CyberSecurity MALAYSIA

An agency under MOSTI

ISMS IMPLEMENTATION GUIDELINE

A PRACTICAL APPROACH

Registered Office:
CyberSecurity Malaysia
Level 5, Sapura@Mines
No. 7 Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia
Telephone: +603 – 8946 0888
Facsimile: +603 - 8946 0999
Website: http://www.cybersecurity.my

Printed in Malaysia

Acknowledgement

CyberSecurity Malaysia wishes to thank the following individuals who have contributed and/or reviewed this guideline.

External Contributors/Reviewers:

1. Lt. Col. Asmuni Yusof (Retired) (Malaysian Communications and Multimedia Commission (MCMC))
2. Azleyna Ariffin (JARING Communications Sdn Bhd)
3. Haliza Ibrahim (SIRIM Berhad)
4. Jamaludin Ibrahim (International Islamic University Malaysia (IIUM))
5. Noorhisam Rusmani (RHB Bank Berhad)
6. Nur Hidayah Abdullah (Malaysian Administrative Modernization and Management Planning Unit (MAMPU))
7. Assoc. Prof Dr. Omar Zakaria (National Defence University of Malaysia (UPNM))
8. Rafidah Abdul Hamid (Cyber Intelligence Sdn Bhd)
9. Raja Azrina Raja Othman (British Telecommunications Malaysia)
10. Rahayu Lop (Extol MSC Berhad)
11. Rodney Especkerman (Extol MSC Berhad)
12. Rozana Rusli (KPMG Management and Risk Consulting Sdn Bhd)
13. Sazlin Alias (SIRIM QAS International Sdn Bhd)
14. Shamsul Baharin Deraman (RHB Bank Berhad)
15. Yap Pei Shan (Price WaterhouseCoopers (PwC) Advisory Services Sdn Bhd)

Internal Contributors/Reviewers:

1. Abd Rouf Mohammed Sayuti
2. Ida Rajemee Ramlee
3. Maslina Daud
4. Noor Aida Idris
5. Norhazimah Abdul Malek
6. Nuzeita Hashim
7. Sabariah Ahmad
8. Siti Hajar Mohamad Ali
9. Syafiqa Anneisa Abdullah
10. Wan Nasra Wan Firuz

Table of Contents

List of Figures

List of Tables

Executive Summary

It is irrefutable that information is a valuable asset to an organisation regardless of the form i.e. on paper or digital. Many business operations depend highly on this information in their critical business processes. Thus, organisations need to protect such information appropriately.

Information should be protected to secure confidentiality, integrity and availability. In addition, other elements such as non-repudiation and authentication should also be considered. More organisations have come to realize the importance of protecting and securing their information.

Information Security Management System (ISMS) is a framework which enables organisations to manage security incidents holistically and systematically. The benefits of adopting and deploying this information security management framework are extensive. Its adoption and deployment is a tedious and lengthy process and the level of commitment is high, but the benefits, surpasses all that.

This guideline provides a holistic view on how to jumpstart the ISMS implementation. Organisations would be able to have a better understanding of ISMS implementation; thus easing the process and ensuring appropriate utilisation of resources whilst implementing ISMS.

1. Introduction

Information Security Management System (ISMS) is defined as that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. The management system, which includes organisational structures, policies, planning activities, responsibilities, practices, procedures, processes and resources; is important due to evolving risks and the need to be managed systematically.

As a whole, ISMS is a systematic approach in managing an organisation's information security. There are various mechanisms being practiced by different organisations in managing information security. Amongst which is through an information security management system based on ISO/IEC 27001:2005[1] Information Security Management Systems (ISMS) - Requirements.

This guideline should not be used as the sole reference when implementing ISMS; other relevant standards and/or guidelines should also be referred to, to complement information shared in this guideline.

NOTE: *This guideline makes reference to various relevant standards. For dated references made to standards e.g. ISO/IEC 27001:2005 ISMS - Requirements, only the edition cited i.e. 2005 applies. For undated references, e.g. ISO/IEC 27001 ISMS – Requirements, the latest edition of the referenced document (including any amendments) applies.*

1.1 Objectives

The objectives of this guideline are as follows:

a) To provide a holistic view and practical guidance of the processes in preparation for ISMS implementation based on ISO/IEC 27001:2005 ISMS - Requirements;
b) To provide guidance that are aligned with the requirements specified in ISO/IEC DIS 27001:2012 ISMS - Requirements[2] ; and
c) To equip all types of organisations with valuable information in implementing ISMS, with only minimal guidance from external parties.

1.2 Scope

This guideline takes the form of explanations of the following processes that are required for ISMS implementation:

a) Pre-implementation process
b) Documentations
c) Risk Assessment
d) Leadership and Support
e) Review and Monitor
f) Maintain and Improve

NOTE: *Certain processes from (a) to (f) can occur simultaneously depending on the organisation's scale and complexity.*

This guideline also describes the processes involved regarding ISMS certification for organisations intending to pursue the stated certification.

[1] ISO/IEC 27001:2005 is an international standard published by International Organisation for Standardization. The standard specifies requirements of an Information Security Management System (ISMS) that an organisation can develop and operate to protect its information assets and manage its information security risks.

[2] ISO/IEC DIS 27001:2012 is published as a Draft of International Standard in 2012. This standard is expected to be published as an International Standard in 2013 (at the time of the publication of this guideline).

The implementation of controls that are described in ISO/IEC 27002:2005 Information Technology - Security Techniques - Code of practice for information security management will not be covered in this guideline.

1.3 Target Audience

The targeted audience includes public and private sectors, Critical National Information Infrastructure (CNII) agencies and Small Medium Enterprises (SMEs) that intend to implement ISMS. For organisations that have implemented and wish to continuously manage and improve the ISMS, this guideline can be used as a reference for the betterment of their current implemented ISMS.

This guideline is targeted for all categories and levels of personnel in an organisation. However, it is highly recommended to be referred to by the personnel who possesses the following roles:

a) Management team that has the authority to decide, approve and endorse ISMS implementation activities. Refer to 3.5.1 and 3.5.2 for details of management team.
b) ISMS Lead Team, that drives, manages and monitors the progress of ISMS implementation activities in an organisation. Refer to 3.5.3 for details of ISMS Lead Team.
c) ISMS Implementation Team that executes the task of ISMS activities. Refer to 3.5.4 for details of ISMS Implementation Team.

1.4 Justifications for ISMS Implementation

When organisations initiate ISMS implementation, the top management will usually ask why and what are the benefits of implementing ISMS. While the justifications for implementing ISMS will vary from one organisation to another, Table 1 may provide the necessary insights.

Table 1: Examples Justifying the Initiation of an ISMS Implementation

No	Questions
1	Does your organisation own assets which are important to your business and/or service; and that any significant damage to these assets may cause serious ramifications to your organisation?
2	Are your organisation's assets (including personnel) appropriately protected in terms of loss of confidentiality, integrity and/or availability?
3	Has your organisation experienced recurring information security incidents?
4	Has the known threat (e.g. natural disaster, accidental or malicious intent) that affects your organisation been managed systematically?
5	Are there any relevant statutory and/or regulatory requirements, or contractual obligations, that apply to your organisation? ***NOTE:*** *Also to consider requirements from industries verticals as well as federal and state*
6	Has your organisation implemented any management of information security in addressing known and unknown information security risks?

No	Questions
7	Does your organisation own information infrastructure(s) which is (are) very important to the nation where significant disruption or destruction would have a devastating impact on any of the following? Consider the following impacts: • National **S**ecurity and Defence • National **E**conomic Strength • National **I**mage • Government Capabilities to Function or • Public **H**ealth and Safety ***NOTE:*** *From here onwards, the five impacts are referred to as "SEIGH".*
8	Has your organisation been identified by your regulator/sector as an organisation that is prone to high risks in which these risks should be managed?

NOTE: *The Malaysian government has initiated several initiatives for ISMS to be implemented. For example:*

- *A cabinet directive was issued on 24th February 2010 for ISMS to be implemented in Critical National Information Infrastructure (CNII) agencies/ organisations (referring to Memorandum No. MOSTI(R)/ICT/PSK-1/67 Jilid from Ministry of Science, Technology and Innovation (MOSTI)).*
- *NSC Directive No. 24 that was issued in 2012 by the National Security Council (NSC) which states that all CNII agencies/organisations are required to implement ISMS as part of the National Cyber Crisis Management Framework.*

1.5 Benefits of ISMS Implementation

By implementing ISMS, organisations should be able to:

a) improve overall governance structure in managing information security in the organisation;
b) achieve greater assurance that information assets are adequately protected against threats on a continual basis;
c) maintain a structured and comprehensive framework for identifying and assessing information security risks, selecting and applying applicable controls, and measuring and improving their effectiveness;
d) improve control environment continuously; and
e) comply with legal and regulatory requirements

1.6 Critical Success Factors for ISMS Implementation

The justifications and benefits of ISMS implementation have been explained. Organisations should be aware of several critical success factors that are vital when implementing ISMS. To ensure an effective and successful ISMS implementation, organisations should consider the following, in no particular order:

a) Commitment and support from the top management should be obtained prior to implementation and continuously throughout the implementation.
b) ISMS implementation should be aligned to the organisation's strategy and business objectives and requirements, and is an integral part of the overall management of the organisation related to and reflecting the organisation's approach to information security risk management.

c) Information security policies and procedures are being communicated promptly to all levels of personnel, from management to the front desk to ensure no misunderstanding and lack of information amongst the personnel.
d) Activities designed for ISMS are supported with various creative mechanisms and approaches so that 'willingness to change' is visible and accepted by all levels of personnel.
e) Personnel who are involved in ISMS implementation should be equipped with relevant competencies and skills.
f) Awareness programmes to all relevant personnel and entities are being held consistently and continuously to create a security culture where they fully understand their security roles and responsibilities.
g) Active monitoring and continuous improvements are crucial to ensure that risks and/or incidents are dealt with promptly; as well as to ensure that all necessary tasks are performed without delay.

2. Terms and Definitions

For the purpose of this document, the following terms and definitions apply:

Asset
Anything that has value to the organisation

NOTE: *There are many types of assets, including:*
a) Information;
b) Software, such as a computer programme;
c) Physical, such as a computer;
d) Services;
e) People, and their qualifications, skills, and experience; and
f) Intangibles, such as reputation and image.
(ISO/IEC 27000:2012)

Auditee
Is an organisation (or parts of an organisation) that is being audited. Organisations can include companies, corporations, enterprises, firms, charities, associations and institutions. Organisations can be either incorporated or unincorporated and can be privately or publicly owned.
(ISO 19011:2011)

Availability
Property of being accessible and usable upon demand by an authorised entity.
(ISO/IEC 27000:2012)

Certification Body
Third party that assesses and certifies the ISMS of a client organisation with respect to published ISMS standards, and any supplementary documentation required under the system.
(ISO/IEC 27006:2011)

Confidentiality
Property that information is not made available or disclosed to unauthorised individuals, entities, or processes
(ISO/IEC 27000:2012)

Control
Means of managing risks, including policies, procedures, guidelines, practices or Organisational structures, which can be administrative, technical, management, or legal in nature.
(ISO/IEC 27000:2012)

Conformity
Fulfilment of a requirement.
[ISO 9000:2005]

Corrective action
Action to eliminate the cause of a detected non-conformity or other undesirable situation.
(ISO/IEC 27000:2012)

Documented Information
Information required to be controlled and maintained by an organisation and the medium in which it is contained.

NOTE 1 to Entry: *Documented information can be in any format or media and from any source.*

NOTE 2 to Entry: *Documented information can refer to: the management system, including related processes; information created in order for the organisation to operate (documentation); evidence of results achieved (records);*
(ISO/IEC DIS 27001:2012)

Guideline
Recommendation of what is expected to be done to achieve an objective.
(ISO/IEC 27000:2012)

Impact
Adverse change to the level of business objectives achieved.
(ISO/IEC 27000:2012)

Information Security
Preservation of confidentiality, integrity and availability of information

NOTE: *In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can may also be involved.*
(ISO/IEC 27000:2012)

Information Security Management System (ISMS)
Part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.
(ISO/IEC 27000:2012)

Information Security Risk
Potential that a threat will exploit a vulnerability of an asset or group of assets and thereby cause harm to the organisation.
(ISO/IEC 27000:2012)

Integrity
Property of protecting the accuracy and completeness of assets.
(ISO/IEC 27000:2012)

Non-Conformity
Non-fulfilment of a requirement.
[ISO 9000:2005]

Policy
Overall intention and direction as formally expressed by management.
(ISO/IEC 27000:2012)

Procedure
Specified ways to carry out an activity or a process.
(ISO/IEC 27000:2012)

Process
Set of interrelated or interacting activities which transforms inputs into outputs.
(ISO/IEC 27000:2012)

Reliability
Property of consistent intended behaviour and results.
(ISO/IEC 27000:2012)

Risk
Combination of the probability of an event and its consequence.
(ISO/IEC 27000:2012)

Risk Acceptance
Decision to accept a risk.
(ISO/IEC 27000:2012)

Risk Analysis
Systematic use of information to identify sources and to estimate risk.

NOTE: *Risk analysis provides a basis for risk evaluation, risk treatment and risk acceptance.*
(ISO/IEC 27000:2012)

Risk Assessment
Overall process of risk analysis and risk evaluation.
(ISO/IEC 27000:2012)

Risk Criteria
Terms of reference by which the significance of risk is assessed.
(ISO/IEC 27000:2012)

Risk Management
Coordinated activities to direct and control an organisation with regard to risk.

NOTE: *Risk management generally includes risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring and risk review.*
(ISO/IEC 27000:2012)

Risk Treatment
Process of selection and implementation of measures to modify risks.
(ISO/IEC 27000:2012)

Service
Service is always the result of an activity or interaction between a service supplier and a customer and can take many forms.

