monthly, bi-monthly, weekly).			

Table C1: Security Controls Requirements in Management Control

Table C2 below lists all tasks that should be executed when conducting information security assessment in technical control.

NO	SECURITY CONTROLS	COMPLETED?	VALIDATED?	COMMENTS
1	**Network Security**			
(a)	A secure network architecture and design that includes network infrastructure facility drawings and topology maps is developed and documented.			
(b)	Components of the network architecture should include the followings:			
(c)	Internet/LAN/WAN, DMZ, server farm, Intranet and remote access/ external connection			
(d)	Internet critical services partition/ logical designs such as internal and external DNS and DHCP servers, email server, web application and other critical systems design			
(e)	Firewall designs, rules and policies			
(f)	Router, VLAN, core switch/switches/ hub configurations			
(g)	Host/network intrusion detection systems (IDS) and Intrusion prevention system (IPS) design and configurations			
(h)	Anti-virus system and update/patch management			
(i)	Backup system designs and procedure reviews			
(j)	Network management systems			
(k)	Centralised logging design review			
(l)	Security testing is conducted to verify the secure network architecture and design as deployed.			
2	**Authentication & Access Control**			
(a)	Procedure is developed for determining authorised access and resources.			
(b)	Access to network and network services are used via appropriate interfaces or specific equipments and locations.			

NO	SECURITY CONTROLS	COMPLETED?	VALIDATED?	COMMENTS
(c)	Authentication for remote users by using cryptographic based techniques, hardware tokens, or a challenge/response protocol (e.g. VPN, IPSec, dedicated private lines, dial-back modems, etc.) is provided.			
(d)	Logical and physical access is provided to authorised personnel only.			
(e)	Link network access rights to certain times of day or dates (if necessary) are provided.			
(f)	All communications devices are password-protected.			
(g)	All default manufacturers passwords have been changed.			
(h)	All mechanisms of authentications and access controls are enforced.			
3	**Network Devices**			
(a)	Internet connections and connections to other networks are secured via firewall.			
(b)	Remote locations, personal firewalls and fire wall appliances are used to secure connections to the Internet and Internet service providers.			
(c)	Firewalls rules and policy are reviewed periodically.			
(d)	A formal process should be used for managing the addition and deletion of firewall rules.			
(e)	Firewalls should be minimally installed or configured to perform the followings:			
(f)	Filter packets and protocols (with the characteristics of protocol), e.g., IP, ICMP, source and destination IP addresses, source and destination ports, (which identify the applications in use), interface of the firewall that the packet entered).			
(g)	Perform a thorough inspection of connections.			
(h)	Log traffic allowed and denied by the firewall.			

NO	SECURITY CONTROLS	COMPLETED?	VALIDATED?	COMMENTS
(i)	Perform proxy operations on selected applications (the proxy operations should, at a minimum, be operable on the content of SMTP, FTP, and HTTP protocol traffic).			
(j)	Provide authentication to users using a form of authentication that does not rely on static, reusable passwords that can be sniffed.			
(k)	Router configurations used at the Internet connection to create an external DMZ are reviewed.			
(l)	Routing controls deployment disallows computer connections and information flows breaching the access control policy.			
(m)	Network gateways that filter traffic by pre-defined tables or rules are reviewed.			
(n)	A VPN is recommended for remote users. (a dial-in server could be located behind a firewall, it is more secure to combine it with a VPN server located at the firewall so that remote connections can be securely authenticated and encrypted.			
(o)	Premise router interfaces that connect to the ISPs are configured with an access control list (ACL) that only permits packets with destination addresses within the site's address space.			
(p)	Workstation clients' real addresses are not revealed to the public by implementing Network Address Translation (NAT) on the firewall or the router.			
(q)	Passwords are not viewable when displaying the switch configuration.			
(r)	Switch allows only in-band management sessions from authorised IP addresses from the internal network.			
(s)	A dedicated management VLAN to keep management traffic separate from user data and data centre traffic.			

