

Implementing an ISMS

Participant Guide

IMPLEMENTING AN ISMS

CONDITION OF USE

© Queensland Government 2017

All rights reserved. No part of this work may be reproduced or copied in any form or by any means (graphic, electronic or mechanical, including photocopying, recording, taping or information retrieval systems) without the written permission of the Queensland Government Chief Information Office or as otherwise permitted by the operation of the law.

IMPLEMENTING AN ISMS

PURPOSE

Critical in today's information centric environment is the subject of 'information security', whether for reasons of safety, security, legal, ethics or compliance. The management of such information is of paramount importance and an essential element of good organisational practice in today's rapidly evolving world. This is equally important in both the private and public sectors.

The international standard ISO/IEC 27001:2013 '*Information Security Management Systems*' and its complementary standard ISO/IEC 27002:2013 '*Codes of Practice for Information Security Management*' form the basis of the controls necessary to ensure risks to information and systems are understood and effectively managed.

ISO/IEC 27001:2013 covers all types of organisations and specifies the requirements for establishing, implementing, operating, reviewing, maintaining and improving an information security management system in the context of risks presented by the organisation's commercial, technical and regulatory environment.

This course provides an opportunity to learn the necessary skills to develop, implement and monitor an Information Security Management System within an organisation and how to assess and protect the organisation against risks.

Participants will learn how to evaluate their agency's information risks and implement a practical Information Security Management System (ISMS) that is compliant with the ISO/IEC 27001:2013 standard.

Participants will also learn the necessary activities to transition from the existing IS18 framework to an operational ISMS and understand the steps necessary to ensure the ongoing operations of the ISMS

The purpose of the course is:

- To understand the concepts contained within ISO/IEC 27001:2013 and its role in defining and operating an Information Security Management System
- To develop the skills needed to implement an ISMS based on the ISO/IEC 27001:2013 Information Security Management Systems standard
- To understand the necessary steps to transition from IS18 to an ISMS

LEARNING OUTCOMES

Upon completion of this course, participants will be able to:

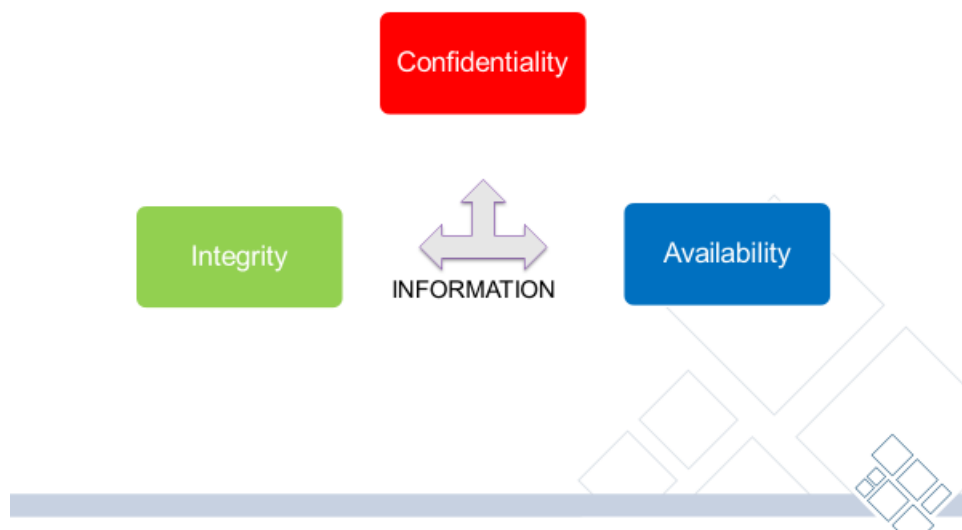
- Identify the need for information security
- Understand the drivers for the change from IS18
- Understand the contents of an ISMS in the context of ISO/IEC 27001:2013
- Define the scope of an ISMS for your agency
- Identify information security risks
- Build the appropriate components of an operational ISMS

Module 1: Information Security



IMPLEMENTING AN ISMS

Characteristics of Information Security



INFORMATION SECURITY

In today's information centric environment, all organisations have a high reliance on the information they own or maintain on behalf of their stakeholders. Risks to this information therefore represent risks to the organisation. Good governance principles suggest that organisations need to have understood their risks and made choices to manage them. The security of this information is critical to the ongoing viability and operations of the organisation.

Information has three main characteristics:

1. Confidentiality - Providing access to only those authorised personnel who need the access
2. Integrity - Keeping the information accurate and complete
3. Availability – Making sure the information is available to the authorised user when they need it

ISO/IEC 27000 defines information security as the “preservation of confidentiality, integrity and availability of information”.

IMPLEMENTING AN ISMS

Other attributes of information that have a bearing on information security include properties such as authenticity, accountability, non-repudiation and reliability but these are not included within the existing ISO 27000 definition.

Information security is important to organisations because the information that is used to deliver services and functions has value. This value is usually related to the consequences to the organisation if the information is compromised in some form.

Such compromises include improper disclosure or misuse of the information, accidental or deliberate modification of the information and the unavailability of the information when access to this is required.

Consequences from such compromises can include:

- financial losses;
- reputational and brand damage;
- breaches of legal, regulatory or contractual obligations;
- risks to a person or persons health or safety;
- inability to deliver organisational services.

Such impacts represent risks to the operations and viability of government agencies and private sector organisations alike. Therefore, the identification and management of these risks is vital.

Information security management relates to the practices involved in understanding and managing these risks.

Please note: For the purposes of this course, when the term ISO 27001 is used, it refers to the ISO/IEC 27001:2013 standard. Similarly, for ISO 27002 read the correct reference as ISO/IEC 27002:2013



ACTIVITY 1: INFORMATION SECURITY

OBJECTIVE

To discuss the information security drivers that may exist within agencies and the perceived value of information security with the agency.

TIME

15 minutes

TASK

Brainstorm as a group the following questions.

1. Is information security seen as important within your agency?
2. Why?
3. What drives this? External or internal factors?

NOTES

[illegible]

Module 2: Background and Context



IMPLEMENTING AN ISMS

Problem

- Compliance approach is not working. 'Tick and Flick' once a year.
- Security is not viewed as a process.
- Security is often considered a technical problem.
- Control maturity is not measured (binary).
- Accountability patchy – some agencies signing off at CEO level, others not.
- Agencies have different objectives, risk tolerances & require flexibility to tailor security responses to risk.
- Still need agencies to secure government data
- Don't want to erode the good that IS18 does during change.

BACKGROUND - IS18

Historically, Queensland Government agencies were required under the QGEA to implement the requirements of IS18 to protect information and ICT assets from unauthorised use, modification, loss or release.

The IS18 framework provides a compliance-based approach to achieving the Government's security objectives.

IS18 aimed to prescribe a minimum set of controls and activities to create a secure ICT posture. This compliance-centric approach was appropriate whilst the Queensland Government developed a security capability. However, as the capability matured, the use of a compliance-based approach was seen to have a number of limitations in its approach. The current version of IS18:

- Is not aligned to the current version of the ISO/IEC 27001:2013 information security standard, having been built against the 2005 version of ISO 27002;
- Needs refreshing to match agency requirements in managing increasing complex ICT and business environments;
- Focuses on controls, not control objectives;
- Lacks guidance on governance and assurance requirements;
- Represents a 'one size fits all' approach to security and may lack flexibility needed in a modern organisation;

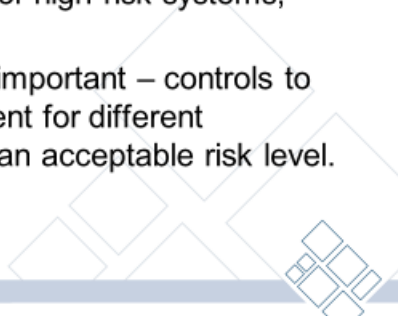
IMPLEMENTING AN ISMS

- Relies on self-assessment, which provides limited assurance;
- Is often viewed as a 'once a year' activity;
- Is not well understood by industry and providers.

Consideration of a more flexible approach to management of information security has led to the development of an approach based on ISO 27001. This approach takes into account the following:

- Compliance to security standards are no longer considered enough to meet increasing threat environment;
- Information security needs to continually evolve to assist agencies to manage their risk to acceptable levels;
- Security is a business issue, not an ICT issue, and a cross-functional approach is critical to success.

The Solution

- Require agencies to run an ISMS based on an international standard.
 - Require accountable officers to attest to Information Security in a similar way to other cross functional risks (e.g. financial/fraud OH&S)
 - Consider assurance, especially for high risk systems, before signing off.
 - The 'control objectives' are very important – controls to meet the objective may be different for different environments. Aim is to achieve an acceptable risk level.
- 

THE CHANGES

The new framework has the following requirements and benefits:

- Agencies will operate ISMS' based on current international standards (ISO/IEC 27001:2013);
- Agencies will take a risk centric approach to managing security posture;
- A reduced set of minimum requirements provides increased focus on meeting control objectives;
- Control objectives are met with a risk based approach;
- A systematic approach to risk analysis will be central to control decisions;
- Security functions are completed during business processes throughout the business lifecycle;
- Better allocation of time and resources to security challenges relevant to specific agencies;
- Increased industry adoption of ISO/IEC 27001:2013 will assist in aligning requirements and improving transparency when using cloud and managed services.

Note that adoption of the ISMS still provides an environment where all requirements of IS18 are met and does not weaken the security posture.

NOTES

[illegible]

Module 3: IS18 Transition



IMPLEMENTING AN ISMS

Key considerations

- Understand that the work done for IS 18 compliance provides key information for the ISMS
- The control information gathered will be useful at the appropriate time during ISMS implementation
- Key is “don’t let the tail wag the dog”
- Still remember that the shift is to a risk-based model
 - Risk assessment and management the key elements

KEY CONSIDERATIONS

The transition from IS18 is not designed to weaken the security posture of agencies. The implementation of an ISMS will leverage the work already done in this space by agencies by utilising the control information during the ISMS construction, implementation and operations phases.