Service can be provided to support an organisation's own products, for a product supplied by a customer or involve the provision of an intangible thing to a customer (e.g. entertainment, transportation, or advisory)
(ISO 9000:2005)

Statement of Applicability
Documented statement describing the control objectives and controls that are relevant and applicable to the organisation's ISMS.
(ISO/IEC 27000:2012)

Threat
Potential cause of an unwanted incident, which may result in harm to a system or organisation.
(ISO/IEC 27000:2012)

Vulnerability
Weakness of an asset or control that can be exploited by a threat.
(ISO/IEC 27000:2012)

3. Abbreviated Terms

For the purpose of this document, the following abbreviated terms apply:

CB	Certification Body
CNII	Critical National Information Infrastructure
CISO	Chief Information Security Officer
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ISMS	Information Security Management System
IT	Information Technology
MOSTI	Ministry of Science, Technology and Innovation
NSC	National Security Council
RTP	Risk Treatment Plan
SME	Small Medium Enterprise
SOA	Statement of Applicability

4. Pre-implementation Process

This chapter explains the pre-implementation process that is required for an ISMS implementation. Figure 1 describes the processes required for pre-implementation, which are crucial for the implementation of an ISMS.

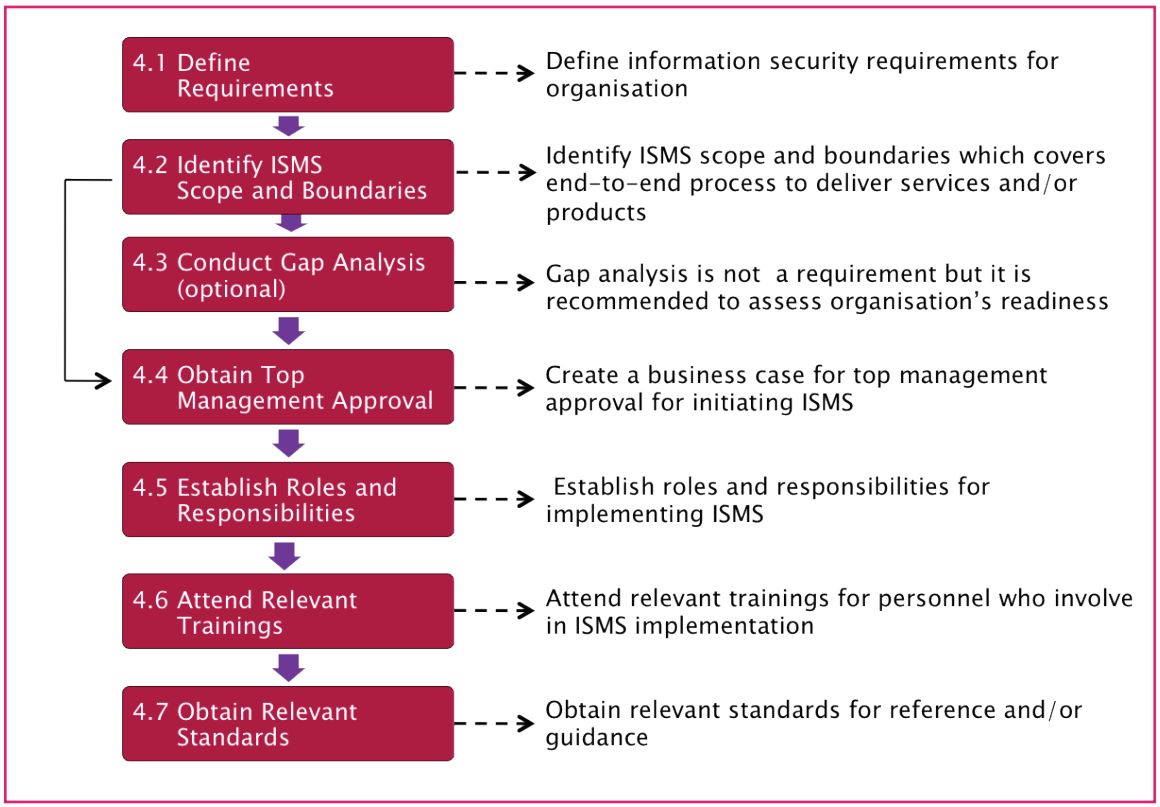

Figure 1: Pre-Implementation Process Flow

NOTE: *Organisations can execute the ISMS implementation process in a way that best suits their needs. In addition, the process flow may not necessarily be in the exact order as described in Figure 1.*

4.1 Define Information Security Requirements

Information security requirements are information security needs or expectations that are stated and are generally implied or obligatory to an organisation. These requirements are required because an organisation should understand its current context and consider external and internal issues that would affect the ISMS implementation. The external issues include business affiliations; constraints from third parties e.g. cloud computing providers, while internal issues may revolve around changes in management and business requirements.

There are several sources[3], which organisations should consider when defining security requirements. This includes:

a) the organisation's strategic objectives;
b) overall business requirements and critical services/functions;
c) overview of the existing management systems;
d) a list of relevant statutory and/or regulatory requirements, or contractual obligations, that apply to the organisation;

[3] ISO/IEC 27003:2010

e) organisation's risks; through risk assessment, risks towards the organisation's critical and valuable assets will be able to be determined; and
f) a particular set of principles, objectives and business requirements for information processing that an organisation has developed to support its operations.

Outcome of security requirements should be used as an input for defining the ISMS scope (refer to 4.2 Identify ISMS Scope and Boundaries).

4.2 Identify ISMS Scope and Boundaries

ISMS scope and boundaries determine the extent to which the ISMS is applied in an organisation. Identifying the right ISMS scope is crucial because it will assist organisations in meeting their security requirements and planning for ISMS implementation, for the organisation e.g. determining resources, timeline and budget required.

However, if the scope is not accurately defined, this will result in unnecessary wastage of resources (in terms of time, cost, and effort) because, when risk assessment exercises are conducted on different scopes, it will result in inaccurate identification of information security risks. Furthermore, if the ISMS scope is not aligned with the organisation's security requirements, the organisation may find that ISMS is a waste of time and resources; thus not valuing the benefits of implementing it.

The scope of ISMS can be defined in terms of the organisation as a whole, or parts of the organisation. The selected ISMS scope should be critical to the organisation in meeting its business objectives.

In general, the ISMS scope should cover the end-to-end process to deliver services and/or produce products. It should cover the complete elements of people, process and technology and relevant assets within the process (Refer to Appendix A - Examples of ISMS Scope Statements).

The ISMS scope should be derived from organisational known risks. For example, in a financial institution, the risks of unauthorised access of online transactions may give critical impact to its business operations. Thus, the ISMS scope for this financial institution can be defined as online transaction services.

Examples of questions that can guide organisations when defining the ISMS scope and boundaries:
a) Which service in your organisation will be covered by the ISMS?
b) How and why is the selected service critical to your organisation?
c) What are the characteristics of the selected service; i.e. business, the organisation, its locations, assets and technologies to be included in the ISMS?
d) Will you require external parties to abide by your ISMS?
e) Are there any interfaces or dependencies between activities performed by the organisation; and those performed by another? Should they be considered?
f) Are there any disruptions to the services that would have impact in terms of SEIGH?

The amount of effort required to implement ISMS is dependent upon the magnitude and complexity (among others) of the scope to which it is to be applied. Nevertheless, organisations should consider factors such as information security and business requirements, expectations from stakeholders and the expected resources when defining the ISMS scope.

To ensure that the ISMS is implemented effectively, it should be viewed as an enabler to achieve organisational business objectives.

In order to identify ISMS scope and boundaries, organisations should perform the following activities[4]:

a) consider the organisation's information security requirements which have been identified in 4.1 - Define Information Security Requirements;
b) consider any interfaces and dependencies between activities performed by the organisation, and those that are performed by other organisations;
c) consider critical services that can cause major impact to the organisation and/or nation arising from losses of confidentiality, integrity or availability;
d) define the organisational scope and boundaries;
e) define Information Communication Technology (ICT) scope and boundaries,
f) define physical scope and boundaries; and
g) integrate elementary scope and boundaries to obtain the ISMS scope and boundaries.

For clarity, organisations may seek the advice of a Certification Body (CB) on the proposed ISMS scope and boundaries, as and when the need arises.

Finally, ensure that the ISMS scope is documented and approved by the top management.

4.3 Conduct Gap Analysis (optional)

Conducting a gap analysis is not a requirement in ISO/IEC 27001; nevertheless it is highly recommended. Gap analysis can be conducted either at the early stage of the pre-implementation process or after the ISMS committee/team has been formed.

If the gap analysis is conducted at the early stage, organisations should be able to have an overview of their current readiness, and a rough estimation of timeline and resources required for ISMS implementation. On the other hand, conducting a gap analysis after the ISMS committee/team has been formed, will provide added advantage as the ISMS committee/team will be able to provide details of required tasks (e.g. based on controls in Annex A of ISO/IEC 27001), resulting in a better estimation of timeline and resources required.

The objectives of conducting a gap analysis are to:

a) assess the level of readiness for implementing ISMS;
b) reduce redundancy and/or conflict of tasks; and
c) estimate the timeline and resources for ISMS implementation

It is recommended to conduct a gap analysis based on the following:

a) mandatory requirements specified in ISO/IEC 27001;
b) controls in Annex A of ISO/IEC 27001; and
c) comparison with other management systems that are implemented by the organisation – several requirements in the management systems e.g. ISO 9001 Quality Management System are similar to the requirements in ISO/IEC 27001

The results of this gap analysis will be used to estimate the amount of time and resources in planning for the ISMS implementation. A sample of a gap analysis can be referred to via "ISO 27001 Security" portal.

4.4 Obtain Top Management Approval

Once the security requirements and objectives for ISMS implementation have been determined; ISMS scope and boundaries have been identified; and estimation of

[4] ISO/IEC 27003:2010

timeline and required resources have been produced based on the gap analysis; all of that will be used as input for developing a business case to the top management. The business case should be presented for approval to initiate the ISMS implementation. Language and style used in the business case should be suited for top management. Top management approval is crucial to ensure continuous commitment towards the implementation of ISMS (see also 7.1 Leadership and Management Commitment for further information).

In summary, the following subjects[5] should be covered when presenting a business case to the management:

a) establishment of the ISMS governing structure, which will have the primary roles and responsibilities in implementing the ISMS in an organisation. (see also 4.5 Establish Roles and Responsibilities);
b) goals and specific objectives of why the ISMS implementation is initiated (see also 1.4 Justifications for ISMS Implementation and 4.1 Define Information Security Requirements);
c) benefits of ISMS implementation to the organisation that includes monetary benefits, competitive advantage and confidence from stakeholders (see also 1.5 Benefits of ISMS Implementation);
d) preliminary scope of ISMS including business units/departments that may be affected during the ISMS implementation (see also 4.2 Identify ISMS Scope and Boundaries). ISMS preliminary scope has to be aligned with existing information security requirements (if any);
e) initial ISMS implementation plan which is derived from results of gap analysis. The plan should include the following:
    i) scope of work that is required for implementing ISMS based on the identified ISMS scope and boundaries (see also 4.3 Conduct Gap Analysis);
    ii) required resources that should include but not limited to applications, systems and technologies;
    iii) proposed personnel who are required not only for the initial ISMS implementation, but also throughout the whole process;
    iv) implementation considerations including existing information security controls that are in place or that may involve external parties;
    v) timeline with key milestones. The timeline will depend on factors such as the readiness of the organisation, competencies of personnel, ISMS scope and boundaries, and resources that are allocated for the implementation. Please refer to Appendix B – Common Timeline for ISMS Implementation and Certification for further information; and
    vi) expected costs; costs may include training that should be attended by relevant personnel, procuring related hardware and software; implementing controls, and hiring personnel and engaging external parties (if any).
f) critical success factors (CSFs) to implement ISMS (see 1.6 Critical Success Factors for further information); and
g) other factors affecting the organisation's ISMS (e.g. technology, business environment, risk tolerance, geographic location)

NOTE: *Details of ISMS scope, timeline and resources presented in a business case can be refined during the ISMS implementation.*

4.5 Establish Roles and Responsibilities

Following the approval from top management on initiation of the ISMS implementation, specific roles and responsibilities should be established for personnel who are involved in ISMS. The personnel should be aware of their responsibilities, and the authority that they possess within the scope of that responsibility.

[5] ISO/IEC 27003:2010

An ISMS governing structure should be established to oversee the overall ISMS implementation activities. The ISMS governing structure should consist of[6]:

- the organisation's management team (this team consists of top management and ISMS Steering Committee);
- ISMS Lead Team; and
- ISMS Implementation Team.

Figure 2 provides an illustration of an ISMS governing structure.

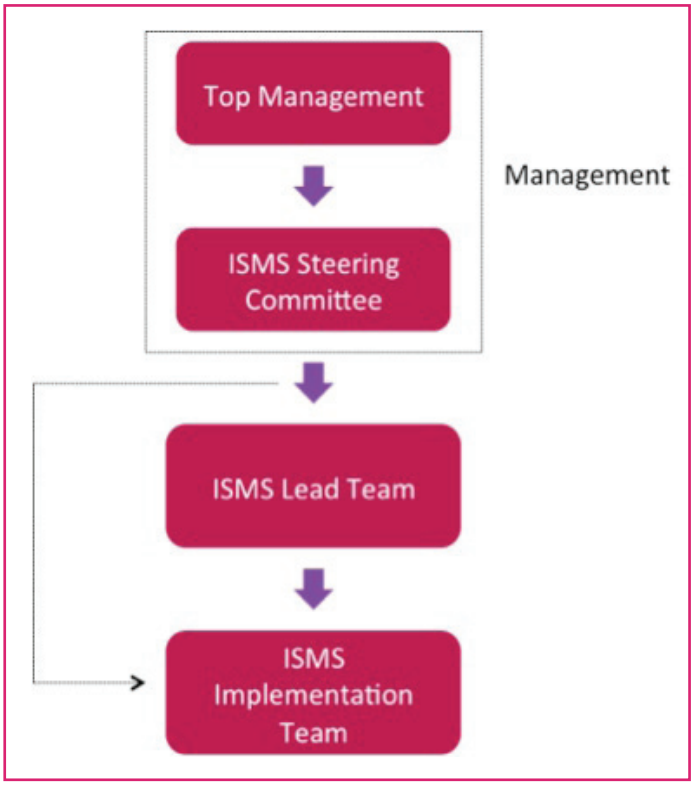

Figure 2: Illustration of ISMS governing structure
Source: Adapted from ISO/IEC 27003:2010

4.5.1 Roles and Responsibilities for Top Management

Top management is a person or group of people who directs and controls an organisation at the highest level subject to the organisation's structure. Top management should determine the organisation's visions, strategic decisions and coordinate activities to direct and control the organisation. The composition of top management may vary and is subject to the organisational chart. Top management may include positions of C-level (e.g. Chief Executive Officer (CEO) and Chief Operating Officer (COO), President and/or Vice President or similar.