NO	SECURITY CONTROLS	COMPLETED?	VALIDATED?	COMMENTS
(t)	IDS/IPS is installed or configured to perform the followings:			
(u)	Information gathering capabilities			
(v)	Logging capabilities (ability to perform analysis, confirm the accuracy of alerts and correlate logged events with events recorded by other sources (e.g. other security controls, OS logs).			
(w)	Stored data and communications to IDS/IPS are protected.			
(x)	Authentication, access control and auditing features for IDS/IPS usage and administration are protected.			
(y)	Detection capabilities are released in response to major new threats.			
4	**Communication Security**			
(a)	Connections to the Internet, or other external networks or information systems, occur through managed interfaces (e.g. Secure Shell, SSH) consisting of appropriate boundary protection devices (e.g. proxies, gateways, routers, firewalls, guards, encrypted tunnels).			
(b)	Management access to a network device is secured using validated encryption (e.g. AES, 3DES, SSH or SSL).			
(c)	Publicly accessible information system components use separate sub-networks (using IP switching) with separate physical network interface.			
(d)	Separate logical network domains (i.e. each internal and external domain is protected by a defined security perimeter) are provided. (The segregation of networks into domains should be based on the access control policy and access control requirements).			
(e)	Number of access points to the information system is limited to allow for better monitoring of inbound and outbound network traffic.			

NO	SECURITY CONTROLS	COMPLETED?	VALIDATED?	COMMENTS
(f)	A managed interface (boundary protection devices in a n effective security architecture) is implemented with any external telecommunication service implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted.			
(g)	Monitoring system/NIDS is installed and configured such that it does not allow incoming network connections from any other system, except from Secure Shell (SSH) for specifically authorised inter-networking Operating System (IP) addresses (i.e. passively monitor network without accepting Telnet, FTP, email, other connections from other systems).			
(h)	All network management ports and services are disabled (except those needed to support the operational commitments of the site).			
5	**Remote, Modem, Wireless and Mobile Protection**			
(a)	Cryptography is provided to protect the confidentiality and integrity of remote access sessions.			
(b)	Remote level access for administrative, end-user and limited vendor access is defined.			
(c)	Two-factor authentication to access network is used by remote users.			
(d)	Remote access infrastructure's session connectivity and termination, user ID, assigned IP address, and success or failure of all session events are logged.			
(e)	Audit logs for any remote access server authentication mechanism periodically are reviewed and maintained.			
(f)	All modem phone lines to single-line operation are restricted if dial back services are not used.			
(g)	RAS/NAS device is located in a DMZ or screened subnet.			
(h)	VPN gateways on or outside of the firewall are terminated.			

NO	SECURITY CONTROLS	COMPLETED?	VALIDATED?	COMMENTS
(i)	Wireless LAN is configured with the followings:			
(j)	Encryption (e.g. WPA/WPA2)			
(k)	Authenticated with Service Set Identifier (SSID)			
(l)	MAC address filtering			
(m)	Access points protection			
(n)	Usage of mobile computing are allowed to access to organisation's systems in accordance with its security policies and procedures.			
(o)	Protection of mobile computing via physical protection, access controls, cryptographic techniques, back-ups, and anti-virus software.			
6	**Malicious Code Protection**			
(a)	Malicious code protection mechanisms at critical information system entry and exit points are provided.			
(b)	Malicious code protection mechanisms to detect and eradicate malicious code are provided.			
(c)	Latest virus definitions or new releases are provided.			
(d)	Malicious code protection software products from multiple vendors are provided.			
(e)	Usage restrictions and implementation guidance for mobile code technologies are reviewed.			
7	**System/server Security**			
(a)	Operating system is hardened or configured securely, patched to the latest version and opened necessary services and ports.			
(b)	Operating system hold only approved executable codes, and not development codes or compilers.			
(c)	Operating system is installed anti-virus with latest signatures and enabled real-time scanning.			
(d)	Separation of duties through assigned access authorisations.			