The key paradigm shift is from a model focussing at a control level to one that considers the objective of the control and the risks being managed. Controls are selected to manage risk and therefore understanding risks and thus the objective of the control set provides a more structured but flexible approach to security management.

The information captured by agencies for their IS18 compliance requirements will be invaluable during the “control selection” phase of the risk management process.

NOTES

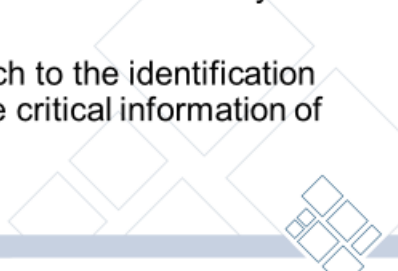
[illegible]

Module 4: ISMS



IMPLEMENTING AN ISMS

ISMS

- A management system that includes organisational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources
 - A management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security
 - A practical and defined approach to the identification and management of risks to the critical information of the organisation
- 

INFORMATION SECURITY MANAGEMENT SYSTEMS


An Information Security Management System (ISMS) comprises the policies, standards, procedures, practices, behaviours and planned activities that an organisation uses in order to secure its (critical) information assets. It provides a clear understanding of the objectives and context of information security both within, and external to, the organisation.

The design of the ISMS and how it is implemented depends on the needs and objectives of the organisation. Factors to be considered include the size and structure of the organisation, the market or service area in which it operates and the sensitivity of the information it owns or manages on behalf of others.

The purpose of an ISMS is to secure an organisation's information and information assets by identifying, assessing and managing risks to that information. This process should not be seen as a "once off" exercise but as part of an ongoing risk management lifecycle. The ISMS provides systematic measurement and reporting of the effectiveness of the implemented controls.

Successful ISMS implementations provide a practical and pragmatic framework for the identification and management of information security risks.

Components of an ISMS?

- A risk assessment method
 - A set of documented security controls and processes
 - Security awareness training, guidance and competencies
 - Tools and technology, including firewalls, AV protection, network scanning and monitoring appliances, logging and reporting tools
 - People
- 

COMPONENTS OF AN ISMS

An ISMS generally contains a number of key elements. These elements include:

- Some form of risk assessment method;
- Documented controls and processes;
- Security awareness, guidance, training and competencies;
- Tools, technology and equipment, including firewalls, antivirus and malware scanners and protection, network security tools and logging and security monitoring tools;
- People.

Personnel within scope of the ISMS represent critical resources. Such personnel may include:

- Management
- Employees
- Suppliers
- Other interested parties (e.g. regulatory authorities)

Ignoring people and their behaviour will compromise the operations of the ISMS and therefore the information security environment.

Implementation Pitfalls

- Generally 2 key reasons for failure
 1. Lack of management commitment
 - Under-resourced
 - “Lip service”
 2. Over-engineering
 - Too complex a design
 - Over-documented
 - Aiming at perfection
 - Too large a scope



IMPLEMENTATION PITFALLS

Choosing to implement an ISMS is a strategic decision for the organisation. Given this strategic focus, it is important to recognise that a successful implementation of an ISMS will require senior management commitment and support.

One common pitfall is that this support is present during the “project” phase, that is, the implementation of the ISMS, but then falls away when the system is operationalised.

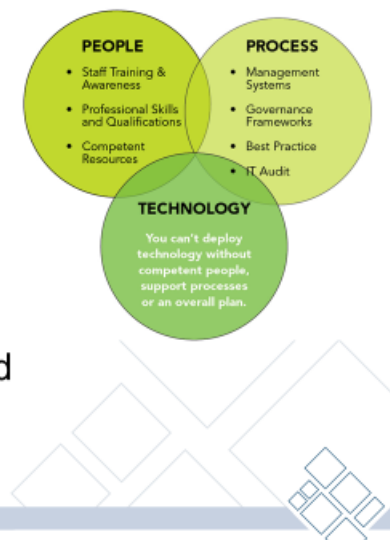
Another key reason that ISMS deployments fail is the “over-engineering” trap. Often those that build such systems seek to build significant detail into the system. However, the ISMS is an organic system and like all organic systems, the more complicated the organism, the more opportunity for failure.

As elements of the system are developed they should be deployed and used. ISMS implementation is not “big bang” and does not require all elements in place to bring benefits.

The key focus should always be on simplicity in terms of design and operations. Do not strive for perfection. The ISMS contains enough mechanisms for self-correction and improvement.

ISMS and ISO 27001

- ISO 27001 provides a framework for the development, implementation, operations and improvement of an ISMS
- Involves people, policies, processes, technologies and tools



ISMS AND ISO 27001

An ISMS does not need to be built on the ISO 27001 standard but this standard provides a globally recognised and understood framework. This common framework also allows globally-recognised certification of the ISMS.

An ISMS based on the ISO 27001 standard adopts a holistic, structured and coordinated approach to identifying and managing information security risks. It involves consideration of issues of policy and procedure, technologies and tools deployed and most importantly, people and their behaviour.

NOTES

[illegible]


IMPLEMENTING AN ISMS

Module 5: ISO/IEC 27001:2013



IMPLEMENTING AN ISMS

ISO/IEC 27001

- Specifies the requirements for a formal Information Security Management System (ISMS)
 - Internationally accepted standard for the design, implementation and operations of an ISMS
 - Part of a family of information security management standards (ISO 27nnn)
- 

ISO 27001

ISO/IEC 27001 specifies the requirements for the implementation, operations and continual improvement of a formal Information Security Management System.

It is part of a broader family of standards relating to information security but forms the cornerstone of any formal security program in the ISO 27000 domain.

It is internationally recognised and formal certification to this standard is globally accepted.

History

- 1995 BS7799 – British standard published
- 1996 AS/NZS 4444 – Australia/New Zealand standard published (later AS/NZS 7799)
- 2005 ISO 27001 specification was published – contains Audit Requirements, with Controls aligned with ISO 17799
- 2007 ISO 17799 renumbered as ISO 27002:2005
- 2013 ISO 27001 and 27002 updated to reflect ISO Annex SL requirements and changing landscape
- 2015 AS ISO/IEC 27001:2015 published – identical to 2013 ISO standard

HISTORY OF ISO 27001

ISO 27001 began as a British standard BS 7799.2 in 1995. This standard outlined the requirements for an ISMS. This standard was the second part of the BS 7799 standard pair.

Australia adopted this standard in 1996 as AS/NZS 4444.2 and then renumbered it to AS/NZS 7799.2 in 2003. In 2005, an ISO version of the standard was released, which was adopted as AS/NZS ISO/IEC 27001:2006.

BS 7799.1 provided guidance and eventually became ISO 17799 and then in 2007, was renumbered to ISO/IEC 27002:2005 to align with ISO/IEC 27001:2005.

Both ISO 27001 and ISO 27002 were updated in 2013. An Australian version eventually followed in 2015 (AS ISO/IEC 27001:2015). Note that this is identical to the ISO version.

THE ISO 27000 SERIES

ISO 27001 is one of a series of standards in the ISO 27000 range. This set of standards is focussed on information security. Whilst ISO 27001 is the most recognised of the family, there are a number of standards in the range providing guidance and information.

The ISO 27000 family includes the following standards:

- 27000 – vocabulary and definitions
- 27001 – requirements
- 27002 – code of practice (replacing ISO 17799)
- 27003 – implementation guidance
- 27004 – ISM metrics and measurement
- 27005 – information security risk management
- 27006 – guide for accredited certification bodies
- 27007 – guidelines for auditing an ISMS.
- 27008 - guideline on auditing information security controls
- 27009 – sector specific application of ISO 27001
- 27010 – guideline on sector to sector communications
- 27011 – guidelines for ISMS for telecommunications organizations
- 27013 – ISMS and ITIL integration
- 27014 – Information Security Governance
- 27015 – ISMS for financial service organizations
- 27016 – information security economics
- 27017 – Security controls in the Cloud
- 27018 – Protection of PII in public clouds
- 27019 – Guidelines for process control systems
- 27031 – ICT focused standard on business continuity
- 27032 – guidelines for Cyber Security
- 27033 – guidelines for IT Network Security
- 27034 – guidelines for Application Security
- 27035 – guidelines for security incident management
- 27036 – guidelines for security of outsourcing, supply chain
- 27037 – guidelines for digital evidence (eForensics)
- 27038 – digital redaction
- 27039 – guidelines for intrusion prevention systems
- 27040 – guidelines for storage security
- 27041 – guidelines on incident investigative methods
- 27042 – guidelines for the analysis and interpretation of digital evidence
- 27043 – incident investigation principles and processes
- 27050 – Electronic discovery
- 27044 – guidelines for security information and event management
- 27102 – Cyber-insurance
- 27799 – guidelines for Healthcare sector

IMPLEMENTING AN ISMS

Note that a number of these standards are still in draft stages. Information about the current status of the standards can be found at

<http://www.iso27001security.com>

Also note that the ISO 31000 standard, whilst not formally part of the ISO 27000 family, plays a critical role in providing information about organisational risk management practices. Most organisations in Australia have adopted this standard as part of their Risk Management framework. The Queensland Government model has taken this approach.

ISO 27001 and ISO 27002

- A set of “paired” standards
- “Closely coupled” through Annex A of ISO 27001
- ISO/IEC 27001 defines the requirements for an ISMS which provides controls for *all* the information assets in scope, and the processes that touch them in a business
- ISO 27002 is a guidance document providing details on implementing the controls required by the ISMS

ISO 27001 and ISO 27002

ISO 27001 defines the requirements for an Information Security Management System. These requirements outline the steps for assessing risks and providing controls for *all* the information assets in scope of the ISMS.