Roles and responsibilities for top management in demonstrating leadership and commitment in respect to the ISMS includes[7]:

a) ensuring that information security polices and the information security objectives are established and compatible with the strategic direction of the organisation;
b) ensuring the integration of the ISMS requirements into the organisation's processes;

[6] Adapted from ISO/IEC 27003:2010

[7] ISO/IEC DIS 27001:2012

c) ensuring that the resources needed for the ISMS are available;
d) communicating the importance of effective information security management and conforming to the ISMS requirements;
e) ensuring that the ISMS achieves its intended outcome(s);
f) approving related information security policies, procedures, risks and residual risks;
g) directing and supporting persons to contribute to the effectiveness of the ISMS;
h) promoting continual improvement; thus it is crucial that the support and commitment from management is consistent and visible during the upcoming years in which ISMS is implemented and being maintained; and
i) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

4.5.2 Roles and Responsibilities for ISMS Steering Committee

ISMS Steering Committee has a leading role for the ISMS in an organisation and should be responsible for the organisational assets. The committee is the platform to discuss any issues related to ISMS and information security in general.

Depending on the structure of the organisation, it is acceptable for an organisation to leverage any existing committee that can serve the similar purpose as the ISMS Steering Committee.

Ideally, the ISMS Steering Committee should consist of:
a) Chairman - the chair for the committee should be appointed from the top management. The chairman's responsibility is to ensure that the ISMS objective is aligned with the organisation's strategic goal. For example, if the Chief Information Security Officer (CISO) has been appointed as the chairperson of ISMS Steering Committee, ideally the CISO should be in the top management and reports directly to the CEO of the organisation;
b) Line managers (e.g. organisation unit heads) – are responsible for each business unit and operations and to ensure that results of risk assessment activities are incorporated into their operational activities;
c) Process and/or asset owners – responsible for ensuring that appropriate controls are in place and assets are protected.

Roles and responsibilities of ISMS Steering Committee includes:
a) providing a clear direction on the organisation's ISMS strategies in managing information security;
b) ensuring that information security policies and objectives are implemented accordingly;
c) ensuring that adequate steps are taken regularly to improve the information security of the organisation;
d) conducting management review (refer to Chapter 8.6 Management Review for further information);
e) ensuring that continual improvements are addressed promptly and without delay; and
f) demonstrating commitment in supporting top management to achieve the organisation's strategic goals.

4.5.3 Roles and Responsibilities of ISMS Lead Team

The ISMS Lead Team, ideally a dedicated team, should be appointed by the top management. The team is responsible to plan, drive and perform the ISMS

implementation as directed by the ISMS Steering Committee. The team should possess in-depth knowledge and/or experience in information security, broad understanding of ISMS, implementation of ISMS and management of information security risks. The team should be aware of existing, and potential security controls, and work across departments to resolve conflicts with regards to ISMS.

Roles and responsibilities of ISMS Lead Team include:
a) planning, driving and managing ISMS related activities;
b) managing information security risks regularly; and
c) coordinating activities related to ISMS in general, ISMS Steering Committee and other information security programmes within the organisation.

4.5.4 Roles and Responsibilities of ISMS Implementation Team

The ISMS Implementation Team is responsible to perform ISMS activities planned by the ISMS Lead Team. Depending on the ISMS scope and organisation's structure, the ISMS Implementation Team should consist of personnel from departments such as[8]:
a) Risk Management – responsible for the enterprise risk management framework;
b) Human Resources (HR) – has overall responsibility for the personnel in an organisation, including recruiting, terminating and training requirements for the personnel;
c) Information Technology (IT) – responsible for the security of an organisation's IT systems and the overall IT resources required for ISMS implementation;
d) Finance and Accounting – responsible for overall budget management in ISMS implementation;
e) Building, Facilities, Administration – responsible for the physical security and general administration of the organisation's physical premise;
f) Audit – responsible for conducting ISMS audit. An auditor team leader is responsible for planning an ISMS audit programme.

NOTE: *The auditor and team leader can also be an internal auditor for the organisation*

Roles and responsibilities of ISMS Implementation Team include:
a) implementing information security policies and procedures (including security controls) accordingly; and
b) reporting and resolving any information security incidents promptly.

NOTE: *Depending on the organisational structure, ISMS Implementation Team occasionally needs to report directly to ISMS Steering Committee.*

Organisations should take note that organisational structure, resources and roles for information security may vary with the size, type and structure of the organisation. For example, in smaller organisations, the same person may carry out several roles. However, organisations should ensure that the roles are appointed appropriately to promote segregation of duties. In addition, roles that are required in ISMS are usually unique to an organisation and best to be determined by that particular organisation.

Upon approval from the top management, appointment letters for each personnel directly involved in ISMS should be produced, detailing the responsibilities for the personnel.

[8] ISO/IEC 27003:2010

Apart from the roles and responsibilities explained above, there are additional roles and responsibilities as stipulated in Appendix C – Additional Roles and Responsibilities in Information Security.

4.6 Attend Relevant Training

In order for the organisation to ensure that the personnel involved in ISMS implementation possesses the necessary capabilities and competencies, it is recommended for the personnel to attend relevant ISMS trainings.

The recommended trainings are as follows:

a) **ISMS Introduction Training**
This training is for beginners and introduces the requirements of ISMS. It is usually a prerequisite training before attending other advanced trainings such as ISMS Implementation Training, ISMS Internal Audit Training or ISMS Lead Auditor Training. This training is suitable for any kind of participants, and can be organized in-house at the organisation's premise.

b) **ISMS Implementation Training**
This training is designed for ISMS implementation team who needs to acquire specific knowledge and skills in implementing ISMS in their organisations. The training covers the requirements specified in ISO/IEC 27001 in depth. In addition, case studies and exercises are also provided to the participants as hands-on training.

c) **ISMS Audit Training**
This training is for personnel who are required to conduct ISMS audits. Those involved in the implementation process can also attend this training. Examples of audit trainings are internal audit training, Lead Auditor training and audit controls training. Through classroom, case studies, and open discussions, this training provides participants with a firm understanding of the concepts that lead to effective audits. Role-play and audit scenarios help participants to develop an understanding that will facilitate the implementation of good ISMS audit programme.

d) **Trainings derived from the Risk Assessment Exercise**
There are specific training requirements, which are derived as a result of a Risk Assessment exercise. Examples of these trainings are incident handling and management, digital forensics, business continuity management and network security trainings.

4.7 Obtain Relevant Standards

In order to implement ISMS, organisations should obtain relevant standards and guidelines for reference and guidance especially during the initial stages of ISMS implementation.

It is recommended to obtain a copy of the ISO/IEC 27001. This standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of an organisation's overall business risks. This is a certifiable standard, in contrast to ISO/IEC 27002, which is not a certifiable standard.

The ISO/IEC 27002 provides guidance for the selection, implementation and management of controls taking into consideration the organisation's information

security risk environment(s). It is recommended to obtain a copy of this standard as it provides implementation guidance for the controls, which are listed in Annex A of ISO/IEC 27001.

Please refer to Appendix D - Recommended Readings, for further information and Appendix E - Methods to Obtain Standard, for further information on how to obtain a copy of the standard.

5. Documentation

This chapter covers the process of managing the lifecycle of documented information, which is from the creation phase to the disposition phase. It describes the mandatory documented information that is required by ISMS and other mandatory documented information derived from a risk assessment exercise.

Documented information created through ISMS implementation are required to be maintained and kept for a period of time that can sufficiently verify the effectiveness of the controls implemented in ISMS. Organisations should refer to regulatory requirements and their organisational retention policy for the established retention period. For the purpose of ISMS certification/recertification, the documented information is to be retained for the next external audit. Please refer to Chapter 10.1 Preparation for ISMS Certification.

5.1 Control of Documented Information

Documented information should be controlled to ensure it is available and suitable for use, where and when it is needed; and it is adequately protected (e.g. from loss of confidentiality, integrity or availability). One of the mechanisms that can be implemented is in the form of a procedure.

Documented information should be controlled in terms of[9] :

a) **Creation and update**
When documented information needs to be created and updated, the following should be considered:
- identification and description (e.g. a title, date, author, version or reference number);
- format (e.g. language, software version, graphics) and media (e.g. paper, electronic);
- review and approval for suitability and adequacy;

b) **Distribution, access, retrieval and use**
Distribution, access, retrieval and usage of documented information is crucial to ensure that confidentiality is preserved where information is accessible only to those authorised to have access. It should also address the availability of the documented information where only authorised users can have access to information and associated assets when required. This can be achieved by having the following:
- Distribution details (e.g. recipient name, number of copies, location, receipt date);
- Access, retrieval and usage control (e.g. level of access, what to be accessed/ retrieved, access/retrieval time, duration of access/retrieval, method to be used and validity period, number of retrieval);
- If access, retrieval of usage is via system or online, audit trails or access logs need to be produced and kept;
- Regular review of given access rights (includes new request for access/ retrieval, termination or revoking an access).

c) **Storage and preservation**
In terms of storage and preservation of documented information, the following needs to be considered:
- Medium of storage (e.g. online, hardcopy or softcopy);
- Capacity of storage (e.g. how long data are able to be kept or archived to);
- Access rights for person to store documented information

[9] ISO/IEC DIS 27001:2012

d) **Control of changes**
Modification of documented information should be controlled in terms of the following:
- Modification details (e.g. name of person, date of changes, history logs, version numbers);
- Reason for the changes.

e) **Retention and Disposition**
Retention and disposition of documented information should be controlled in terms of the following:
- Retention period (e.g. how long data should be kept). The retention period is subject to organisation's regulatory and/or security requirement;
- Reasons for retention (e.g. why the need to keep the documented information. For some organisations, the reasons may be due to legal obligations;
- Disposition details (e.g. responsible person, date of disposal, which and why documented information need to be disposed)

5.2 Mandatory Documented Information

Mandatory documented information is documented information that should be produced, documented and maintained as proof of evidence that the ISMS has been implemented in an organisation. In addition, the mandatory documented information is necessary to avoid confusion among personnel and/or clarify processes that should be performed.

While ISO/IEC DIS 27001:2012 explicitly states several mandatory documented information, the extent of documented information for the ISMS may differ from one organisation to another due to several factors such as size of the organization, complexity of the ISMS being implemented, the determined ISMS scope and competencies of the personnel in the organisation. The mandatory documented information[10] is listed in Table 2:

Table 2: List of Mandatory Documented Information

Information	Description	Reference in ISO/IEC DIS 27001:2012
1. ISMS Scope	ISMS scope and boundaries that were identified should be documented and maintained. It should also be reviewed regularly. Any changes to the current ISMS scope and boundaries should be reflected in the documented information.	Clause 4.3

[10] ISO/IEC DIS 27001:2012

Information	Description	Reference in ISO/IEC DIS 27001:2012
2. Information Security Policy	Information Security Policy is the highest-level policy, which overarches other supporting policies for ISMS implementation. Guidance on the content of an information security policy document is provided in ISO/IEC 27002. In addition, Annex D of ISO/IEC 27003:2010 provides additional guidance on the structure of Information Security Policy. The Information Security Policy should be made available to the respective people within the organisation as well as other interested parties.	Clause 5.2 e)
3. Information security risk assessment process	The information security risk assessment process to be documented should cover the end-to-end process of risk assessment.	Clause 6.1.1
4. Information security risk treatment process	Information security risk treatment process should be documented in terms of selection of appropriate risk treatment options considering the risk assessment results.	Clause 6.1.2
5. Information security objectives	Information security objectives should be established at relevant levels and functions that are consistent with the information security policy. The objectives should be measurable, communicated and updated as and when required. These objectives should be retained and documented.	Clause 6.2
6. Evidence of competence	Organisations should determine the competencies required for the personnel responsible to perform tasks related to ISMS and controls that may affect the ISMS. Evidence of competence should be documented in terms of provision of trainings, actions taken to acquire the necessary competence and evaluation for the effectiveness of the actions taken.	Clause 7.2
7. Documented information to the necessary extent to meet the confidence that the processes have been carried out as planned	Operational processes and activities related to ISMS should be carried out regularly. Organisations should plan and implement the operational processes and activities to meet the security requirements and address risks and opportunities. Furthermore, organisations should implement plans to achieve the information security objectives. Any changes related to these operational processes and activities should be documented to provide evidence that the processes and activities have been carried out as planned.	Clause 8.1

Information	Description	Reference in ISO/IEC DIS 27001:2012
8. Results of the information security risk assessments	Information security risk assessments should be conducted at planned intervals or when there are changes that may introduce new threats within the organisation. The results of these risk assessment exercises should be documented and monitored regularly.	Clause 8.2
9. Statement of Applicability (SOA)	The SOA contains the necessary controls and justifications for inclusions or exclusions, whether they have been implemented or not implemented.	Clause 6.1.2 d)
10. Information security risk treatment plan (RTP)	A risk treatment plan (RTP) needs to be formulated based on the outcome of a risk assessment exercise. This plan needs to be documented and monitored to ensure that the risks are being treated accordingly.	Clause 6.1.2e
11. Results of the information security risk treatment	The results of the risk treatment exercise needs to be documented, which includes status of treating the risks. The documented results should be presented to top management for approval.	Clause 8.3
12. Evidence of monitoring and measuring results	Monitoring and measuring is an important process in ISMS. Any evidence that exists as a result of monitoring and measuring activities should be documented. The documented information should include what is to be monitored and measured (which can include information security processes and controls), the mechanisms to perform this; and also the personnel responsible to monitor, measure, analyse and evaluate the outcome of monitoring and measuring the ISMS.	Clause 9.1
13. Evidence of the audit programme and the audit results	Internal ISMS audit is another requirement in ISMS. Evidence that exists as a result of the internal ISMS audit should be kept and documented. The documented information may include (but not limited to) the audit programme, policies and procedures related to internal ISMS audit, audit reports and audit notes.	Clause 9.2
14. Evidence of the results of management reviews	The review of ISMS may be conducted via management review. Thus any evidence that may exist as a result of management review should be kept and documented. The documented information may include (but not limited to) minutes of meetings, memos, approval sheets and emails related to ISMS.	Clause 9.3

Information	Description	Reference in ISO/IEC DIS 27001:2012
15. Evidence of the nature of the non-conformities and any subsequent actions taken	Actions that have been taken to record non-conformities should also be kept and documented. The documented information may include (but not limited to) non-conformity policies, procedures and reports.	Clause 10.1 f)
16. Evidence of the results of any corrective action	Actions that have been taken to rectify non-conformities should also be kept and documented. The documented information may include (but not limited to) details of the corrective actions taken to resolve the non-conformities, status of the corrective actions and duration for the non-conformities to be resolved.	Clause 10.1 g)

NOTE: *The requirements for the information above may be covered by one or more documents.*

5.3 Other Mandatory Documented Information Derived From Risk Assessment

On top of the previous list on mandatory documented information, other mandatory documented information can also be determined by the organisation as being necessary for the effectiveness of the ISMS. These documented information should be derived from risk assessments and can be based on controls listed in Annex A of ISO/IEC 27001. Table 3 describes a list of security controls and the general description of possible documented information, which should be produced by organisations[11].