NO	SECURITY CONTROLS	COMPLETED?	VALIDATED?	COMMENTS
(e)	Further access to system is prevented by initiating a session lock after a defined time period of inactivity.			
(f)	A limit of consecutive invalid access attempts in enforced.			
(g)	Hard disk partition used for operating systems, applications and data files is separated.			
(h)	User functionality from information system management functionality is separated.			
(i)	Program source libraries should not be held in the operating systems.			
8	**Audit Logs**			
(a)	Audit logs recording user activities, exceptions and information security events are produced and kept.			
(b)	Audit records from multiple components throughout the system into a system-wide, time-correlated audit trail are compiled.			
(c)	Selection of events to be audited by individual components of the system is managed.			
(d)	Information system audit records and necessary actions taken are periodically reviewed/analysed.			
9	**Security Requirements Analysis and Configurations**			
(a)	Security requirements and specification for new information systems or enhancements to existing information systems are documented.			
(b)	Operating system is implemented and configured after extensive and successful testing.			
10	**Web Server Security**			
(a)	Web server's operating system is deployed and configured with the followings:			
(b)	Patch and upgrade the operating system.			
(c)	Remove or disable unnecessary services and applications.			

NO	SECURITY CONTROLS	COMPLETED?	VALIDATED?	COMMENTS
(d)	Configure operating system user authentication.			
(e)	Configure access control.			
(f)	Install and configure additional security control.			
(g)	Perform security testing of the operating system.			
(h)	Web server application is deployed and configured and with the followings:			
(i)	Install web server software either on a dedicated host or on a dedicated guest OS if virtualisation is being employed.			
(j)	Patch or upgrade web server application.			
(k)	Remove or disable all services installed by the Web server application but not required.			
(l)	Remove all manufacturers documentation from the server.			
(m)	Remove all example or test files from the server, including scripts and executable code.			
(n)	Apply appropriate security template or hardening script to server.			
(o)	Reconfigure HTTP service banner not to report Web server and OS type and version.			
(p)	Configure Web server user authentication and access controls.			
(q)	Configure web server resource/ access controls.			
(r)	Access controls for web server‘s OS enforce the followings:			
(s)	Service processes are configured to run as a user with a strictly limited set of privileges.			
(t)	Web content files can be read but not written by service processes.			
(u)	Only authorised process for Web server administration can write Web content files.			

NO	SECURITY CONTROLS	COMPLETED?	VALIDATED?	COMMENTS
(v)	Web server application can write Web server log files, but log files cannot be read by the Web server application.			
(w)	Security of web server application and web content is tested.			
(x)	Authentication and cryptography technologies are used appropriately to protect sensitive data.			
11	**Application Security**			
(a)	Identification is uniquely used and all types of users are defined accordingly.			
(b)	User identities are configured through passwords, tokens, and biometrics.			
12	**Access Control**			
(a)	User accounts for all application are reviewed periodically.			
(b)	Application enforced assigned authorisation for controlling access.			
13	**Information Security in SDLC**			
(a)	Security requirements are applied in each phase of SDLC.			
(b)	Initiative phase is reviewed, expected inputs/activities include:			
(c)	Identify security requirements and controls.			
(d)	Engineer security and develop controls.			
(e)	Design security architecture.			
(f)	Test development functional and security controls.			
(g)	Assess system risk.			
(h)	Develop security documents.			
(i)	Development phase is reviewed, expected inputs/activities include:			
(j)	Integrate systems.			
(k)	Test and evaluate security (final).			
(l)	Certify systems (optional).			

NO	SECURITY CONTROLS	COMPLETED?	VALIDATED?	COMMENTS
(m)	Implementation/Assessment phase is reviewed, expected inputs/activities include:			
(n)	IT deployment or connection.			
(o)	Disposal phase is reviewed, expected inputs/activities include:			
(p)	Management and controls of configurations.			
(q)	Continuous monitoring.			
(r)	Continuous assessments.			
14	**Secure Configurations**			
(a)	Input data is validated.			
(b)	Content of key fields or data files is reviewed periodically.			
(c)	Log of activities in data input process is provided.			
(d)	Control of internal processing failures.			
(e)	Common application vulnerabilities are tested.			
(f)	Output data is validated.			
15	**Secure Source Code & Encryption**			
(a)	Source code repositories with access control are implemented.			
(b)	Role based access are applied to access source code repositories and logs are reviewed periodically.			
(c)	Source code is developed in accordance with standard practice.			
(d)	Secure coding patterns embody code level examples and accompanying documentation that illustrate how to meet specific functional requirements.			
(e)	Performing code review before application is released.			
16	**Database Security**			
(a)	Identification is uniquely used and all types of users are identified.			
(b)	Authentication is reviewed and verified accounts are valid.			