The ISO 27001 standard uses ‘**Shall**’ within the text.,. All mandatory elements and selected controls are therefore mandatory.

ISO 27001 can be used for Third Party Audit and Certification.

ISO 27002 provides detailed guidance on implementing the controls required by an ISMS based on the ISO 27001 standard.

ISO 2701 and ISO 27002 are paired standards. ISO 27001 Annex A is derived from ISO 27002.

The Scope of ISO 27001

- The ISO 27001 standard outlines the requirements for establishing, implementing, maintaining and continually improving an ISMS ***within the context of the organisation***
- The context is defined as the environment in which the organisation seeks to achieve its objectives. It includes factors relating to both the external and internal context.
 - ISO 31000 provides further information on organisational context

THE SCOPE OF ISO 27001

The ISO 27001 standard outlines the requirements for establishing, implementing, maintaining and continually improving an ISMS ***within the context of the organisation***.

Context is defined as the environment in which the organisation seeks to achieve its objectives. Information to assist understanding an organisation's context is available in the ISO/IEC 31000 standard. It includes factors relating to both the external and internal context. Consideration needs to be given to all interested parties, both internal and external, and their security expectations or requirements.

ISO 27002

- This standard supplies additional information about the controls selected from Annex A of ISO 27001
- Language used within the standard is “should”
- Controls within ISO 27002 are not mandatory but are a reference control set
- Contains details on 114 controls aligned with Annex A
 - Implementation guidance
 - Other information on the controls

ISO 27002

Within ISO 27002 ‘**should**’ is used in the text. The use of this term differentiates this standard from ISO 27001. Controls listed in this standard are therefore “optional”. Use of this language makes this standard ineligible for use for certification purposes. It is a guideline only.

The objective and purpose of ISO 27002 is to provide guidance to those implementing an ISMS. It provides additional detail on the 114 controls listed in Annex A.

NOTES

[illegible]

Module 6: Structure of ISO 27001



IMPLEMENTING AN ISMS

Contents

1. Scope
2. Normative References
3. Terms and Definitions

- Clauses 4 – 10 are mandatory
- An ISMS based on ISO 27001 must contain all elements of these clauses
- Annex A provides a control set you should consider

CONTENTS

ISO 27001 comprises a number of clauses and one annexure. Within the standard clauses 4-10 are mandatory and any ISMS claiming conformance to ISO 27001 MUST implement all components of those clauses.

In addition, the standard contains Annex A. This annexure lists 35 control objectives and a set of 114 controls that may be applicable to the ISMS.

The mandatory clauses are:

4. Context of the Organization
 1. Understanding organization and its context
 2. Understanding third party needs and expectations
 3. Determining the scope of the ISMS
5. Leadership
 1. Commitment
 2. Information security policy
 3. Roles and responsibilities
6. Planning
 1. Addressing risks and opportunities
 2. Addressing information security objectives
7. Support
 1. Resources
 2. Competence
 3. Awareness

IMPLEMENTING AN ISMS

- 4. Communication
- 5. Documentation
- 8. Operation
 - 1. Planning and control
 - 2. Risk assessment
 - 3. Risk treatment
- 9. Performance Evaluation
 - 1. Monitoring and analysis
 - 2. Internal audit
 - 3. Management review
- 10. Improvement
 - 1. Nonconformity and corrective action
 - 2. Continual improvement

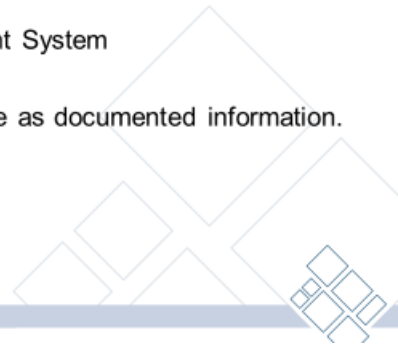
The relationship of the clauses to various stages in the design, implementation, operations and improvement of an ISMS are represented in the following table.

ISO 27001 Clause	ISMS Stage
Clause 4	Design
Clause 5	Design
Clause 6	Implement
Clause 7	Implement / Operate
Clause 8	Operate
Clause 9	Monitor / Improve
Clause 10	Improve

Details of ISO 27001:2013 Clauses

Clause 4. Context

- 4.1 Understanding the organization and its context
 - 4.2 Understanding the needs and expectations of interested parties
 - 4.3 Determining the scope of the information security management system
 - 4.4 Information Security Management System
- NOTE: The scope shall be available as documented information.



DETAILS OF CLAUSE 4

Clause 4 addresses the context of the organisation. Clauses 4.1 and 4.2 requires the consideration of internal and external issues that affect the organisations ability to achieve its intended security outcomes and to consider the requirements and expectations of interested parties. These requirements must include any legal, regulatory or contractual obligations.

Clause 4.3 then requires the scope of the ISMS to be defined and documented.

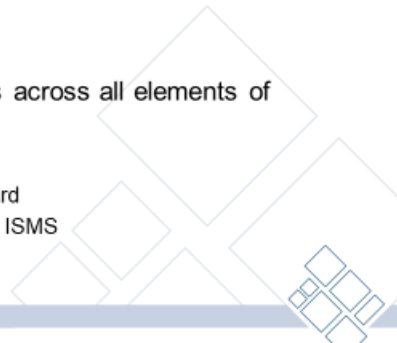
You need to consider what third parties (if any) are within scope.

Clause 4.4 requires a commitment by the organisation to establish, implement, maintain and continually improve an ISMS, in accordance with the requirements of ISO 27001.

Details of ISO 27001:2013 Clauses

Clause 5. Leadership

- 5.1 Leadership and commitment
 - Demonstrable
- 5.2 Information security policy
 - High level
 - Includes objectives
- 5.3 Roles and responsibilities
 - Defined roles and responsibilities across all elements of the ISMS
 - 2 more specific roles
 - Ensuring conformance to the standard
 - Reporting on the performance of the ISMS



CLAUSE 5 LEADERSHIP

Covered in Clause 5 are the issues of:

1. Commitment
2. Information security policy
3. Roles and responsibilities

Clause 5 requires commitment by “top” management, referring to executive levels of management. This clause addresses the issue of visible and demonstrable commitment to the implementation, operations and improvement of an ISMS. It is recognised that for an organisation to maintain their management system effectively, senior management must provide the commitment and guidance.

Usually, certification audits start with a Senior (Top) Management interview. Senior Management should be aware of the requirements of ISO 27001 and how their organisation has achieved conformance to the requirements of the standard.

Clause 5.2 addresses the requirement for the creation of a high-level information security policy. This policy document needs to:

- be appropriate to the purpose of the organisation;

- includes information security objectives or provide the framework for setting the information security objectives;
- include a commitment to satisfy applicable requirements related to information security; and
- includes a commitment to continual improvement of the ISMS.

This policy document needs to be approved by top management and circulated within the organisation and to any other interested parties, as appropriate.

Note that this policy requirement replaces the ISMS Policy required by ISO/IEC 27001:2005. The ISMS policy document is no longer required as a mandatory document but its purpose may still exist and therefore the document may still exist in that form.

Many organisations already have an information security policy document. This document needs to be examined to ensure that the requirements of the standard are included. If not, these requirements must be captured in a policy document approved by top management.

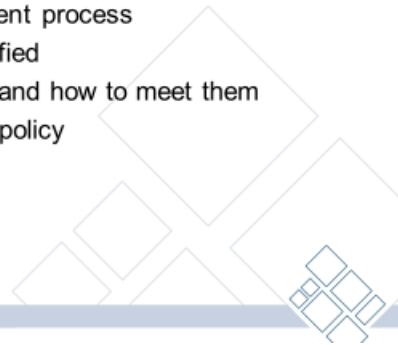
Clause 5.3 addresses ensuring the allocation of appropriate resources to the ISMS. It also explicitly addresses two specific roles. Responsibilities need to be assigned to roles to:

- Ensure compliance of the ISMS to the ISO 27001 standard;
- Report on the performance of the ISMS to top management.

Details of ISO 27001:2013 Clauses

Clause 6. Planning

- 6.1 Actions to address risks and opportunities
 - Requires risk assessment
 - Documents risk acceptance criteria
 - Documents when risk assessments will be done
 - Includes definition of risk treatment process
 - Also how opportunities are identified
- 6.2 Information security objectives and how to meet them
 - Must be consistent with security policy
 - How are they communicated?
 - What, who, when how?



CLAUSE 6 PLANNING

Covered in Clause 6 are:

- 6.1 Actions to address risks and opportunities
- 6.2 Information security objectives and how to meet them

Section 6 provides information on risk assessment and treatment, and also activities designed to continually improve the ISMS. It is a core clause supporting critical activities in relation to the implementation of an ISMS.

The first part of this clause captures the requirement to ensure that both corrective action (ensure event does not re-occur) and improvement (ensure event does not occur) activities are undertaken as part of continually improving the ISMS.

Note that this clause does not attempt to deal only with **negative** outcomes. The use of identified **opportunities** to ensure the ISMS can achieve its intended outcomes provides a focus on the positive aspects of good information security management.

Clause 6.1, also deals with the risk assessment process. This clause requires that a documented risk assessment process exists and that the criteria for performing the risk assessments has been identified.

This clause also mandates the documentation of the risk acceptance criteria.

The standard also requires the identification of the “risk owner”. The definition of the risk owner as per ISO 31000 is the “person or entity with the accountability and authority to manage a **risk**”. This person or entity may not be charged with any risk remediation activity but is the individual or entity who is accountable to top management in terms of ensuring proper management of the risk.

Clause 6.1 also addresses control selection, the creation of the Statement of Applicability, acceptance of risk by the risk owner and approval of risk treatment plans.