Table 3: List of Other Mandatory Documented Information Derived from Risk Assessments

Areas of Security Control	General Description
1. Organisation of information security	Procedures, measures and processes relating to how your organisation structures, forms and coordinates its personnel and related resources to achieve efficient and effective management of its security activities.
2. Asset management	Procedures and processes relating to achieving effective management of your organisational assets to ensure appropriate protection is given to the different types/classes and values of assets.
3. Human resources security	Policies, procedures, technical measures and processes relating to all the phases of personnel employment from recruitment and deployment to termination.
4. Communications and operations management	Policies and procedures for the protection, deployment, use and management of the communications and operational facilities of your organisation.

[11] Adapted from ISO/IEC 27001 for Small Businesses-Practical Advice

Areas of Security Control	General Description
5. Access controls	Policies, procedures, technical measures and processes relating to all forms of access control deployment, use and management encompassing access to your information, applications, services and operating systems.
6. Information systems acquisition, development and maintenance	Policies, procedures and processes relating to the acquisition, development and maintenance of information systems to ensure effective protection of your organisational assets.
7. Information security incident management	Procedures and processes relating to deployment, use and management of an information security incident programme.
8. Business continuity management	Plans, procedures and processes relating to the information security aspects of business continuity.
9. Compliance	Procedures, measures and processes relating to your compliance with legal, regulatory and contractual requirements, commitments and obligations.

6. Risk Assessment

Information security risk management is defined as a process to analyse what can happen and what are the possible consequences, before deciding what should be done and when, to reduce the risk to an acceptable level[12].

In ISMS, a risk management process is conducted for the purpose of preserving the confidentiality, integrity and availability of its information assets and to manage information security risks. Risk assessment, an important process in risk management, is the determination of the potential impact of all risks by assessing the likelihood that it will occur and the impact if it should occur[13].

NOTE: *ISO/IEC 27005:2011 - Information Security Risk Management - provides guidelines to organisations for managing information security risk. It supports the general concepts specified in ISO/IEC 27001:2005 and is designed to assist the satisfactory implementation of information security based on a risk management approach[14]. Organisations should obtain a copy of this standard for a detailed understanding on information security risk management (refer to Appendix E - Methods to Obtain Standard, for further information on how to obtain a copy of the standard).*

There are several processes that will be discussed in this chapter. Figure 3 describes the risk assessment process flow.

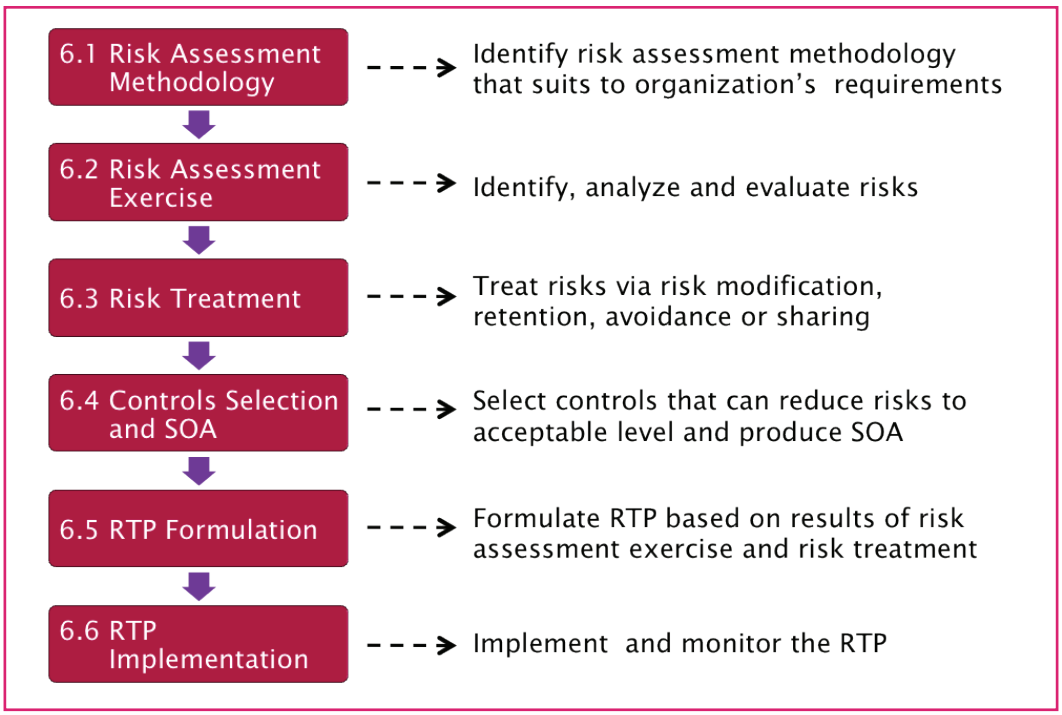

Figure 3: Risk Assessment Process Flow

[12] ISO/IEC 27005:2011

[13] ISO/IEC 27005:2011

[14] www.iso.org

6.1 Risk Assessment Methodology

Choosing a risk assessment methodology is one of the most important parts of establishing an ISMS. There is a need to define and document a risk assessment methodology.

Both ISO/IEC 27001:2005 and ISO/IEC DIS 27001:2012 do not specify any risk assessment methodology for organisations to adopt. However, both state that an organisation should apply a methodology that enables the following:

- The selected risk assessment methodology suits the identified business, information security, legal and regulatory requirements;
- The criteria for accepting risks are developed and acceptable levels of risk are identified and accepted by management;
- The information security risks are evaluated based on loss of confidentiality, integrity, and availability of assets; and
- The selected risk assessment methodology should ensure that repeated risk assessment exercises produce consistent, valid and comparable results.

NOTE: *There are various types of risk assessment methodologies that organisations can adopt depending on size, types and the ISMS scope. Organisations are free to adopt their existing risk assessments or develop new methodologies that suit their requirements and meets the four criteria's above.*

In general, a risk assessment methodology should include details for:

a) approach of the risk assessment, either qualitative or quantitative;
b) levels for the asset valuation in terms of loss of confidentiality, integrity and availability, for example a 3-tier valuation (high, medium, low); however, it is up to the organisation to determine the number of tiers;
c) levels for likelihood for combination of threats and vulnerabilities, for example a 3-tier valuation (high possibility, possible, rare); however, it is up to the organisation to determine the number of tiers;
d) levels for business impact in terms of loss of confidentiality, integrity and availability, for example a 3-tier valuation (high, medium, low); however, it is up to the organisation to determine the number of tiers;
e) risk levels, for example a 3-tier valuation (high, medium, low); however, it is up to the organisation to determine the number of tiers;
f) criteria for acceptable risk levels such as implementation of controls will not reduce the risk levels; and
g) criteria for acceptable residual risks such as cost of implementing controls are higher than the value of impact

NOTE: *Criteria for acceptable risk levels and residual risks are subjected to decisions made by the top management of an organisation.*

6.2 Risk Assessment Exercise

Risk assessment exercise is a systematic process for identifying and evaluating events (i.e. possible risks and opportunities) that could affect the achievement of objectives, positively or negatively. Such events can be identified in the external environment (e.g. economic trends, regulatory landscapes, and competition) and within an organisation's internal environment (e.g. people, process, and infrastructure). When these events intersect with an organisation's objectives - or can be predicted to do so - they become risks.

Risk assessment exercise is perceived as one of the most tedious processes encountered by organisations while implementing ISMS. Please refer to Appendix F – Examples of Challenges in Conducting Risk Assessment, which describes several challenges in the risk assessment exercise, as well as the recommended approaches to ensure a smooth process. The risk assessment exercise is illustrated in Figure 4.

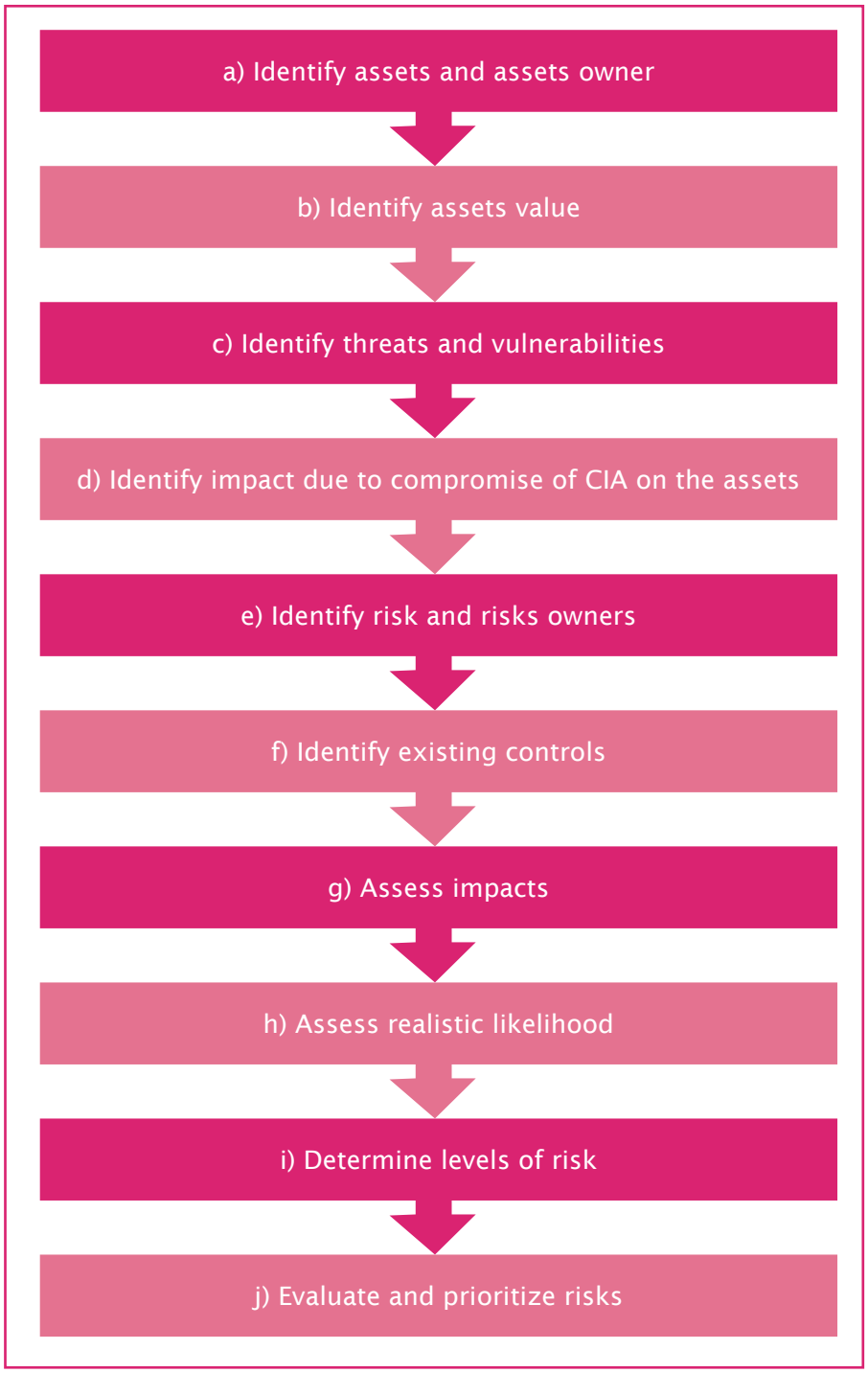

Figure 4: Risk Assessment Exercise Process Flow

Risk assessment exercise should be conducted based on risk methodology defined earlier.

The exercise should include the following:

a) **Identify assets and asset owners**
ISMS Implementation Team should identify assets in order to produce an inventory of assets that are to be protected. Asset identification should be performed at a detailed level that provides sufficient information for the risk assessment exercise. Asset owners should also be identified for each asset. The asset owner may not have property rights to the assigned asset, but possesses the responsibility for its production, development, maintenance, use and security.

More information on the identification of assets as related to information security can be referred to in Annex B of ISO/IEC 27005:2011.

b) **Identify value of assets**
The value of assets has then to be identified. That is, asset value in terms of its confidentiality, integrity and availability, which is based upon the risk methodology, defined earlier. This process should be discussed by a group of people that consists of, risk management personnel, asset owners and asset custodians. The asset owner is often the most suitable person to determine and assign the asset value. The identified asset value can be used in identifying impacts that losses of confidentiality, integrity and availability may have on the assets.

More information on the valuation of assets as related to information security can be referred to in Annex B of ISO/IEC 27005:2011.

c) **Identify threats and vulnerabilities**
Once assets and the owners have been identified, and the assets have been valued, there is then the need to identify the threats for each asset. It would be helpful to identify the threats generically and by type (e.g. unauthorised actions, physical damage, and technical failures) and then where appropriate, to identify individual threats within the generic class. Thus, no threat is overlooked. As an example, instead of identifying "earthquake" as a threat, it is more common to identify the threat as "natural disaster".

More information on the types of threats can be referred to in Annex C of ISO/IEC 27005:2011.