NO	SECURITY CONTROLS	COMPLETED?	VALIDATED?	COMMENTS
17	**Access Control**			
(a)	User accounts for database are reviewed periodically.			
(b)	Assigned authorisations for controlling access to database in accordance with applicable policy.			
(c)	Permissions that control access to database software libraries are given to authorised personnel.			
18	**Secure Database Configurations**			
(a)	Database software is not unsupported software version.			
(b)	Database software and security are patched and tested.			
(c)	Configurations management procedures are in place.			
(d)	Capability to encrypt data and applications within data files.			
(e)	Network communications encryption options, data object encryption and encryption key management are reviewed.			
(f)	Mechanism to validate data before storage, maintained integrity of data relationships, recovered data to known reliable state, logged changes to data items, controlled simultaneous actions by different uses to same data.			
(g)	Audit trail retention policies are reviewed periodically.			
(h)	Data stored in database is secured (e.g. encryption).			

Table C2: Security Controls Requirements in Technical Control

Table C3 below lists all tasks that should be executed when conducting information security assessment in technical control.

NO	SECURITY CONTROLS	COMPLETED?	VALIDATED?	COMMENTS
1	**Physical & Environmental Protection**			
(a)	Policies and procedures relevant to physical and environmental protection are produced and endorsed by senior management.			
(b)	Awareness and dissemination of policies and procedures to employees are sufficient.			
(c)	Policies and procedures are reviewed periodically or at planned intervals.			
2	**Human Resources Security**			
(a)	Roles and responsibilities of employees and external parties (contractors and third party users) are defined.			
(b)	Background verification of employees and external parties (contractors and third party users) are performed.			
(c)	Terms and conditions of employment to employees and external parties (contractors and third party users) are provided.			
(d)	Termination procedures of employees is provided and closely followed.			
3	**Security Awareness & Training Programme**			
(a)	Security training and awareness programme is developed.			
(b)	Appropriate security training and awareness programme is conducted to employees and external parties (where relevant).			
4	**Incident Handling & Response Management**			
(a)	All information security incidents are reported.			
(b)	Mechanism to monitor and quantify security incidents is identified.			

NO	SECURITY CONTROLS	COMPLETED?	VALIDATED?	COMMENTS
5	**Business Continuity Management**			
(a)	Business continuity management plan is developed.			
(b)	The business continuity management plan is tested and maintained.			

Table C3: Security Controls Requirements in Operational Control

References

[1] *ISO/IEC 27001:2005, Information Technology – Security Techniques – Information Security Management Systems*, First Edition 2005-10-14.

[2] *ISO/IEC 27002:2005, Information Technology – Security Techniques – Code of Practice for Information Security Management*, First Edition 2005-06-15.

[3] *NIST IR 7328, Security Assessment Provider Requirements and Customer Responsibilities: Building a Security Assessment,* Initial Public Draft, September 2007.

[4] *NIST Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans*, Third Public Draft, June 2007.

[5] Open Information Systems Security Group (OISSG), *Information Systems Security Assessment Framework (ISSAF) Draft 0.2.1.A & Draft 0.2.1B*, May 1, 2006.

[6] Nelson, Karen. Dec 2002, *Security Assessment Guidelines for Financial Institutions*, http://www.sans.org/reading_room/whitepapers/auditing/993.php, retrieved on 4 February 2008.

[7] *Implementing a Successful Security Assessment Process*, https://www2.sans.org/reading_room/whitepapers/basics/450.php, retrieved on 11 February 2008.

[8] *Internet Security Systems Application Assessment*, http://documents.iss.net/literature/PS/Application_Assessment_datasheet.pdf,retrieved on 11 February 2008.

[9] *Delivering more secure services*, http://www.sun.com/service/security-assessment.com, retrieved on 11 February 2008.

[10] *Security Assessment*, http://www.security-assessment.com, retrieved on 11 February 2008.

[11] *Information Security Risk Assessment – Practices of Leading Organisations*,http://www.goa.gov/speacial.pubs/ai00033.pdf, retrieved on 11 February 2008.

CyberSecurity Malaysia
Block A, Level 8, Mines Waterfront Business Park
No. 3, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia
Tel : +603 - 8992 6888 Fax : +603 - 8945 3205
E-mail : info@cybersecurity.my
www.cybersecurity.my