Again, the standard requires the retention of documented information about the risk treatments. This may exist in documentation such as risk treatment plans or risk registers or may be contained within a risk management tool.

ESTABLISHING SECURITY OBJECTIVES AND REQUIREMENTS?

Clause 6.2 identifies the need to document the information security objectives.

It is critical that the organisation identifies its security requirements. There are three main sources of security requirements:

- a) the assessment of risks, taking into account the organisation’s overall business strategy and objectives;
- b) the legal, statutory, regulatory and contractual requirements that an organisation, its trading partners, contractors and service providers have to satisfy;
- c) the set of principles, objectives and business requirements for information handling, processing, storing, communicating and archiving that an organisation has developed to support its operations.

Defining information security objectives can be a difficult process. A common way of addressing this is by linking the objectives to the strategic intent of the statements within the high-level information security policy document. This document generally outlines the core security strategies and is commonly the

IMPLEMENTING AN ISMS


link between the organisation's business strategies and the implementation of security initiatives.

So, an organisation's security objectives must consider the following:

- The business requirements for information processing. These requirements should be derived from a number of sources, both internal and external, but should include the business strategies of the organisation.
- Any and all legal, statutory, contractual and regulatory requirements
- The security requirements of customers, suppliers and other third parties
- Requirements contained in applicable standards and frameworks

Details of ISO 27001:2013 Clauses

Clause 7. Support

- 7.1 Resources required to establish and operate an ISMS
 - 7.2 Competency
 - 7.3 Awareness
 - 7.4 Communication
 - 7.5 Documented Information
-
- All personnel within scope of the ISMS should be competent in their roles
 - Evidence of competency is required
- 

CLAUSE 7 SUPPORT

This clause of the standard provides the requirements supporting the establishment and operations of an ISMS. Included in Clause 7 are:

- 7.1 Resources required to establish and operate an ISMS
- 7.2 Competency
- 7.3 Awareness
- 7.4 Communication
- 7.5 Documented Information

Clause 7 provides information on selection and allocation of resources to implement and operate an ISMS, and the requirements for ongoing awareness for all person's performing work within scope of the ISMS and under the organisation's control. Clause 7.2 requires all persons to be competent in their roles within the ISMS. Competency comes about through the provision of training, education, experience and skills. These are all to be considered in the management of human resources.

There is a logical sequence that is reflected within this clause of the standard when addressing competency:

- Determine the necessary competency requirements

IMPLEMENTING AN ISMS

- Provide training or other actions to fill any gaps, considering past qualifications and experience. This may include recruiting.
- Evaluate the effectiveness of the training or actions
- Maintain records of education, training, skills, and experience, etc.

The need for people to be aware of their ISMS responsibilities is contained within Clause 7.3. This generally will drive some level of training and awareness sessions targeting different audience groups. Awareness of non-conformance to the requirements of the ISMS must also be addressed.

Clause 7.4 deals with communications, a topic covered in depth later.

Clause 7.5 addresses the requirements relating to maintaining the relevant documents and records that support the operations of the ISMS. Formal records of document approval demonstrate conformance with this clause.

Details of ISO 27001:2013 Clauses

Clause 8. Operations

- 8.1 Operational planning and control
- 8.2 Information security risk assessment
 - At planned intervals
 - Significant changes
- 8.3 Information security risk treatment



CLAUSE 8 OPERATIONS

This clause of the standard defines the requirements necessary to operate an ISMS. They include the following key elements:

- 8.1 Operational planning and control
- 8.2 Information security risk assessment
- 8.3 Information security risk treatment

Clause 8.1 requires demonstration of processes controlling critical security-related activities. Some mechanisms to assist with conformance to this subsection include:

- The use of documented security plans or security calendars;
- Monitoring and controlling changes to the environment;
- Implementing controls around third-party outsourcing arrangements.

Clause 8.2 requires risk assessment to be performed when significant changes occur **or are proposed**. In addition, this clause requires review of the risk assessments at planned intervals. In a practical sense, this usually is performed annually and is tracked by an activity in the security calendar. Evidence of the output of such planned risk reviews must be available.

Clause 8.3 requires risk treatments to be implemented and monitored.

Details of ISO 27001:2013 Clauses

Clause 9. Performance Evaluation

- 9.1 Monitoring, measurement, analysis and evaluation
 - Identifying what to monitor/measure
 - Don't need to measure everything
- 9.2 Internal audit
 - At planned intervals
- 9.3 Management review
 - Also at planned intervals
 - Usually after the ISMS Internal Audit



CLAUSE 9 PERFORMANCE EVALUATION

This clause of the standard provides the requirements for the assessment of the performance of the ISMS. It includes the requirements for:

- 9.1 Monitoring, measurement, analysis and evaluation
- 9.2 Internal audit
- 9.3 Management review

ISO 27001 does not require you to measure everything. An organisation must determine the following:

- a) what needs to be monitored and measured, including processes and controls;
- b) the methods for monitoring, measurement, analysis and evaluation, to ensure valid results;
- c) when the monitoring will happen;
- d) who shall perform the activity;
- e) when the results will be analysed; and
- f) who shall do this.

Clause 9.2 of the standard specifies the requirements for ISMS Internal Audit.

Key considerations are:

- They occur at planned intervals;
- That the auditor selected will be objective and impartial. Generally, this means the ISMS cannot be audited by persons involved in its implementation or operations.

ISMS internal audits must be conducted to determine the status of the system. The organisation needs to plan audits, taking into account the most important aspects of the business, then conduct the audits using competent staff.

Note that an ISMS audit does not need to cover off all elements of the ISMS during the audit. An ISMS audit program is produced which may contain a number of audits. The audit program must ensure that all elements of the system are reviewed.

NOTE: ISO 27007, ISO TR 27008 and ISO 19011:2002 (Guidelines for quality and/or environmental management systems auditing), will provide helpful guidance for carrying out the internal ISMS audits.

Clause 9.3 addresses the need for a Management Review. This occurs at planned intervals, generally after the completion of the ISMS Internal Audit.

The standard explicitly defines the minimum inputs into the Management Review. These include:

- 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:
 - a. nonconformities and corrective actions;
 - b. monitoring and measurement results;
 - c. audit results; and
 - d. fulfilment of information security objectives;
- d) feedback from interested parties;
- e) results of risk assessment and status of risk treatment plans; and
- f) opportunities for continual improvement.

Outputs include recommendations for improvements and any identified changes to the ISMS.

These reviews by management are conducted for the purposes of ensuring the ISMS is operating as expected. These reviews are often performed by the governance forum of the ISMS.

Details of ISO 27001:2013 Clauses

Clause 10. Improvement

- 10.1 Nonconformity and corrective action
 - Correcting weaknesses in the ISMS
 - Correcting non-conformances with the standard, policies etc
- 10.2 Continual improvement
 - Fundamental objective of ISO 27001
- By design, the ISMS should improve by utilising mechanisms to detect weaknesses or failures



CLAUSE 10 IMPROVEMENT

Clause 10 of the standard specifies the requirements for improving the ISMS. An effective ISMS contains a number of elements that assist with the aim of continually improving the operations of the management system. Such elements include identifying areas of non-conformity with the standard or the organisation's own policies and procedures and taking any necessary actions to correct the non-conformance. This is addressed in Clause 10.1

Clause 10.2 addresses the requirement for continual improvement of the ISMS. Improvement of the ISMS will occur provided all of the previous requirements of the standard have been implemented and are working effectively. Evidence of such improvements should be maintained.



ACTIVITY 2: ISMS Stages and Documentation

OBJECTIVE

To identify required documentation from the mandatory clauses (Clauses 4-10) of the standard.

TIME

10 minutes

TASK

- In your teams identify 4 core documents/documentation required by ISO 27001 and the relevant clause that specifies that requirement.

NOTES


[illegible]

Module 7: ISMS Design and Implementation



IMPLEMENTING AN ISMS

Key Activities

1. Gain commitment
 2. Identify and document scope
 3. Build governance framework
 4. Obtain the necessary resources and competencies
 5. Identify the targets for risk assessment (information assets)
 6. Document risk approach
 7. Perform Risk assessment, select treatment options and controls and get approved
 8. Build the Statement of Applicability
 9. Build documentation control processes
 10. Deliver training
 11. Identify metrics and improvement mechanisms
- 

KEY ACTIVITIES

Implementing an ISMS is a reasonably linear process and follows clauses 4-8 closely. Some activities however, can be performed in parallel, including building documentation control, internal audit and management review procedures.

A sample project plan is provided for an ISMS implementation. Note that the timings will be affected by the size and complexity of the agency, the availability of resources, the scope of the ISMS and external factors affecting timing.

NOTES

[illegible]

Module 8: ISMS Scope



IMPLEMENTING AN ISMS

The Scope of the ISMS

- Important in that it determines:
 - Physical boundaries
 - Logical boundaries
 - “Interested parties”
 - Exclusions
- Scope allows us to focus on critical information assets for the risk assessment stage



ISMS SCOPE

A very important element of the ISMS is its scope. The scope will be used for identifying the targets of the risk assessments and thus supports the remaining elements of the ISMS. As the agency is required to implement an ISMS based on the international standard, it must define the scope of the ISMS.


Note that it is not necessary to implement the same level of security for the whole agency.

One reason for the failure of an ISMS implementation is a poorly defined scope.

Whatever the scope, a formal documented definition of the scope of the ISMS is required (clause 4.3).