Next, for each identified threat, relevant vulnerabilities must be identified. The presence of any vulnerability will not cause harm until it is exploited by a threat.

Examples of vulnerabilities and methods for vulnerability assessment can be referred to in Annex D of ISO/IEC 27005:2011.

d) **Identify impacts**
Impacts can occur in the form of loss of effectiveness, adverse operating conditions, loss of business, reputation, damage etc. The identification of impacts helps to identify the damage to the organisation that could be caused by the combination of threats and vulnerabilities. Impacts may also affect one or more assets or a part of an asset.

Organisations should identify impacts that can arise due to the following[15]:

i. Investigation and repair time
ii. (Work) time loss
iii. Opportunity loss
iv. Health and Safety
v. Financial cost of specific skills to repair damages
vi. Image reputation and goodwill

e) **Identify risks and risk owners**
Then, risks will be identified after taking into consideration the identified threats and vulnerabilities as well as possible impacts on the assets. Risks that have been identified should be documented clearly and concisely. It is also useful if the risk can be categorised, for example, management, operational, reputation, governance, and project risks for easy segregation. For each risk, it is important to identify the risk owner. Nevertheless, some risks are shared by various risk owners due to the interdependencies of business processes and/or the nature of risks.

[15] ISO/IEC 27005:2011

f) **Identify existing controls**
Upon identification of risks, the ISMS implementation team should then identify the existing controls in place to gauge the real existing risks in the particular asset and to avoid similar controls being re-identified.

g) **Assess impacts**
Next, is to assess the potential impacts on losses of confidentiality, integrity and availability on the assets. Impacts can be assessed based on selected risk assessment methodologies. The assessed impacts should take into consideration the existing controls that are already in place.

h) **Assess realistic likelihoods**
After the impacts have been assessed, organisations should assess the realistic likelihoods of the occurrence of the identified risks. To estimate a particular likelihood, organisations should consider controls that are currently in place, which were identified earlier. In addition, organisations may need to refer to historical data, previous reports and/or interviews with asset owners as well as incident statistics (if any).

i) **Determine risk levels**
The levels involved for all risks should be identified. Organisations should be able to determine such levels based on the selected risk assessment methodology.

j) **Evaluate and prioritise risks**
Finally, organisations should then evaluate the risks and decide whether the risk is acceptable or requires treatment using the selected risk assessment methodology earlier. It should also prioritise the risks for risk treatment processes based on relevant risk criteria's that were established in the risk assessment methodologies.

For example, several factors should be considered in the risk evaluation process such as contractual, legal and regulatory requirements. If certain risks may cause losing a beneficial contract, then, treating this risk must be made a priority as opposed to other risks that may cause just minimal disruption to business operations.

6.3 Risk Treatment

There are four (4) options for treating risks[16]

NOTE: *The terms used in these risk treatment options may sometimes differ in other standards and guidelines, however the concept and general definition remain the same.*

The options for risk treatment are[17]:

a) **Risk modification**
For treating risk by modifying the risk, the level of risk should be managed by introducing, removing or altering controls so that the residual risk can be reassessed as being acceptable.

Risk modification (also known as risk reduction) is done by applying appropriate controls to meet the requirements identified by the risk assessment. The application of appropriate controls should take account of the risk acceptance criteria as well as legal, regulatory and contractual requirements. They should also take account of cost and timeframe for implementation of controls, or technical, environmental and cultural aspects.

[16] ISO/IEC 27005:2011

[17] ISO/IEC 27005:2011

b) **Risk retention**
If the level of risk meets the risk acceptance criteria, as defined in the risk methodology, there is no need for implementing additional controls and the risk can be retained. Risk retention (also known as risk acceptance) is selected by organisations when a decision has been made to accept the risk and to bear with the consequences if the risk occurs. Organisations should document these decisions. Thus, top management are aware of the risk and can knowingly accept it.

c) **Risk avoidance**
When the identified risks are considered too high, or the costs of implementing other risk treatment options exceeds the benefits of its implementation, a decision may be made to avoid the risk completely, by withdrawing from a planned or existing activity or set of activities, or changing the conditions under which the activity is operated. For example, for risks caused by nature, it may be more cost effective to physically move the information processing facilities to a place where the risk does not exist or is under control. However, consideration must be given to impacts and implications before opting for risk avoidance.

d) **Risk sharing**
Risk sharing (previously known as risk transfer) involves a decision to share certain risks with external parties. Risk sharing can create new risks or modify existing, identified risks. As such, additional risk treatment may be necessary. In addition, there is a need to analyse the costs of these risks, for example, costs that include external parties such as insurance companies, who will bear the consequences (generally, on monetary loss) if the risk materialises.

6.4 Controls Selection and Statement of Applicability (SOA)

Selection of controls should be based upon the results of a risk assessment exercise. Controls can be selected to treat one or many risks. Controls are unique for each organisation. Thus, a control that is selected by an organisation may not be applicable to other organisations.

Organisations should refer to Annex A of ISO/IEC 27001 when selecting controls. Controls are applied to:
- reduce risks to an acceptable level as defined in Chapter 6.1 - Risk Assessment Methodology;
- reduce the likelihood of threats or vulnerabilities that causes such risks;
- ensure the fulfilment of legal or business requirements;
- reduce the possible impact if the risk occurs; and
- detect unwanted security events or incidents, and aid to react and recover from them.

There are thirteen (13) domains as described in Annex A of ISO/IEC DIS 27001:2012:
[1] Information Security Policy
[2] Organisation of Information Security
[3] Human Resources Security
[4] Asset Management
[5] Logical Security / Access control
[6] Physical and Environmental Security
[7] Operations Security
[8] Communications Security
[9] Systems Acquisition, Development and Maintenance
[10] Supplier Relationships
[11] Information Security Incident Management
[12] Information Security Aspects of Business Continuity Management
[13] Compliance

Each domain contains a number of security categories within the domain; and each security category contains:

a) a control objective stating what is to be achieved and
b) one or more controls that can be applied to achieve the above control objective.

The list of Annex A of ISO/IEC 27001 is not exhaustive. Organisations are free to add new controls as required, or identify additional controls from any source, which are deemed necessary. Nevertheless, organisations are recommended to refer to the Annex A of ISO/IEC 27001 prior to looking at other sources. This is to ensure that no important control options are overlooked. Also, not all controls will be relevant to every situation; organisations should consider local environmental or technological constraints that may affect the selection of controls.

Statement of Applicability (SOA) is one of the mandatory documented information produced after the selection of controls (refer to item number 9 Statement of Applicability of Table 2: List of mandatory documented information in Chapter 5.2 - Mandatory Documented Information).

The SOA should consist of the following[18]:

- Controls and the associated control objectives that have been selected;
- Existing controls and controls that are to be implemented based on the risk assessment exercise mapped to the relevant references; and
- Justifications for exclusion of controls in Annex A of ISO/IEC 27001; for example, organisations that do not provide electronic commerce services. Therefore, controls on electronic commerce may not be suitable or applicable.

6.5 Risk Treatment Plan Formulation

Organisations should formulate an information security Risk Treatment Plan (RTP) after the risk assessment exercise. The RTP should provide details of how the organisation is responding to the identified risks. It should also outline how each risk will be managed and should include the controls that were selected earlier; but with other details such as who will be assigned with tasks to respond to the risk, timeline of the task as well as the status of each task.

The plan should be approved by top management (to ensure that they are aware of the risks, are responsible and will provide the necessary resources for treating such risks) and risk owners (to ensure that the risks are treated accordingly).

In addition, residual risks, which are risks that still exist after being treated, should also be accepted by both top management and risk owners. This is to ensure that top management is aware and is accountable for the residual risks that still exist.

[18] ISO/IEC DIS 27001:2012

6.6 Risk Treatment Plan Implementation

Once the RTP has been formulated and approved by top management, the plan should be implemented promptly. Status of the RTP implementation should be monitored consistently and results of the RTP is documented and presented to top management for approval.

If, for any reason, the RTP implementation has been delayed, reasons for the delay should also be documented and approved by top management. Any RTP that exceeds the approved timeline, a revised timeline should be produced and approved by the top management.

7. Leadership and Support

This chapter explains the leadership and commitment of the management, which, is crucial to ensure effective implementation of ISMS. In addition, it describes supporting needs in ISMS implementation such as required resources for ISMS implementation, ensuring awareness and competence of personnel who are directly involved in ISMS. Lastly, the chapter discusses the need for communicating relevant information with regards to ISMS to the appropriate personnel and/or external parties.

7.1 Leadership and Management Commitment

When ISMS is implemented, the involvement of top management is critical to ensure that the ISMS is implemented effectively and efficiently. The management should understand the actual requirements for the implementation and benefits of the ISMS.

Management commitment spearheads efforts to gain cooperation of personnel in implementing ISMS and would provide a clearer company-wide understanding of security expectations. Those expectations can be used as a baseline for continuous performance improvement. Continuous commitment should also include morale support and recognition that should be visible. Please refer to 4.5.1 - Roles and Responsibilities for Top Management and 4.5.2 - Roles and Responsibilities for ISMS Steering Committee, for further information on roles and responsibilities for management.

7.2 Provision of Resources

To successfully implement the ISMS, the top management should be committed to provide the necessary resources. The resources may include, but not limited to, money, time, expertise (people), technology and assets.

7.3 Competence and Awareness Programme

Competence and awareness programmes are important in ISMS. An organisation should determine the types of competence and awareness programmes in ISMS and information security in general, which are required by its personnel.

Training supports development of competence and it enables personnel to understand and acquire knowledge to perform their information security related roles. However, training is not the only element in establishing competence. It involves a combination of education, training and work experience. For certain roles, specific benchmarks should be defined to measure the competencies of personnel in performing their respective tasks.

Awareness programmes facilitates the promotion of a security programme, establishment of responsibilities, communication of policies and procedures and inculcation of a security culture among employees. Awareness programmes should be initiated prior to an ISMS kick-off to ensure that the relevant parties involved are provided with a clear understanding of stated objectives, thus minimising challenges during implementation. These awareness programmes should be conducted on an on-going basis to continuously educate personnel to stay alert, recognise security incidents and respond accordingly.

The competence and awareness programmes should be developed in accordance to different target audiences' e.g. top management, line managers, users and new employees. As an example, Table 4 below provides an illustration of an ISMS competence and awareness programmes and the targeted audience.

Table 4: Example of ISMS Competence and Awareness Programme

Name of Programme	Target Audience
ISMS awareness to management	Top management
ISMS Implementation Training	ISMS Lead Team, ISMS Implementation Team, ISMS Steering Committee, ISMS Internal Auditors
ISMS Auditor Training	ISMS Lead Team, ISMS Internal Auditors
Technical training for specific tasks	ISMS Lead Team, ISMS Implementation Team, Personnel who perform specific technical tasks e.g. network, digital forensics, incident handling, web development, etc.
General ISMS awareness	All personnel, third parties (vendor, consultant, etc)

The programme can be in any form of activity (such as classroom training, outdoor activities, posters, quizzes and emails) depending upon the resources and the target audience.

A general ISMS awareness programme should be conducted, at least once, prior to ISMS implementation. The frequency to conduct general ISMS awareness programmes varies and depends largely on the organisation and its available resources. Ideally, the general ISMS awareness programme may need to be conducted periodically at planned intervals (e.g. quarterly basis). It is also useful if the organisation includes the general ISMS awareness programme during induction programmes for new personnel.

7.4 Communication

Any information related to ISMS needs to be communicated to the personnel so that they are aware of any updates, activities and changes to existing policies and procedures. In addition, certain information related to ISMS may need to be communicated to external parties such as vendors or service providers. In general, organisations are required to[19]:

a) determine what information should be communicated;
b) specify when the information is to be communicated;
c) identify who the information should be communicated to

NOTE: *different audience may require different mechanism of communication;*

d) select an appropriate personnel (or department) to be responsible for execution of the communication; and
e) establish a communication process.

Organisations should determine the mechanism for the communication process, based on their requirements. Communication can be in various forms. It can be via electronic mediums (emails, online quizzes, etc), on paper (memos, letters, posters, etc) or verbally (meetings, awareness and training sessions). Organisations may also wish to organise outdoor activities such as treasure hunts or games as a means of communication.

[19] ISO/IEC DIS 27001:2012

8. Review and Monitor

This chapter explains the need for organisations to measure the effectiveness of the selected controls, conduct internal ISMS audit and undertake regular review of the effectiveness of the ISMS.

8.1 ISMS Measurement

There is a need for organisations to establish an ISMS measurement process to measure the effectiveness of ISMS and selected controls resulting from the risk assessment exercise. In addition, conducting the ISMS measurement helps to determine if the intended objectives of the controls' implementation are met.

8.1.1 Information Security Measurement Programme

One of the methods to establish ISMS measurement is via development of an information security measurement programme[20]. Organisations may refer to ISO/IEC 27004:2009 Information Security Management – Measurement - for further information on the programme.

The information security measurement programme should directly relate to the operation of the ISMS, other measures, as well as organisations' business processes. It should ensure that an organisation effectively achieves objectives and repeatable measurements and provides measurement results for relevant stakeholders, to identify needs for improving the implemented ISMS, including its scope, policies, objectives, controls, processes and procedures.

The measurement programme should cover the following[21]:

a) Measurement development (including calendar plan to perform measurement activities);
b) Measurement operations;
c) Data analysis and measurement results reporting; and
d) Information security measurement programme evaluation and improvement.

The overall measurement programme should be documented. In addition, the activities and data produced by (a) to (d) should be documented and maintained. Details of (a) to (d) are described below.

a) **Measurement development (including calendar plan to perform measurement activities)**
Organisations should develop measurements for the purpose of assessing the effectiveness of the implemented ISMS and controls. However, the measures and measurement development adopted by an organisation will vary based on a number of significant factors:
   - the information security risks that the organisation faces;
   - organisational size;
   - resources available; and
   - applicable legal, regulatory, compliance and contractual requirements.