Defining Scope

Steps in defining scope

1. Understand organisational objectives –what's important
 2. Identify “interested parties” and their security requirements/interests/concerns
 3. Identify legal/regulatory/contractual requirements
 4. Identify “logical boundaries”
 5. Identify “physical boundaries”
 6. Consider exclusions
 7. Create scope
- 

Considerations when assembling the ISMS scope are:

- What are the objectives for the ISMS?
- What does the agency do?
- Who is concerned about information security?
 - The agency
 - The Queensland Government
 - Who are the other interested parties?
 - Customers?
 - Any regulators?
- What are their security requirements and expectations?
- What is important and needs protecting?
 - E.g. intellectual property, customer records
- What is the physical scope?
 - Locations or facilities covered by the ISMS
- Are there any logical boundaries?
 - Are all business units included in the ISMS?
- Are service providers included?
- Are there any exclusions?

Exclusions may occur when the agency has limited or no management control across that area, making it difficult to manage any risks.



ACTIVITY 3: Constructing the Scope

OBJECTIVE

To identify some of the key elements of the ISMS scope.

TIME

20 minutes

TASK

- In your teams, attempt to capture (in bullet point form) the key elements of a scope statement for your agencies
 - Core objective(s)
 - Interested parties
 - Boundaries
 - Exclusions

NOTES

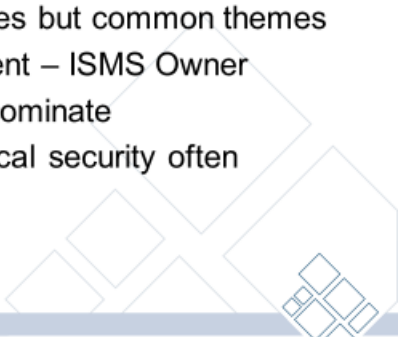
[illegible]

Module 9: ISMS Governance



IMPLEMENTING AN ISMS

Governance

- ISMS is an organic system, requires “care and feeding”
 - Fed by risk, improvements, incidents, corrective actions
 - Care provided by management commitment - governance
 - Many different governance choices but common themes
 - Involvement of senior management – ISMS Owner
 - IT has a presence but does not dominate
 - Human resources, risk and physical security often involved
- 

Governance

The governance forum (steering committee, security committee etc) plays a vital role in the ongoing health of the ISMS. This committee has oversight of the key activities, risk treatments and changes to the management system.

Membership of the governance forum should be carefully considered and should not be dominated by ICT.

Including groups such as human resources, corporate communications, operational risk management and facilities does provide significant value to the ISMS.

The ISMS Owner is usually the chair of this forum.

Sample Agenda Items

- Oversight of progress against risk treatments, slippages, resource or priority issues
 - Action against non-conformances
 - Review of the responses to major security incidents
 - Assessment of progress against key security initiatives
 - Monitoring status of activities in the security/compliance calendar
 - Reviewing key security metrics/dashboard
- 

AGENDA CONSIDERATIONS

The governance forum operates from a standard agenda. Items on such an agenda can include:

- Consideration of any new “in-scope” assets & associated risks
- Review of the current items in the Improvements & Actions Register against delivery dates
- Review of the items in Risk Register against delivery dates
- Review of major security incidents and the response
- Review of the status of ISMS security calendar activities for the current period plus those due in the next period
- Review of measures and metrics on the performance of the ISMS

The review of the metrics should be focussed on the review of a limited number of metrics. These metrics are generally those that executive and senior management have a strong interest in. These metrics may form the elements of security dashboards for reporting to audit committees and executive forums.



ACTIVITY 4: Brainstorming forum membership

OBJECTIVE

To identify potential members for the ISMS governance forum.

TIME

15 minutes

TASK

As a group, discuss the possible membership that may be valuable within the governance forum.

Discuss benefits and challenges.

NOTES


[illegible]

Module 10: Resourcing



IMPLEMENTING AN ISMS

Key Considerations

- The ISMS Owner
 - Membership of the governance forum
 - Resources required as part of the ISMS implementation team
 - Roles and responsibilities for the ongoing operations of the ISMS
 - ISMS internal auditor
 - Responsibilities for reporting conformance to the standard
 - Responsibilities for reporting to executive management on the performance of the ISMS
- 

RESOURCING CONSIDERATIONS

One critical success factor for an ISMS implementation is having access to the right resources at the appropriate time. Remember that each person fulfilling a role within the ISMS is required to be competent in that role. It is therefore important to remind yourself of the core roles and consequently the core resources you will require. This applies to both the implementation and operations of the ISMS.

Core roles will likely include:

- The ISMS Owner. Usually a very senior manager.
- The members of the governance forum, whatever label it is given.
- The person responsible for information security management within the agency.
- Those responsible for various operational activities affecting information security. This includes operational support personnel such as server and network support teams, service desk personnel and human resource management staff.
- The ISMS Internal Auditor
- The role charged with the responsibility to ensure the ISMS conforms to the standard.
- The role charged with reporting the performance of the ISMS to executive management.

Resourcing Questions

- Do we know what competencies we need?
- Do we have these competencies available?
- If not, can we obtain by recruiting?
- Short term, can we contract them in?
- Longer term, what training and development is required internally to ensure we maintain the necessary competencies?



RESOURCING QUESTIONS

There are a number of questions that need to be posed and answered during implementation planning.

These questions primarily relate to ensuring the appropriate competencies are available when required. They include questions around documenting the required competencies, identifying the existing competency set and developing possible strategies for addressing any competency gaps.

Gaps are generally addressed by:

- Hiring – obtaining permanent resources with the right competency set;
- Buying in short-term contract resources;
- Developing competencies “in house” through training and mentoring.

Decisions about these choices will depend on the extent of the competency gap and whether the competencies are required for implementation or ongoing operation of the ISMS.

Module 11: Information Asset Identification



IMPLEMENTING AN ISMS

Asset Identification

- ISO 27001 does not require this to occur before risk assessment is performed
- Benefit of doing this early – provides clear targets for risk assessments
- Is required by Annex A.8.1.1 control, so this will need to be done at some stage
- Requires asset owner to be identified who may also be the risk owner

INFORMATION ASSET IDENTIFICATION

Whilst the latest version of ISO 27001 does not require you to identify assets before undertaking risk assessments, it is often a good strategy to provide clarity around the risk targets. This will allow a more focussed approach to risk assessment.

Note that Annex A.8.1.1 still requires the creation of an information asset inventory. Ownership of assets must also be identified as part of Annex A.8.1.2.

This Information Asset inventory should not be confused with any fixed asset registers. They serve different purposes.

Asset Identification

A process for identifying assets

- Start with the critical business functions
- Identify the information used to support that function and its value
- Identify the “supporting assets” needed to use this information effectively
 - Applications
 - Databases
 - Servers
 - Networks
 - Support facilities
 - People



INFORMATION ASSET IDENTIFICATION

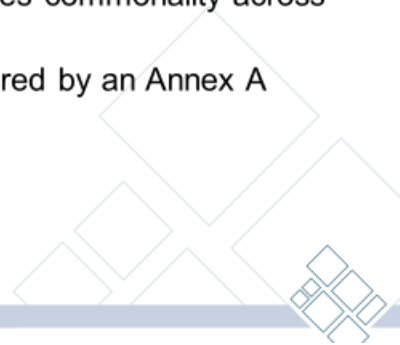
There are a number of ways of identifying critical information assets. It is possible that such a list of assets already exists as an outcome of a Business Impact Analysis activity driven by the Business Continuity Management program.

However, if no such list is available, the following method may be applied:

1. Identify the critical business processes within scope. For most agencies, this will be all their critical processes given the expected broad nature of the scope of the agency's ISMS;
2. Identify the core (primary) information required by each process. This will be information such as financial information, health records, citizen information;
3. Identify all the supporting (secondary) assets that are required to allow access to this information. Such supporting assets will include all necessary ICT and physical infrastructure and also include the human assets required;
4. Identify the information asset owners for all assets;
5. Discuss and agree the value of the asset with the owners. This can use the information classification framework discussed next.

Information Classification

- Need to understand the importance of the information
- In broad terms, what is important and what is less important
- Queensland Government have an information classification scheme that provides commonality across government
- Information classification is required by an Annex A control (A.8.2.1)



INFORMATION CLASSIFICATION

Classifying information is one of the more challenging tasks within an ISMS implementation. Often, organisations find it too complex and abandon both it and the project.

Using the “keep it simple” principle, it may be worth considering an approach where only the sensitive or high value assets are formally classified. Other asset categories can be placed into classification “buckets” in the short term.

All state governments and the Commonwealth Government have adopted information classification schemes. These are generally aligned but due to timing issues they are not always consistent at any given moment.

The Queensland Government classification scheme is documented in the Queensland Government information security classification framework.

Link: [Queensland Government information security classification framework](#)



ACTIVITY 5: Building an Information Asset Register

OBJECTIVE

To build a brief information asset register for your agency, identifying information owners and value.

TIME

20 minutes

TASK

Individually, use the template provided to capture 3 critical information assets for your agency.

- Identify possible owner
- Identify possible value (low, moderate, high)

Prepare to discuss as a group

NOTES

[illegible]

NOTES

[illegible]

Module 12: Risk Assessment



IMPLEMENTING AN ISMS

Risk Assessment

- Fundamental part of an ISMS
- Needs to address risks and opportunities
- Standard requires the following:
 - Process must be defined (6.1.2)
 - Includes criteria for accepting or treating risks (6.1.2.a)
 - Includes criteria for performing risk assessments (6.1.2.a)
 - Risk assessments produce consistent, valid and comparable results (i.e. repeatable risk assessment method) (6.1.2.b)
 - Review risk assessments at planned intervals (8.3)

RISK ASSESSMENT

Given that ISO 27001 is inherently a risk management standard it is no surprise that there are a number of specific clauses addressing this area.

The clauses and the expectations outlined in the standard are:

- **Process must be defined (6.1.2)**

The standard does not dictate specific methods for risk assessment. It is up to the organisation to select a method that aligns with the organisational risk methodology. However, consequence and likelihood must be considered.

ISO 27001 references ISO 31000 as a risk standard.

Queensland Government follows the ISO 31000 organisational risk framework

- <https://s3.treasury.qld.gov.au/files/guide-to-risk-management.pdf>
 - **Established and maintains information security risk criteria that includes the risk acceptance criteria and criteria for performing information security risk assessments (6.1.2 (a))**

Management must determine and approve criteria for accepting the risk. For example, an organisation may say “We will accept all risks in the ‘low’ category and treat those rated above this value”.

Management must also determine the criteria for performing risk assessments. This may include consideration of risk assessments during projects, significant changes, as a result of incident reviews or as an outcome of business continuity exercises.

Criteria may also be based on the value of the information assets involved. For instance, highly sensitive assets may automatically require a risk assessment around any changes on how those assets are used.

- **Risk assessments produce consistent, valid and comparable results (i.e. repeatable risk assessment method) (6.1.2 (b))**

The process of risk assessment should be documented. People undertaking risk assessments must be competent to perform these activities. Training may be required.


A general “rule of thumb” regarding “producing consistent, valid and comparable results” should be “if two people of similar competence undertake the same risk assessment the results will be comparable (not necessarily identical)”.

- **Review risk assessments at planned intervals (8.2)**

Risk assessments should also be performed at planned intervals to address changes in the security requirements and in the risk situation, e.g. in the likelihood or consequences of previously identified risks and also when significant changes occur or are planned.

Risk Assessment

A sample method for Risk Assessments

- Identify the critical processes within scope
 - Identify the information assets required
 - Consider threats (agencies that could cause loss) against the asset
 - Identify vulnerabilities (weaknesses exploited by threat)
 - Assess consequences to agency if the threat occurs
 - Assess realistic likelihood of risk eventuating
 - Determine risk rating
 - Compare against acceptance criteria
 - Determine treatment options if required
 - Monitor treatment implementation
- 

STEPS IN A SAMPLE RISK ASSESSMENT METHOD

1. Identify the critical processes within scope
2. Identify the information assets required
3. Consider threats (agencies that could cause loss) against the asset
4. Identify vulnerabilities (weaknesses exploited by threat)
5. Assess consequences to agency if the threat occurs
6. Assess realistic likelihood of risk eventuating
7. Determine risk rating
8. Compare against acceptance criteria
9. Determine treatment options if required
10. Monitor treatment implementation
11. Repeat from step 1

Note that the standard does not require you to adopt this approach. In fact, as previously discussed, the standard does not require you to identify the information assets before undertaking the risk assessment.

Example likelihood table

Level	Descriptor	Description
5	Near certain	Is expected to occur in most circumstances. Could occur within 'days to weeks'
4	Highly Likely	Will probably occur in most circumstances. Could occur within 'weeks to months'
3	Likely	Could occur 'within a year or so'
2	Unlikely	Could occur but not expected. Could occur 'after several years'
1	Remote	Occurs only in exceptional circumstances. A '100 year event' or greater

MEASURES OF LIKELIHOOD

Tables similar to the one below are often seen within risk models. One consideration should be if the timeframes within these types of tables are appropriate for assessing information security risks. One challenge related to the use of a single likelihood table for all types of risk has been the relevance to information security events.

Use of single likelihood tables across an organisation have been known to skew risk values related to security risks down.

Level	Descriptor	Description
5	Near certain	Is expected to occur in most circumstances. Could occur within 'days to weeks'
4	Highly Likely	Will probably occur in most circumstances. Could occur within 'weeks to months'
3	Likely	Could occur 'within a year or so'
2	Unlikely	Could occur but not expected. Could occur 'after several years'
1	Remote	Occurs only in exceptional circumstances. A '100-year event' or greater

Likelihood should take into account the effectiveness of the current control environment.

Example consequence table

Rating		Area of Impact			
		Financial	Customer service /business continuity	Regulatory/legal	Reputation/image
Catastrophic	5	Financial loss greater than \$5m	Loss of service capacity for more than 1 week	Significant legal, regulatory or internal policy failure	Severe difficulties leading to sustained adverse business press and brand damage
Critical	4	Financial loss \$500k to \$1m	Loss of service capacity between 1 day and 1 week	Major legal, regulatory or internal policy failure	Sustained difficulties identified in industry blogs
Marginal	3	Financial loss \$100k to \$500k	Loss of service capacity between 1 hour and 1 day	Limited legal, regulatory or internal policy failure	Matter raised in trade press or industry blogs
Minor	2	Financial loss \$25k to \$100k	Loss of service capacity between 15 minutes and 1 hour	Minor legal, regulatory or internal policy failure	Some press mention - senior management required to resolve
Negligible	1	Financial loss less than \$25k	Loss of service capacity for less than 15 minutes	Insignificant legal, regulatory or internal policy failure	Resolved through day-to-day management

MEASURES OF CONSEQUENCE


It is more common to use a single consequence table across the organisation. For this to be practical, the consequence (or impact) domains must represent all possible areas of impact across the risk portfolio.

The more detailed the information in the consequence table, the more likely that a comparable value will be selected during risk assessments.

Note that there may be consequences in a number of impact areas. The risk assessor should select the highest impact value.

Risk Ratings – Example table

Likelihood	Near Certain	Low	Medium	High	High	High
	Highly Likely	Low	Medium	Medium	High	High
	Likely	Low	Low	Medium	Medium	High
	Unlikely	Low	Low	Low	Medium	Medium
	Remote	Low	Low	Low	Low	Low
		Negligible	Minor	Marginal	Critical	Catastrophic
		Consequence				



MEASURES OF RISK

Once the consequence and likelihood have been assessed, generally there is some form of lookup table to determine the risk value. This risk tables may look similar to that above, although sometimes the axes are transposed or the scales on the axes are transposed.

Note that likelihood assessment may include business and control owners and consequence assessment will certainly include the business owner.

The risk value obtained from the risk assessment will be used to determine whether further risk treatment is required.

Risk Assessment

- Why not do risk assessment against ALL assets?
- A question of return on the time investment required
- The assets not specifically included in the detailed risk assessment will be protected by a set of minimum baseline controls (policy requirement 3)
- Example:
 - Unique user names and passwords protecting against risks related to unauthorised access - applies across asset groups



DETAILED RISK ASSESSMENT

A question is often posed that if ISO 27001 is about risk management, why do we not do risk assessments against all in-scope assets? This is fundamentally a question on practicality. Few organisations have enough competent resources to undertake such an intensive program.

In addition to resources, there is a question of exposure. During the time taken to conduct such risk assessments, the organisation is exposed to potentially high risks.

The most common approach is to perform detailed risk assessments on “high value” assets and have the risks to those assets of a lower value managed by sets of baseline controls. These controls are the minimum set of controls to provide appropriate protection.

For Queensland Government agencies, this minimum control set is outlined in Policy Requirement 3.



ACTIVITY 6: Risk Assessment

OBJECTIVE

To undertake a high-level risk assessment, focussing on consequence and likelihood.

TIME

30 minutes

TASK

As a group, use the template provided to assess the risks against one of the information assets identified previously

NOTES

[illegible]

NOTES

[illegible]

Module 13: Risk Treatment



IMPLEMENTING AN ISMS

Risk Treatment

- Risks that have a rating ABOVE the risk acceptance criteria must be treated
- Treatment options
 - Accept the risk
 - sign-off based on the risk management policy
 - Avoid the risk
 - by ceasing the activity that creates the risk
 - Transfer the risk
 - Particularly if consequence is financial, then insurance is an effective treatment
 - Mitigate the risk with additional controls

RISK TREATMENT

Once the risk assessment has been concluded and the risk is rated, the rating is compared to the agreed risk acceptance criteria.

If the risk rating is greater than the acceptable level of risk treatment options need to be considered.

There are four alternatives for risk treatment. These are:

1. Mitigating the risk by applying additional appropriate controls;
2. Knowingly and objectively accepting the risk, providing this clearly satisfies the organisation's risk management policy in terms of the levels of authorisation required to accept risks above the defined risk acceptance criteria;
3. Avoiding the risk by avoiding or terminating the activity that creates the risk; and,
4. Transferring the associated business risks to other parties, e.g. insurers.

Transference of risk is an effective choice when the impact from this risk is financial in nature. For instance, insuring against loss from an environmental event such as a flood reduces the financial impact on the organisation.

IMPLEMENTING AN ISMS

Some believe that outsourcing is a form of risk transference. However, the question remains “who suffers the most impact?”. Generally, it is not the outsourcer’s business that is most affected. Outsourcing transfers some of the operational aspects of risk mitigation to the outsourcer but it still remains the organisation’s risk to manage.

If the treatment choice is “mitigate” with additional controls, what control sets should be considered? As with the existing control environment, the standard does not mandate any specific set.

Possible control sets include:

- ISO 27002 (ISO 27001 Annex A)
- PCI-DSS for credit card security
- Australian Government’s Information Security Manual (ISM)
- NIST frameworks
- Other ISO 27nnn standards
- Unique controls designed by the organisation

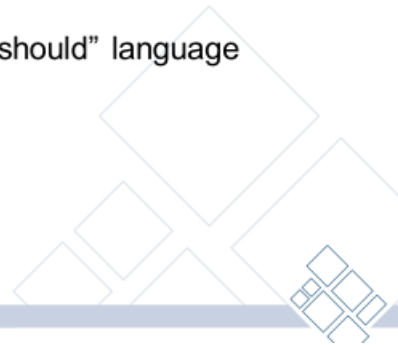
Remember that after the risk treatment has been determined, you need to reassess the ‘likelihood’ and “consequence” and calculate the measure of residual risk.

At the conclusion of the control selection process, the control objectives and controls selected need to be compared to the control objectives and controls from Annex A to ensure that no necessary controls have been omitted.

Note that the risk owner **MUST** approve the risk treatments selected and also must accept any residual risk. This must be documented.