[20] ISO/IEC 27004:2009

[21] ISO/IEC 27004:2009

The following should be considered when developing measurements:

i) **What to measure?**
Sources to measure can be derived from the results of a risk assessment (e.g. high risk assets), internal audit findings, corrective actions, security incidents or issues highlighted from a management review. Examples include, performance of controls implemented in the ISMS; status of information assets protected by the controls; performance of processes implemented in the ISMS; and competence level of personnel who will be responsible the implemented ISMS.

ii) **When to measure?**
The frequency of measurement will be based upon planned intervals or when there are significant changes that relate to the ISMS scope. Organisations should develop a calendar plan to perform the measurement activities.

iii) **How to measure?**
Methods of measurement should be determined to ensure the efficacy of the measurement. A measurement method may be subjective (relying on qualitative methods involving human judgment) or objective (using quantification based on numerical values). Whichever method is selected, it should produce comparable and reproducible results to be considered valid.

b) **Measurement operations**

Measurement operations include activities that are essential in ensuring that the developed measurement results provide accurate information with regard to effectiveness of the ISMS and controls and needs for appropriate improvement actions.

The following should be considered during measurement operations:

i) **What types of data to be collected?**
Types of data to be collected should depend on the measurement development defined earlier. It is also important to define a process or procedure for data collection.

ii) **Who should perform data collection?**
Relevant personnel should be assigned to perform the measurement from the respective areas/divisions related to types of data collected. For example, a system administrator should perform data collection for network security breaches, whereas a physical security officer should perform data collection for physical security breaches.

c) **Data analysis and measurement results reporting**

Data that has been collected should be analysed to produce results; and the results should be reported to relevant stakeholders. A number of analysis techniques can be applied by organisations. Data analysis should identify gaps between the expected and actual measurement results of an implemented ISMS, controls or groups of controls. These gaps will assist organisations in identifying needs for improvement of the implemented ISMS, including its scope, policies, objectives, controls, processes and procedures.

The following should be considered when analysing data and reporting measurement results:

i) **When and who should analyse and evaluate?**
The data should be analysed and evaluated based on the pre-determined calendar plan. The personnel who collects the data and/

or the personnel who understands the objective of the measurement should conduct the measurement analysis. The process for data analysis should be documented.

ii) **To whom results should be reported?**
Measurement results should be reported to the management[22]. The results from the measurement can assist during management review where it facilitates decision-making and justifies improvement of the implemented ISMS.

In addition, the results can provide inputs during an ISMS audit exercise. Furthermore, the measurement results should be reported and communicated to other personnel such as asset owners, ISMS process owners, personnel in charge of the information security risk management; and personnel who are responsible for the identified areas in need of improvement. Organisations should use the measurement results as a means to implement improvement of the overall ISMS.

d) **Information security measurement programme evaluation and improvement**
Organisations should evaluate the programme at planned intervals to gauge:
i) Effectiveness of the implemented information security measurement programme in ensuring that it:
- produces measurement results in a systematic manner;
- is executed as planned;
- addresses changes in the implemented ISMS and/or controls; and
- addresses changes in the environment (e.g. requirements, legislation, or technology).

ii) Usefulness of the measurement results to ensure that the relevant organisational information security needs are satisfied.

8.2 ISMS Internal Audit

Internal audit is one of the requirements in implementing ISMS. The purpose of this internal audit exercise is to determine whether controls, processes and procedures have been implemented and maintained in accordance with ISO/IEC 27001. An internal audit should be carried out based on the following:
- internal audit plan of an organisation;
- whenever an incident occurs;
- when there is a change in information asset; or
- when there is a requirement from an interested party.

There are other standards that organisations can use as a reference for internal audit i.e. ISO 19011:2011 - Guidelines for auditing management systems, ISO/IEC 27007:2011 - Guidelines for information security management systems auditing and ISO/IEC TR 27008:2011 - Guidelines for auditors on information security controls.

NOTE: *The ISO/IEC 27007:2011 should be read together with ISO 19011:2011*

The general process of an internal audit is described in Figure 5 where it is broken down into three (3) phases; as adapted from ISO 19011:2011 and ISO/IEC 27007:2011.

[22] ISO/IEC DIS 27001:2012

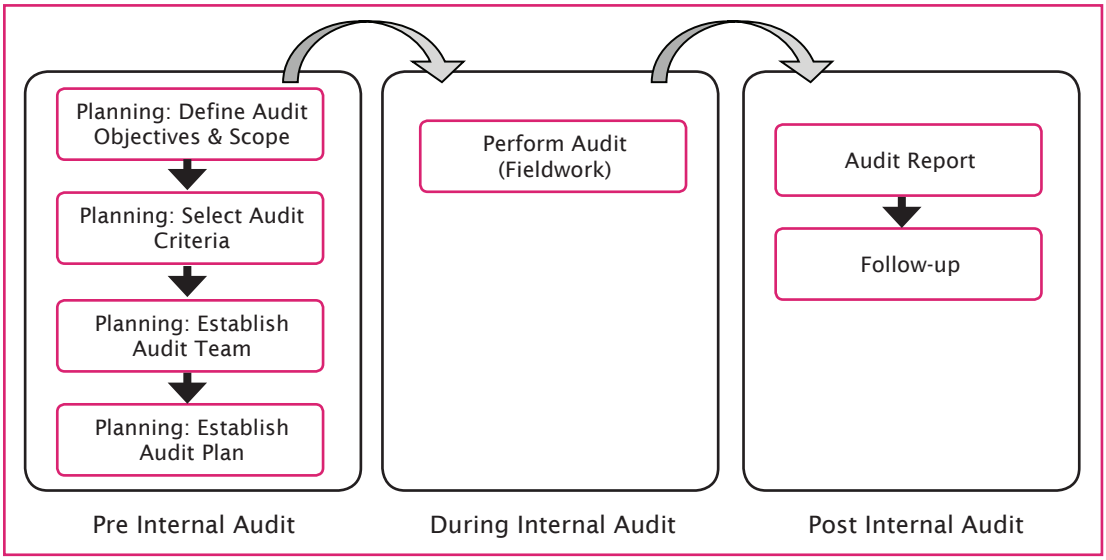

Figure 5: General Internal Audit Process

(Source: Adapted from ISO 19011:2011)

8.3 Phase 1: Pre Internal Audit

Prior to conducting an internal audit; an organisation should develop an audit programme that defines the frequency, methods, responsibilities, planning requirements and reporting. The audit objectives, scope and criteria of audit should also be established, followed by the establishment of audit team and audit plan.

a) **Define audit objectives and scope**
An organisation should define the audit scope to ensure that the objective of the audit can meet the requirements of the ISMS. The audit scope includes a description of the physical locations, organisational units, activities and processes, as well as the time period covered by the audit. For organisations with multiple sites, the internal audit should cover all sites within the ISMS scope.

b) **Select audit criteria**
An audit criteria encompasses the ISO/IEC 27001 requirements, applicable organisational policies and procedures, legal requirements (statutory, regulatory or industry body), management system requirements, contractual requirements, sector codes of conduct or other planned arrangements. Audit criterions are used as a reference against which conformity is determined.

c) **Establish audit teams**
Organisations may establish their own audit teams or appoint external parties to conduct the internal audit. The size, composition of the audit team is determined by the overall competence of the team, complexity of the audit, audit methods and legal and contractual requirements. Management should approve the selected audit team members and their appointments should be formalised.

The following are applied for establishing an internal audit team:

i) **Members of audit team**
The audit team members should include an audit team leader, auditor(s) and technical expert(s) (if any). An audit team leader should be able to identify the competency of each auditor; and ensure that each auditor possesses the required competence to achieve the objectives within the defined scope and time line. Technical expert(s) may be needed during the audit. Technical experts would advise auditors on matters related to their expertise only.

ii) **Competencies and skills required by audit team members**

The audit team members should demonstrate the following competencies and skills:

[1] Knowledge of ISO/IEC 27001 ISMS;
[2] Understanding of information security;
[3] Understanding of risk assessment and risk management from business perspectives;
[4] Technical knowledge of activities to be audited;
[5] General knowledge of regulatory requirements relevant to ISMS;
[6] Knowledge of management systems;
[7] Understanding of the principles of auditing based on ISO 19011;
[8] Knowledge of ISMS effectiveness review and measurement of control effectiveness.

iii) **Other skills required by the audit team members**

The audit team members are expected to demonstrate the following abilities, but not limited to:

[1] Identifying and solving problems;
[2] Undertaking appropriate technical research;
[3] Ability to work in teams in a consultative process;
[4] Apply professional scepticism[23] in gathering, evaluating and reviewing evidence provided by the auditees; Present, discuss, and at times defend views effectively through formal, informal, written, and oral communication;
[5] Treat sensitive and confidential information appropriately;
[6] Ability to apply relevant audit standards and guidance;
[7] Capacity for inquiry, abstract logical thought, and critical analysis; and
[8] Observe ethics and code of conducts in carrying out the audit.

d) **Develop audit plan**

The audit plan is prepared by the audit team leader and the following has to be taken into consideration:

- the effect of the audit activities on the auditees' processes and provide the basis for the agreement among the audit team and the auditees regarding the conduct of the audit
- the efficient scheduling and coordination of the audit activities in order to achieve its objectives effectively
- the details provided in the audit plan should reflect the scope and complexity of the audit, as well as the effect of uncertainty in achieving its objectives.

The audit plan should be documented and communicated to auditees and it should cover or make reference to the following[24]:

a) Audit objectives
b) Audit scope, including identification of the organisational and functional units, as well as processes to be audited
c) Audit criteria and any reference documents
d) Audit methods to be used, including the extent to which audit sampling is needed to obtain sufficient audit evidence and the design of the sampling plan, if applicable
e) Roles and responsibilities of the audit team members, as well as guides and observers
f) Allocation of appropriate resources to critical areas to be audited e.g. the need to engage a technical expert when an audit involves critical areas
g) Locations, dates, expected time and duration of audit activities to be conducted, including scheduling meetings with individuals in-charge

[23] Scepticism is an attitude of doubting that particular claims or statements are true or that something will happen (source: Longman Dictionary of Contemporary English)

[24] ISO 19011:2011

8.4 Phase 2: During Internal Audit

During the process of an internal audit, an opening meeting should be conducted prior to performing the audit activities; and concluded with a closing meeting to present the audit findings.

a) **Opening meeting**
The purpose of this opening meeting is to officiate the internal audit exercise. The meeting will be chaired by the CISO or anyone of a similar position preferably from top management and attended by auditors and business owners. During the opening meeting, the audit team leader will introduce the team members to the management and other respective auditees. The audit team leader should ensure that all planned audit activities can be performed.

b) **Perform audit**
The audit exercise will be carried out as specified in the plan. The auditees are expected to be prepared throughout the audit.

c) **Closing meeting**
The purpose of a closing meeting is to officially close the audit exercise. This closing meeting will be chaired by the CISO or anyone of a similar position preferably from top management and attended by auditors and business owners. The audit team leader presents the audit findings and conclusions. The audit findings should cover the following:
- The list of non-conformities
- The list of opportunities for improvement
- Observations and constructive feedback

All parties (auditees and audit teams) should agree on the time frame to produce an action plan in addressing their findings. This meeting also serves as a platform for discussion on any diverging opinions regarding the findings or conclusions, between the audit team and the auditees.

8.5 Phase 3: Post Internal Audit

Preparation and distribution of the audit report and a follow-up plan are performed during the post internal audit process.

a) **Prepare audit report**
The audit report will be prepared after the audit exercise is concluded. The report should include the following:
- The audit criteria, scope, methods and objectives
- The dates and places where the audit activities were conducted
- Summary of findings
- Statements on positive points, non-conformities, weaknesses, and/or opportunities for improvement
- Follow-up plan

b) **Distribute audit report**
The audit report should be ready within a timely manner or any period of time agreed upon after the closing meeting. The report has to be approved by the top management and distributed to the intended recipients.

c) **Conduct audit follow-up**
Before conducting the follow-up, the following should be agreed upon between the auditors and the auditees:
- depending on the audit objectives, the conclusions of the audit can indicate the need for corrective, or improvement actions
- rectification time-frame
- actions to be taken

A follow-up needs to be performed after auditors and auditees agree on the above. All the findings need to be verified to ensure that corrective or improvement actions have been taken and issues have been addressed.

8.6 Management Review

Management should review the ISMS to ensure its continuous suitability, adequacy and effectiveness. Management review can be conducted as a meeting subject to the organisational structure. An organisation can convene a specific meeting or create a slot in existing management meetings to specifically discuss on ISMS and information security issues.

The management review should include consideration of[25]:
a) the status of actions from previous management reviews;
b) changes in external and internal issues that are relevant to the information security management system;
c) feedback on the information security performance, including trends in nonconformities and corrective actions; monitoring and measurement results; audit results and fulfilment of information security objectives;
d) feedback from interested parties;
e) results of risk assessment and status of risk treatment plan; and
f) opportunities for continual improvement.

The results from the management review should be documented and maintained.

The frequency of the management review can be set at planned intervals (at least once a year) or depending on organisational decisions that are based on several factors e.g. organisational structure, previous management review outputs etc.

[25] ISO/IEC DIS 27001:2012

9. Maintain and Improve

Organisations need to ensure continual improvement of the ISMS. This is achieved through corrective actions to prevent recurrence of nonconformities and preventive actions to avoid potential non-conformance.

9.1 Nonconformities and Corrective Actions

Nonconformity can be defined as non-fulfilment of a requirement. Nonconformities and potential nonconformities can be identified based on the findings during the audit exercise as well as normal monitoring events. Corrective actions are the parts of improvement and effectiveness of ISMS and helps to deal with these nonconformities. The actions to rectify nonconformities and potential nonconformities should be recorded and communicated to the affected parties. Organisations should have mechanisms (e.g. documented information) in place that can be used to record details of nonconformities and corrective actions.

The details that should be recorded are details of personnel who have raised the nonconformities, root causes of nonconformities, areas affected and actions that have been planned. The actions taken should address the nonconformities raised. The nonconformities report should be presented to management periodically so as to ensure that the ISMS is implemented and enforced. The process from identifying the nonconformities until they have been satisfactorily closed should be documented. The process should be communicated and synchronized throughout the organisation. This is one of the functions of management review. The details of management review activities are explained in Section 8.6 Management Review.

9.2 Continual Improvement

The management should ensure the improvement and effectiveness of the ISMS and to also ensure the continual improvement of the ISMS through the use of information security policies, audit results, corrective actions and management review. Top management should mainly support the continual improvement as they play a vital role in delivering an effective ISMS.

10. ISMS Certification Process

This chapter provides an overview of the general ISMS certification process, surveillance audits and recertification for organisations that intend to pursue an ISMS certification.

Certification of ISMS is a third party conformity assessment activity conducted by a certification body (CB). A CB can be a non-governmental or a governmental body.

ISMS certification is voluntary, hence, organisations have a choice of pursuing certification or not. However, organisations should consider business, regulatory, legal or contractual requirements when deciding on ISMS certification.

There are many benefits of ISMS certification, amongst them are[26]:

- Enhances competitiveness and benchmarks an organisation within its peer community globally
- Increases trust from clients and partners via management's transparency to demonstrate due diligence
- Opportunities to maximise shareholders' value via optimising risks
- Recognises an organisation's established information security as an integral part of its business
- Promotes cost optimisation via pragmatic structures and system interoperability

10.1 Preparation for ISMS Certification

In order to be ISMS certified, organisations have to demonstrate the functionality of the ISMS. Programmes and procedures should be shown to be operational and various control mechanisms are properly implemented.

Preparation for ISMS certification includes, but not limited to:

a) The ISMS implementation (refer to Chapter 4 – 8) is complete and adequate;
b) Documented information retention: The organisation should retain at least six (6) months of documented information as evidence that ISMS is functional;
c) ISMS internal audit and management review: A complete internal audit and, at least, one management review should be conducted. Records of at least one ISMS internal audit and management review are needed;
d) Status of non-conformities: All non-conformities should be closed prior to the audit by CB.

[26] CSM27001, csm27001.cybersecurity.my/services.html

10.2 ISMS Certification Process by Certification Body

In general, ISMS certification process by a certification body (CB) is described in Figure 6:

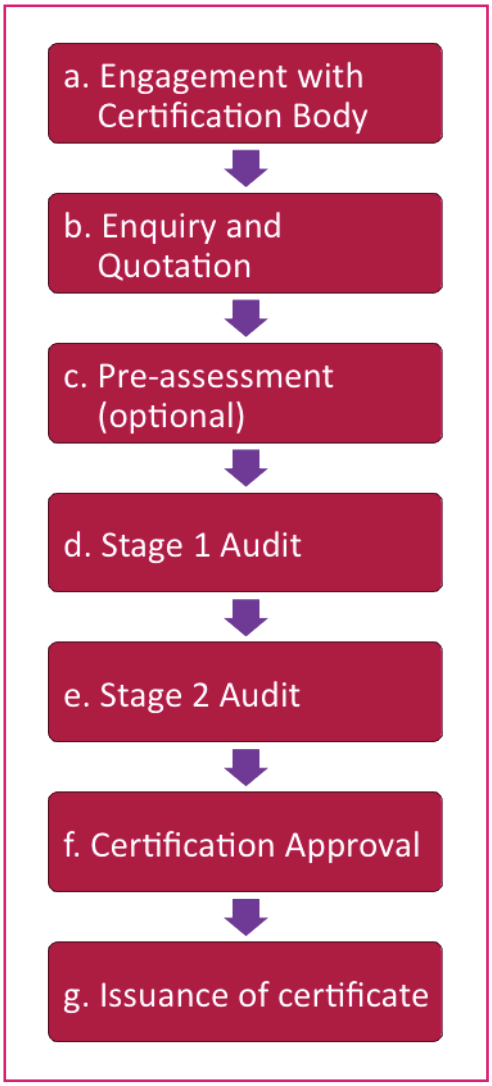

Figure 6: ISMS Certification Process

a) **Engagement with Certification Body (CB)**
The organisation can engage with a CB to discuss the organisation's ISMS scope for ISMS certification. A CB will verify that the scope and boundaries of the organisation's ISMS are clearly defined in terms of characteristics of business, the organisation, its location, assets, and technology. Discussion on scoping can be carried out when the organisation is ready to submit a certification enquiry to the CB or earlier.

b) **Enquiry and Quotation**
Organisations should complete the enquiry form and forward it to the CB for application review. If there is a need to obtain more information about the organisation's ISMS, or if there is a need to clarify some of the details contained in the application, then, the organisation will be contacted by the CB to obtain the required additional information.

Once the CB is satisfied with the organisation's application, a quotation will be generated for the certification work to be done. If the organisation accepts the quoted price, provision for legal agreements will be made.

c) **Pre-assessment (optional)**
The pre-assessment is an optional process. It is conducted as a preliminary step to evaluate whether the organisation's ISMS is functioning in accordance to necessary requirements and meets with the organisation's policies and objectives.

d) **Stage 1 Audit**
It is recommended that at least part of the Stage 1 audit be carried out at the organisation's premises in order to achieve the objectives stated below[27]:

i) to audit the organisation's ISMS documentation;
ii) to evaluate the organisation's location and site-specific conditions and to undertake discussions with the organisation's personnel to determine the preparedness for the Stage 2 audit;
iii) to collect necessary information regarding the scope of the management system, processes and location(s) of the organisation; and related statutory and regulatory aspects and compliance (e.g. quality, environmental, legal aspects of the organisation's operation, associated risks etc.); and
iv) to provide a focus for planning the Stage 2 audit by gaining sufficient understanding of the organisation's ISMS and site operations.

The minimum documentation required for Stage 1 audit are those defined in ISO/IEC 27001. This is then supported by the organisations' documents in relation to the ISMS scope.

The organisation is required to inform the CB if there are any critical documents that cannot be made available for the purpose of the audit. The CB will then determine if the audit can proceed or to be put on hold until such information can be made available.

Stage 1 audit findings should be documented and communicated to the organisation, including identification of any areas of concern that could be classified as non-conformity during the Stage 2 audit. Consideration will be given to the needs of the organisation to resolve areas of concern identified during the Stage 1 audit before Stage 2 is conducted.

e) **Stage 2 Audit**
The purpose of the Stage 2 audit is to evaluate the implementation, including effectiveness, of the organisation's ISMS. The Stage 2 audit should take place at the site(s) of the organisation. In the case of multiple sites, the organisation should inform the CB the difference in function between these sites. The CB will then determine the sites to be audited.

Stage 2 audit should include at least the following[28]:

i) information and evidence about conformity to ISO/IEC 27001 requirements;
ii) performance monitoring, measuring, reporting and reviewing against key performance objectives and targets (consistent with ISO/IEC 27001 requirements);
iii) the organisation's ISMS and performance as regards to legal compliance (if any);
iv) operational control of the organisation's processes;
v) internal ISMS audits and management reviews;
vi) management responsibility for the organisation's policies;

[27] ISO/IEC 27006:2011

[28] ISO/IEC 27006:2011

vii) whether the organisation's procedures for risk assessment and risk treatment appropriately reflects its activities and extends to the boundaries of the ISMS scope, and that it also addresses services or activities that are not completely within the scope of the ISMS; and
viii) links between the normative requirements, policy, performance objectives and targets, any applicable legal requirements, responsibilities, competence of personnel, operations, procedures, performance data and internal audit findings and conclusions.

Where non-conformities are observed, the CB will formally document it in a Non-Conformity Report (NCR)/Opportunities For Improvement (OFI) template. The organisation should define all non-conformities and provide an appropriate set of corrective actions to resolve the identified non-conformities.

f) **Certification Approval**
All information and audit evidence gathered during the Stage 1 and Stage 2 audits will be analysed to review the audit findings and agree on the audit conclusions.

The CB will make the final decision after all non-conformities have been resolved on the basis of an evaluation of the audit findings. The organisation will be informed of this decision immediately.

g) **Issuance of Certificate**
Once approved for certification, the organisation will be entitled to receive a copy of the ISMS certificate.

A CB grants to the organisation, upon receipt of the certificate, a non-exclusive, non-transferable and revocable license to use a certification mark applicable to the scope that has been certified in the manner described by the CB.

Information about ISMS certified organisations will be made available publicly on the CB's website.

Organisations may request to amend details in their ISMS certificate at any point of time. These amendments may include the name of the organisation, change of address or the scope of the ISMS certification. Request for such changes should be made in writing to the CB.

10.3 Surveillance Audit

Surveillance audits are to be conducted at least once a year. The first surveillance will be carried out within twelve (12) months from the last day of the Stage 2 audit. Surveillance audits are conducted on-site, but are not necessarily a full ISMS audit.

Surveillance audits should review the following[29] (this list is non-exhaustive):
i) internal ISMS audit, management review and corrective action;
ii) progress of planned activities aimed at continual improvement;
iii) effectiveness of the ISMS to achieve the information security policy objectives;
iv) treatment of appeals and complaints, and whether this treatment was adequate;
v) changes to the documented management system;
vi) correct use of the certificate and certification logo; and
vii) actions taken on non-conformities identified during the last audit.

[29] ISO/IEC 27006:2011

10.4 Recertification

Renewal of certification is subject to a satisfactory recertification audit carried out before the expiry date of the certificate. A recertification audit should be planned and conducted to evaluate the continued fulfilment of ISO/IEC 27001 requirements.

The recertification audit should include an on-site audit that addresses the following[30]:

i) confirmation of the continued conformity and effectiveness of the ISMS as a whole, and its continued relevance and applicability for the scope of certification;
ii) review of the effectiveness of the ISMS in light of internal and external changes, and its continued relevance and applicability to the scope of ISMS certification;
iii) demonstrated commitment to maintain the effectiveness and improvement of the ISMS in order to enhance overall performance;
iv) whether the operation of the certified ISMS contributes to the achievement of the organisation's policies and objectives; and
v) consideration of the performance of the organisation's ISMS over the period of certification, and inclusion of the review of previous surveillance audit reports.

Recertification audit activities may need to have a Stage 1 audit in situations where there have been significant changes to the ISMS, the organisation, or the context in which the ISMS is operating.

During a recertification audit, if instances of non-conformity or lack of evidence of conformity are identified, the CB will define time limits for corrective actions to be implemented prior to the expiration of certification.

[30] ISO/IEC 27006:2011

Appendix A - Examples of ISMS Scope Statement

Examples of ISMS scope statement for services and production of products are as follows[31]:

Example 1:
ISMS for the provision of managed security services (intrusion prevention guard, virus guard, and content guard) provided by the security operation centre located at [location name]. This is in accordance with Statement of Applicability Revision [number] dated [date].

Example 2:
ISMS for data centre operations for delivery of managed ICT services to [Organisation's name]; 2) Data centre operations for supporting internal [organisation's name] ICT. This is in accordance with Statement of Applicability version [number] dated [date].

Example 3:
ISMS for managed security services covering security alert monitoring and notification and security incident management for security operation centre located at [location name]. This is in accordance with Statement of Applicability Revision [number] dated [date].

Example 4:
ISMS for the provision of supporting activities for treated water to be supplied to end customer at [location name] water treatment plant. This is in accordance with Statement of Applicability Revision [number] dated [date].

Example 5:
ISMS for an air conditioning manufacturing plant as well as a Research and Development Centre. This is in accordance with Statement of Applicability Version [number] dated [date].

Example 6:
ISMS for manufacturing of refrigerant compressors, motors and components (motor protectors and relays). This is in accordance with Statement of Applicability Version [number] dated [date].

Example 7:
ISMS for the manufacturing of precision casting components. This is in accordance with Statement of Applicability Version [number] dated [date].

Example 8:
ISMS for the design, development and manufacturing of liquid-crystal display televisions (LCD TVs). This is in accordance with Statement of Applicability Version [number] dated [date].

[31] www.iso27001certificates.com

Appendix B - Common Timeline for ISMS Implementation and Certification

According to the ISO 27001 Global Survey, 2008, the common timeline for ISMS implementation and certification varies between six (6) months to 2 (two) years[32].

Details are provided in Table 5. Ultimately, it is the top managements decision to determine the timeline for the implementation depending on their commitment and availability of resources.

Table 5: Timeline for ISMS Implementation and Certification

Timeline	Percentage of organisations that received ISMS certification
Within 2 years	93 percent
12 months or less	60 percent
6 months or less *NOTE: This timeline is observed for organisations that are already certified to quality standard – ISO 9001 (80 percent) or environmental standard – ISO 14001 (12 percent)*	20 percent

[32] ISO 27001 Global Survey, 2008, www.d1073625-1.blacknight.com/format/ISO27001GlobalSurvey.pdf

Appendix C - Additional Roles and Responsibilities in Information Security

Table 6 below provides additional roles and responsibilities in information security[33].

Table 6: Additional Roles and Responsibilities in Information Security

Role	Brief Description of Responsibility
Stakeholder	The stakeholder is primarily defined as persons/bodies outside the normal operations – such as the board, owners (both in terms of organisational owners if the organisation is part of a group or a government organisation, and/or direct owners such as shareholders in a private organisation). Other examples of stakeholders could be affiliated companies, clients, suppliers or more public organisations such as governmental financial control agencies or relevant stock exchange, if the organisation is listed.
Chief Information Security Officer (CISO)	CISO has the overall responsibility and governance for information security ensuring the correct handling of information assets.
Chief Risk Officer (CRO)	CRO has the overall responsibility and governance for managing risks in the organisation.
System Administrator	The person responsible for an IT system.
IT Manager	The manager of all IT resources.
Legal Advisor	Many information security risks have legal aspects and the legal advisor is responsible for taking these into consideration.
Archive Officer	All organisations have archives containing vital information that needs to be stored for long periods of time. The information may be located on multiple types of media and a specific person should be responsible for the security of this storage.
Privacy Officer	If required by national law, there may be a person responsible for being the contact for data inspection board or similar official organisation that oversees personal integrity and privacy issues.
System Developer	If an organisation develops their own information system, the development of the system should be performed by the system developers.
Specialist/Expert	The specialists and experts responsible for some operations in an organisation should be referred to in terms of their intention about ISMS matters as it relates to use in their specific fields.

[33] Adapted from ISO/IEC 27003:2010

Role	Brief Description of Responsibility
External Consultant	External consultants may provide advice based on their macroscopic points of view of an organisation and industry experience. However, consultants may not possess in-depth knowledge of the organisation and its operations.
Employee/Personnel/ Staff/User	Each employee is equally responsible for maintaining information security in the workplace and in his/her environment.
Trainer	The trainer implements training and awareness programmes. The trainer can be a process or policy owner, who has knowledge and experience in a particular process.
Local IT or IS responsible	In a larger organisation there is often somebody in the local organisation that has local responsibility for IT matters, and possibly for information security as well.
Champion (Influential Person)	In a larger organisation it may be of great help in the implementing stage to have people who have in-depth knowledge about the implementation of an ISMS and can support the understanding and reasons behind the implementation. They may influence opinions in a positive way and may also be called “Ambassadors”.