ISO 27001 / ISO 27002

- Annex A is directly derived from ISO 27002
- Control references in Annex A can be mapped back
- Example:
 - ISO 27001 Annex A.5.1.1 \equiv ISO 27002 5.1.1
- Only difference is the “shall” vs “should” language
- 114 controls in both documents



ISO 27001 AND ISO 27002

As mentioned previously, these are a “paired” set of standards.

Annex A of ISO 27001 is derived directly from ISO 27002. The only difference is in the use of “shall” and “should”.

There are 35 control objectives and 114 controls in the 2013 versions of these standards.


There is a one-to-one relationship between each control in Annex A and ISO 27002. The mapping works as follows:

Annex A.x.x.x additional information is contained in 27002 section x.x.x

For example, the Annex A control A.5.1.1 relating to organisations and their security policies is supported by ISO 27002 section 5.1.1. This section provides additional implementation guidance.

Note again that the control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may be selected from any source.

ISO 27001 Annex A

- A.5 Information security policies
 - A.6 Organization of information security
 - A.7 Human resource security
 - A.8 Asset management
 - A.9 Access control
 - A.10 Cryptography
 - A.11 Physical and environmental security
 - A.12 Operations security
 - A.13 Communications security
 - A.14 System acquisition, development and maintenance
 - A.15 Supplier relationships
 - A.16 Information security incident management
 - A.17 Information security aspects of business continuity management
 - A.18 Compliance
- 

ISO 27001 ANNEX A

As mentioned, Annex A of ISO 27001 contains 35 control objectives and 114 controls. These are contained in 14 domains and address ICT and non-ICT controls. Annex A provides a consistent and globally recognised control set.

The 14 domains are:

- A.5 Information security policies
- A.6 Organization of information security
- A.7 Human resource security
- A.8 Asset management
- A.9 Access control
- A.10 Cryptography
- A.9 Physical and environmental security
- A.12 Operations security
- A.13 Communications security
- A.14 System acquisition, development and maintenance
- A.15 Supplier relationships
- A.16 Information security incident management
- A.17 Information security aspects of business continuity management
- A.18 Compliance



ACTIVITY 7: Control Selection

OBJECTIVE

To identify controls from a control source to manage risks.

TIME

30 minutes

TASK

As a group, reference the risks previously identified.

- Consider what existing controls are managing the risk
- What other controls may assist?

NOTES

[illegible]

Module 14: The Statement of Applicability

Statement of Applicability

- Mandatory document required by ISO 27001 (Clause 6.1.3)
- Standard requires that you:
 - Identify control objectives, controls selected, reasons for selection (from whatever source)
 - Compare the controls selected against Annex A (for completeness)
 - Document the controls selected in a Statement of Applicability
- The SoA must contain at least the 114 controls listed in Annex A (even if they are not selected)
- It describes the control environment of the ISMS

THE STATEMENT OF APPLICABILITY

The Statement of Applicability (commonly called the SoA) is a critical document required by ISO 27001. It effectively documents the control environment of the ISMS.

It is built from the results of the risk assessments and risk treatments, so is composed both of controls that are already implemented and those controls contained in risk treatments.

The template used is based in Annex A.

You are required to compare these selected controls against Annex A to ensure no areas have been missed.

Statement of Applicability

Must document:

- The control objective, control and reason for selection
- The implementation status of the control
 - E.g. Implemented if it is existing control
 - E.g. Not yet implemented if it is a control related to a risk treatment
- Whether the control is applicable to the ISMS or not
- The reason for exclusion for any Annex A control not applicable
 - Could have a better control or no risks in that domain

THE STATEMENT OF APPLICABILITY (continued)

The SoA must contain the following information:

- The control objective, the control information and the reason that control has been selected. This reason may be risk-related or even compliance related. Generally, there is always some associated risk;
- The implementation status of the control. If it is an existing control this status is likely to be “implemented”. If the control forms part of a risk treatment not already applied, the status may be “Not yet implemented” or words to that effect. Often the SoA also contains details on how the control is implemented;
- Whether the Annex A control is applicable to this ISMS or not. Some controls may not apply because that domain is outside the scope of the ISMS. For instance, controls in A.14 relating to systems development may not apply because the organisation does not have any development functions. Another reason for excluding a control is that a more effective control has been selected;
- The reason for exclusion for any Annex A control that has been assessed as “not applicable”.

Any controls from other controls sets also must be documented in the SoA.

Statement of Applicability

The SoA

- Is linked to the certification process and the certificate
- Is often “paired” with the Risk Register
 - Controls are only implemented to manage risk
- Is a core audit document
 - Both for planning and conducting and ISMS audit
- Sample SoA template

[QGCIO Sample SoA annd Essential 8.xlsx](#)



THE STATEMENT OF APPLICABILITY (continued)

The ISMS certification process and the certificate itself is linked to a particular version of the SoA. Therefore, if there is a change in the number of controls, the certified organisation should prepare a new SOA and have the certificate reissued.

The SoA is derived from the output of the risk assessment/risk treatment process and therefore is often linked to the risk register.

When planning an audit and selecting the audit team, the SoA is important to facilitate the development of the audit plan and to ensure appropriate audit resources are selected.

Remember, in an ISMS based on ISO 27001, clauses 4 – 10 are mandatory. However, all the 114 controls in Annex A are not. Therefore, the SoA indicates which of these controls are required and why.

QGCIO has a sample template available. It can be found at:

[QGCIO Sample SoA annd Essential 8.xlsx](#)



ACTIVITY 8: SoA Creation

OBJECTIVE

To understand the required elements of the Statement of Applicability.

TIME

15 minutes

TASK

In your teams, using the SoA template provided, complete the relevant rows for the controls previously selected

NOTES

[illegible]

Module 15: Documentation



Mandatory Requirements

• ISMS Scope	4.3
• High level information security policy	5.2
• Risk Assessment Methodology	6.1.2
• Risk Assessment Report and Risk Treatments	6.1.2/3, 8.2, 8.3
• Statement of Applicability	6.1.3 d)
• Information security objectives	6.2
• Evidence of competencies	7.2
• Documented information as required by the ISMS	7.5.1 b)
• Documents and records required by ISO 27001	7.5.1 a)
• Monitoring and measurement results	9.1
• Internal audit program and results	9.2
• Results of management review	9.3
• Non-conformances and results of corrective action	10.1

DOCUMENTATION

Throughout clauses 4 -10 there are references to required documentation. This documentation, both documents and records, and the related clauses are:

Name	Clause	Documentation type
ISMS Scope	4.3	Document
High level information security policy	5.2	Document
Risk Assessment Methodology	6.1.2	Document
Risk Assessment Report and Risk Treatments	6.1.2, 6.1.3, 8.2, 8.3	Record
Statement of Applicability	6.1.3 d)	Document
Information security objectives	6.2	Document
Evidence of competencies	7.2	Record

IMPLEMENTING AN ISMS

Name	Clause	Documentation type
Documented information as required by the ISMS	7.5.1 b)	Documents and Records
Documents and records required by ISO 27001	7.5.1 a)	Documents and Records
Monitoring and measurement results	9.1	Record
Internal audit program and results	9.2	Record
Results of management review	9.3	Record
Non-conformances and results of corrective action	10.1	Record

The difference between a document and a record: records are evidence of an activity at a point in time. Documents are reviewed and updated on a periodic basis. They are usually versioned.

Apart from the record types listed above, other useful records may include:

- Management decisions – e.g. evidence of the risk owner's approval for selected controls or acceptance of risk;
- Visitor's logs, access logs and CCTV images;
- Records of security incidents, root cause analysis, corrective actions and improvements.

Documentation

Documentation should be:

- “fit for purpose”
- constructed with the audience in mind
- well-managed (clause 7.5)
- suited to the agency, its size, internal competencies and culture
- should say what you do and then you need to do what you say!

The standard does not require you to formally document everything

DOCUMENTATION

Documentation is important to ensure that processes are performed in a manner consistent with the objectives of the management system. Documentation defines what you are going to do and provides evidence of you doing what you say.

The extent of documentation is not defined by the standard and is influenced by a number of factors. These include:

- The size and primary functions of the organisation;
- The complexity and interaction of business processes;
- The control environment, possibly influenced by external obligations;
- The competence of personnel;
- Any other legal or regulatory obligations.

Documents should always be constructed with the target audience in mind. They must be useful to those who need access to the information contained within the documentation.

Organisations are expected to define their processes and document as appropriate. They must then follow their own documentation. **“Say what you do and do what you say”**

IMPLEMENTING AN ISMS

You don't need to document everything. If the standard uses terms such as "formal" or "established, documented and reviewed" then these documents must formally exist.

Procedure that are not formally documented are permissible and have the following characteristics:

- Procedure is systematically:
 - Communicated
 - Understood
 - Applied
 - Effective

Documentation, however, does require management. Such management includes document approvals, requirements on access and legibility and other specifications outlined in Clause 7.5 of the standard.

Module 16: Training and Communications



IMPLEMENTING AN ISMS

Training Requirements

Training plan should consider the following:

- user awareness training
- briefings for the Governance Forum
- targeted training for key “control owner” groups
 - Network support
 - Server support
 - Service desk (user support, incident response)
 - Human resources
- briefings for key executives and line management

TRAINING

The ISMS requires that all personnel are competent in terms of their role within the ISMS. Any competency gaps that have been identified need to be addressed.

However, there is some specific ISMS-focussed training for some target user groups. Some of these groups and the type of training that may be required are listed in the following table.