Appendix D - Recommended Readings

Table 7 provides recommended readings for implementing ISMS.

Table 7: Recommended Readings and Description

No	Recommended Readings	Description
1	ISO/IEC 27000:2009 - Information security management systems - Overview and vocabulary	Provides terms and definitions, and an introduction to the ISMS family of standards that: 1. defines requirements for an ISMS and for those certifying such systems; 2. provides direct support, detailed guidance and/or interpretation for the overall Plan-Do-Check-Act (PDCA) processes and requirements; 3. addresses sector-specific guidelines for ISMS; 4. addresses conformity assessment for ISMS.
2	ISO/IEC 27002:2005 - Code of practice for information security management	Contains best practices of control objectives and controls in the following areas of information security management: • security policy; • organisation of information security; • asset management; • human resources security; • physical and environmental security; • communications and operations management; • access controls; • information systems acquisition, development and maintenance; • information security incident management; • business continuity management; • compliance
3	ISO/IEC 27003:2010 - Information security management system implementation guidance	Provides practical guidance in developing the implementation plan for an Information Security Management System (ISMS) within an organisation in accordance with ISO/IEC 27001:2005. The actual implementation of an ISMS is generally executed as a project.
4	ISO/IEC 27004:2009 - Information security management – Measurement	Provides guidance on the development and use of measures and measurement in order to assess the effectiveness of an implemented information security management system (ISMS) and controls or groups of controls, as specified in ISO/IEC 27001.
5	ISO/IEC 27005:2011 - Information security risk management	Provides guidelines for information security risk management. It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.

No	Recommended Readings	Description
6	ISO/IEC 27006:2011 - Requirements for bodies providing audit and certification of information security management systems	Specifies requirements and provides guidance for bodies providing audit and certification of an information security management system (ISMS), in addition to the requirements contained within ISO/IEC 17021 and ISO/IEC 27001. It is primarily intended to support the accreditation of certification bodies providing ISMS certification.
7	ISO/IEC 27007:2011 - Guidelines for information security management systems auditing	Provides guidance on managing an information security management system (ISMS) audit programme, on conducting the audits, and on the competence of ISMS auditors, in addition to the guidance contained in ISO 19011.
8	ISO/IEC TR 27008:2011 - Guidelines for auditors on information security controls	Provides guidance on reviewing the implementation and operation of controls, including technical compliance checking of information system controls, in compliance with an organisation's established information security standards.
9	ISO/IEC 27011:2008 - Information security management guidelines for telecommunication organisations based on ISO/IEC 27002	Defines guidelines supporting the implementation of information security management in telecommunication organisations. The adoption of this Recommendation International Standard will allow telecommunication organisations to meet baseline information security management requirements of confidentiality, integrity, availability and any other relevant security property.
10	ISO 27799:2008 - Information security management in health using ISO/IEC 27002	Provides guidance to health organisations and other holders of personal health information on how to protect such information via implementation of ISO/IEC 27002.
11	ISO/IEC 27001 for Small Businesses - Practical Advice, Edward Humphreys, ISO/IEC, 2010	This handbook takes the mystery out of information security and presents a practical, clearly explained step-by-step approach for SMEs to implement an information security management system (ISMS) based on ISO/IEC 27001.
12	Information Security Risk Management - Handbook for ISO/IEC 27001, Edward Humphreys, BSI, 2010	Gives guidance to support the requirements given in ISO/IEC 27001:2005 and the advice given in ISO/IEC 27005, regarding all aspects of an ISMS risk management cycle. This cycle includes assessing and evaluating the risks, implementing controls to treat the risks, monitoring and reviewing the risks, and maintaining and improving the system of risk controls.
13	Manual ISMS, MAMPU, 2010	Provides explanation regarding ISMS based on MS ISO/IEC 27001:2006.

No	Recommended Readings	Description
14	Risk Assessment Guideline, MAMPU, 2010	Provides an understanding for a security risk assessment in information security management systems.
15	Risk Management Guide for Information Technology Systems, NIST SP 800-30, 2002	This guide provides a foundation for the development of an effective risk management programme, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems. The ultimate goal is to help organisations to better manage IT-related mission risks.

Appendix E - Methods to Obtain Standard

Standards are developed by ISO (International Organisation for Standardisation), which is the world's largest developer of voluntary International Standards[34]. ISO comprises of various national bodies that represent ISO in their respective countries. Standards are developed by a panel of experts from these national bodies and through a consensus process. This means they reflect a wealth of international experience and knowledge.

Once the need for a standard has been established, these experts meet to discuss and negotiate a draft standard. As soon as a draft has been developed, it is shared with ISO members who are asked to comment and vote on it. If a consensus is reached, the draft becomes an ISO standard; else the standard will be reverted for further editing.

To implement ISMS, the relevant standards in ISO/IEC 27000 families (refer to Appendix D - Recommended Readings) should be obtained.

There are several ways to obtain a copy of the standard:

a) Purchase via ISO portal[35]
   ISO standards and other ISO publications can be obtained from the ISO Central Secretariat via the ISO Online Store or may be ordered by telephone, e-mail, facsimile and by traditional mail order. For online purchases, simply visit store.iso.org.

b) Purchase via MSonline portal[36]
   For purchasing Malaysian standards online, you can visit www.msonline.gov.my. This portal provides a one-stop access to a collection of Malaysian standards.

   NOTE: *This portal is for purchasing Malaysian standards.*

c) Volunteer as Member of Working Group
   In Malaysia, Technical Committee of Information Security (TC/G/5)[37] currently oversees the development of international standards in information security areas. Several working groups are formed under this TC/G/5, which are[38]:
   - WG/G/5-1 Information Security Management Systems
   - WG/G/5-2 Cryptography and Security Mechanisms
   - WG/G/5-3 Information Security Evaluation Criteria
   - WG/G/5-4 Security Control and Services
   - WG/G/5-5 Identity Management and Privacy Technologies
   - WG/G/5-7 Industry Automation and Control Systems

WG/G/5-1[39] currently oversees the development of international standards in ISO/IEC 27000 families. A member of this working group will have access to standards in ISO/IEC 27000 families.

[34] www.iso.org

[35] www.iso.org

[36] www.msonline.gov.my

[37] smsonline.sirim.my/Committee_Ctrl.do?op=retrieveISCCommittee&page=isc&id=ISC/G&type=I&isccode=G

[38] smsonline.sirim.my/Committee_Ctrl.do?op=retrieveTCCommittee&page=1&id=TC/G/5&type=T&isccode=G

[39] smsonline.sirim.my/Committee_Ctrl.do?op=retrieveWGCommittee&page=1&id=WG/G/5-1&type=W&isccode=G

Appendix F - Example of Challenges in Conducting Risk Assessments

Table 8 below provides examples of challenges in conducting risk assessments.

Table 8: Challenges in Risk Assessment and Recommended Approaches
Source: Slides on Case Study ISMS Risk Management, KPMG, accessed on 7 Feb 2013

Challenges in Risk Assessment	Recommended Approaches
Challenge #1: **An organisation has an existing Enterprise Risk Management (ERM)/ Operational Risk Management Framework.** Typically this is a challenge, due to the fact that the ISMS Risk Management approach is asset based, compared to the overall Enterprise Risk Management (ERM), which will typically look at broader categories of the risks at the enterprise level. In this case, the Enterprise Risk Management team will have to be involved during the alignment of frameworks, however the asset based risk assessment is still seen as a very operational matter and often the risk management team will prefer not to facilitate these risk assessment exercises. However if the alignment is not performed, apart from potential non – compliance against the standard (alignment clauses), there will also be the challenge for the operational team to complete more than one risk assessment exercise per quarter/ defined period. This will also mean that there is a potential duplication of work and even potentially different ratings of similar risks.	**To address Challenge #1:** 1. ISO/IEC 27001 standard dictates the ISMS Risk Management Framework will have to be aligned to the Enterprise Risk Management Framework, the approach includes identification of responsibilities under the ERM Framework and establishing the context under the scope of ISMS implementation. 2. Perform discussions with risk management unit on alignment. Likelihood is that a separate procedure document will be required, which will adopt the ERM framework, and will be reported to Risk Management on an on-going basis. 3. Typical areas of alignment include: - Risk assessments - Categories of risks - Risk acceptance criteria's - Risk treatment options
Challenge #2: **There are no existing detailed asset inventories.** Typically this is a challenge, since there is no single inventory, which will cover all the details around the required information in ISO/IEC 27001. Typical examples include physical assets where it is difficult to obtain all serial numbers for specialised equipment (e.g. telecommunication modules, Supervisory Control and Data	**To address Challenge #2, #3 and #4:** 1. In order to address these challenges, inquiries are essential on available sources of asset information – this will include financial systems, store systems, any existing ISO 9000 documentation, backup library documentation, commissioning documentation, etc. 2. Once the sources are identified, obtain reports and details to identify the missing data.

Challenges in Risk Assessment	Recommended Approaches
Acquisition (SCADA) system modules, etc – where the serial numbers information is located at the module itself.	3. In CNII areas and critical infrastructures such as power / water /nuclear plants, oil and gas, core telecommunication networks, etc. – it is quite likely that there are large and dispersed amounts of assets, which will not be easy to be inventoried – e.g. serial numbers information might not be available and may not be collectable from the assets, since this may cause operational downtime. 4. Solution is to combine the assets in logical groups – *(e.g. Cabinet with core modules which includes (number) x type of modules))*. 5. The criteria for grouping however should be clearly defined – e.g. the assets / modules from the same type, same threats and vulnerabilities, same owner, same business value and same location could be combined with clear identification of how many unit numbers are included. 6. Asset information that is incomplete will have to be updated either manually or in an automated way (through discussions with owners, questionnaires, etc.).
Challenge #3: **Large scale of assets within scope of implementation and therefore no central inventory exists.** The bigger the scope of implementation is the bigger the scope of the assets – this typically brings the issue that the operational teams will tend to combine the assets to bypass the asset listing process – however sometimes by doing this they will omit certain critical components, and might not assign the correct value to them. To overcome this issue it is suggested that a formal method for grouping of assets is defined.	
Challenge #4: **No assigned owners or incomplete owners' information.** The bigger the organisation is the higher the chances are that asset related information is incomplete and not up-to-date. Various reasons exist – e.g. the assets were transferred, the asset owner left the company, the asset was only reviewed once a year, the asset location was changed, equipment was removed for maintenance and was taken off premises, etc.	

Challenges in Risk Assessment	Recommended Approaches
Challenge #5: **Certain assets are maintained/ managed by outsourced vendors or by third parties.** The challenge is related to the ability to know the latest status of the asset and to ascertain the related security controls implemented by a third party. Typically, this concerns direct relationship in regards to the security requirements for outsourcing vendors. The challenge here could extend further for outsourcing environments in which the assets are located in a different location, which does not belong to the organisation. As such, what could potentially occur as an issue, is that the outsourcing vendor provides its own security policy and the customer's security policy does not align in terms of controls. E.g. physical zoning controls, ways of handling critical information – in order to ensure that these issues are tackled earlier in the process and resolved, both parties should work towards the definition of the formal SLA and reporting on compliance.	**To address Challenge #5 and #6:** 1. In order to address these issues, inquiries are essential on available sources of contractual agreements, which should include the roles and responsibilities in relation to these assets, etc. 2. Based on the nature of the assets, these assets will have to be listed either as a service provided to the organisation or as detailed assets, where the owner / custodian is not the implementing organisation. 3. The Service Level Agreement (SLA)/ contract with vendors should also clearly address the security requirements for these types of devices and should be monitored as part of an on-going process. 4. Multi-tenancy of assets might results into multiple owners/custodians – however a primary role will have to be assigned to an individual who will be the ultimate owners and ultimate custodian for accountability purposes.
Challenge #6: **Multi-tenancy of assets.** The challenge here talks about assets of multiple organisations hosted at the same location – e.g. co-hosting, co-sharing of infrastructure, cloud services, etc. Typically, concerns are raised during risk assessment phases – since either the clients do not have control over the way the service is provided or if it is a national, regional or international service, further security controls might not be easy to implement. Multi-tenancy brings in the issues in relation to data leakage, information privacy and confidentiality, integrity issues, etc.	

Appendix G - References

[1] ISO/IEC DIS 27001:2012, Information technology - Security techniques - Information security management systems – Requirements

[2] ISO/IEC DIS 27002:2012, Information technology - Security techniques - Code of practice for information security controls

[3] ISO/IEC 27000:2012, Information technology - Security techniques - Information security management systems – Overview and vocabulary

[4] ISO/IEC 27001:2005, Information technology - Security techniques - Information security management systems – Requirements

[5] ISO/IEC 27002:2005, Information technology - Security techniques - Code of practice for information security management

[6] ISO/IEC 27003:2010, Information technology - Security techniques - Information security management system implementation guidance

[7] ISO/IEC 27004:2009, Information technology - Security techniques - Information security management – Measurements

[8] ISO/IEC 27005:2011, Information technology - Security techniques - Information security risk management

[9] ISO/IEC 27006:2011, Information technology - Security techniques – Requirements for bodies providing audit and certification of information security management systems

[10] ISO 19011:2011, Guidelines for auditing management systems

[11] Humphreys, Edward. 2010, ISO/IEC 27001 for Small Businesses – Practical advice

[12] ISO 17021:l2011 Conformity assessment – Requirements for bodies providing audit and certification of management systems

CyberSecurity MALAYSIA

An agency under MOSTI

People First, Performance Now

MOSTI
Ministry of Science, Technology and Innovation

Corporate Office:
CyberSecurity Malaysia, Level 5, Sapura@Mines, No 7, Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan, Selangor Darul Ehsan | Tel : +603 8992 6888 | Fax : +603 8992 6841
Email: info@cybersecurity.my | Customer Service Hotline: 1300-88-2999 | www.cybersecurity.my