Audience	Type of training
General users	Information security user awareness training
The ISMS governance forum	On their role within the ISMS
The Information Security Manager/Officer	The mechanisms of keeping the ISMS operating
Service Desk personnel	Normal user and access management Their role in security event and incident management

IMPLEMENTING AN ISMS

Audience	Type of training
Human resource staff	Responsibilities in employee management including recruiting, induction and termination
ICT support personnel	Role in incident response Secure infrastructure commissioning and operations
Executives	Role in messaging the support for the ISMS

Training

Training plan should cover:

- who the target audience is
- what messages they need
- how the message/training will be delivered
- when the training will occur
- how often the training needs to happen
- who will be responsible for organising/delivering
- Whether any assessment mechanisms are required
 - If so, what would that look like?

TRAINING

When developing any training plan consideration must be given to the following:

- who the target audience is?
- what messages do they need?
- how will the message/training be delivered? Face-to-face, online, PowerPoint, team briefings?
- when the training will occur and how often it needs to happen?
- who will be responsible for organising the training, updating the content and delivering the material?
- Are assessments or effectiveness metrics required? Quizzes? Surveys?

This type of information can be captured through a “training needs analysis” exercise.

Once this type of information is captured, a training program can be developed.



ACTIVITY 9: Training Needs

OBJECTIVE

To identify organisational training requirements

TIME

15 minutes

TASK

- In your teams, identify 2 target groups that will require some form of training
- Document:
 - A few of the key messages
 - How the training will be delivered
 - How often it will happen
 - Assessment requirements

NOTES

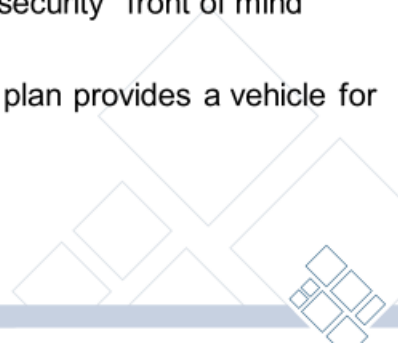
[illegible]

Communications

Communication strategies play an important role:

- to maintain commitment to the implementation and operations
- to win support for the ISMS
- To continue to keep information security “front of mind”

Development of a communications plan provides a vehicle for messaging



COMMUNICATIONS

Communications play a key role within the implementation of an ISMS. They help garner and maintain support for the program by keeping it and its benefits visible both within, and external to, the organisation.

The benefits of strong communications programs include ensuring information security is “front of mind” and not considered a “side issue”.

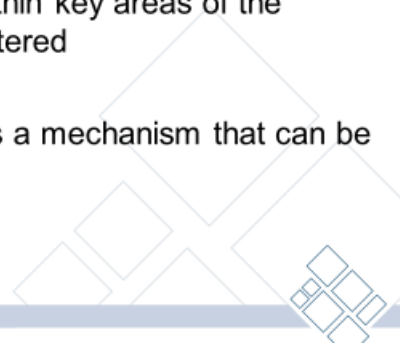
Good communications strategies extend beyond implementation and into normal ISMS operations. Key security dashboards, briefing’s and alerts all form part of a strong communications regime.

Communications Plans

Communications plans should consider:

- What existing communication mechanisms can be utilised
- What involvement from corporate communications and other groups within the agency may be required
- The existing levels of support within key areas of the agency and how this could be altered

Communications Needs Analysis is a mechanism that can be used to assist in this space



COMMUNICATIONS

Similar to the training domain, good communications require the identification of the target audiences, the mechanisms that can be used (either existing or new), the content of the communications and the frequency of such communications.

Again, some process like a Communications Needs Analysis can identify these elements and allow for the development of a comprehensive communications plan.

Involvement of resources from corporate communications areas add significant benefit in this domain.

NOTES

[illegible]

Module 17: Measurements and Metrics



IMPLEMENTING AN ISMS

Measurement

- ISO 27001 does not require you to measure everything
- Part of the continual improvement approach
- The agency needs to determine
 - What needs to be measured
 - How and when this measurement done
 - Who shall do perform the measurement
 - What will happen to the results
 - Who shall analyse the results
 - Who the results are reported to

MEASUREMENT

There are several ways of monitoring an ISMS. Measuring the effectiveness of various components of the ISMS is one of the key mechanisms to assess the performance of the ISMS and drive improvements.

ISO 27001 does not require you to measure everything. It is up to the organisation to determine what metrics are important and how these will be collected and presented.


Measurements can include specific measures of control effectiveness. These could be a bounded range, a trending measure or an absolute value. Again, it is the organisation's choice.

Qualitative assessment of control effectiveness (e.g. marginal, strong etc) does not in itself provide enough detail in terms of the measurements required to drive improvements.

Note that more mature management systems tend to have more metrics available than systems in the early days of operations.

An annual Security Calendar assists in ensuring timely collection and reporting of metrics.

Initial Metrics

- Agencies generally already collect some metrics
 - Start with those as the base measures
 - Identify other areas of high risk/high impact and associated relevant metrics
 - Don't over-measure early, let these develop as the ISMS matures
 - These measures form part of the improvement framework
 - Internal audit and management review form other elements
- 

MEASUREMENT

Agencies should not try to “reinvent the wheel”. Most agencies already accumulate some data or information about information security and how certain controls are functioning. This is a good place to start.

Expansion of the measurement regime should be based on the important or relevance of the control or system component being measured. The more important or sensitive the control area, the more focus should be applied to defining an appropriate metric.

One strategy commonly used is to select controls based on the types or levels of risks that they are mitigating. The more risks a control is mitigating, the more likely that control is important and should be measured.

Another approach suggests measuring the effectiveness of the controls managing higher rated risks.

Again, the choice is the organisation's.

Remember that Internal Audit and Management Review are also both improvement vehicles.



ACTIVITY 10: Identifying Metrics

OBJECTIVE

To identify some key security metrics.

TIME

15 minutes

TASK

In your teams, identify 3 security metrics that are already being collected by agencies

Document in the supplied template:

- Who is responsible for the metric?
- How often is it collected?
- How is it collected?
- What is it used for?

NOTES

[illegible]

Module 18: ISMS Internal Audit



IMPLEMENTING AN ISMS

ISMS Internal Audit

- Required by Clause 9.2 of ISO 27001
- Performed on a planned basis
- A number of audits form the ISMS Internal Audit program
- Individual audits do not need to cover all parts of the ISMS, but the audit program must
- Focus of an ISMS audit is to improve the ISMS
 - System not people

An ISMS audit is more than a “controls” audit



ISMS INTERNAL AUDITS

A requirement under clause 9.2 of the standard, the objective of an ISMS Internal Audit is twofold. First it seeks to assess the conformance of the ISMS with the requirements of the standard, the organisation's own policies and procedures and the legal and regulatory environment under which the organisation operates. The outcome of this element of the ISMS audit includes statements of conformance and non-conformance with those criteria.

The second objective of the ISMS Internal Audit is the opportunity to identify improvements to the ISMS.

Internal audits are conducted under the banner of the ISMS audit program. This program tends to span a period of several years and outlines the scope of each of the planned audits within the program. Audits need to occur at planned intervals. This does not mean regular intervals.

The audit program must address all mandatory clauses and all controls specified within the SoA.

IMPLEMENTING AN ISMS

Each individual ISMS audit may only be focussed on certain clauses and control domains. The auditor for each of these audits cannot audit outside the scope of that specific audit without approval.

The focus on any ISMS audit is on the system and NOT the people. If any resource weaknesses are identified it must always be related to a system weakness. It could be mistakes introduced because of a lack of awareness of their responsibilities, a competency gap or poor supporting policies and procedures. These are the deficiencies that need to be addressed.

An ISMS audit is more than a controls assessment. The management system is the key. Failure of controls usually means a failure in one of the core ISMS components. Fixing the underlying issue will generally address control failures.

ISMS Internal Auditors

Must:

- be competent to audit the management system
- be non-judgmental, objective
- reference is the ISO 27001, not own opinions
- be able to provide objective assessment of ISMS effectiveness, focusing on the system, not the people
- be able to report fairly and without bias
- be selected to ensure impartial and objective results

ISMS INTERNAL AUDITORS

As with all roles within the ISMS, ISMS Auditors need to be competent and have the necessary skills to conduct an ISMS audit. Whilst the general ICT auditor has the necessary skills to audit the control elements, it is important that the auditor has sufficient skills to audit the management system components.

ISMS auditors add value to the ISMS.

Some of the personal attributes of good ISMS auditors are:

- ethical, fair and truthful;
- objective and audit against the criteria (ISO 27001) rather than their opinion;
- diplomatic;
- observant;
- culturally sensitive;
- collaborative.

An ISMS audit should not be adversarial.


IMPLEMENTING AN ISMS

Module 19: Management Review



IMPLEMENTING AN ISMS

ISMS Management Review

- Required by Clause 9.3 of ISO 27001
 - Performed on a planned basis
 - Should occur after the ISMS Internal Audit
 - Must consider as input all elements defined in Clause 9.3
 - Outputs are recommended changes and improvements to the ISMS
 - Should be performed by senior management
 - Often the Governance Forum
 - Must be documented
- 

MANAGEMENT REVIEW

A requirement under clause 9.3 of the standard, the objective of the Management Review is to assess the performance of the ISMS, taking into account a number of inputs, and to determine any necessary changes or improvements to the system.

Management Reviews are conducted at planned intervals and are performed by senior management. Generally, this is the ISMS governance forum.

Management Reviews must consider the following mandatory inputs as defined by ISO 27001:

- the status of actions from previous management reviews;
- changes in external and internal issues that are relevant to the information security management system;
- feedback on the information security performance, including trends in:
 - 1) nonconformities and corrective actions;
 - 2) monitoring and measurement results;
 - 3) audit results; and
 - 4) fulfilment of information security objectives;
- feedback from interested parties;
- results of risk assessment and status of risk treatment plan; and
- opportunities for continual improvement.

IMPLEMENTING AN ISMS

Outputs from the Management Review will include decisions related to continual improvement opportunities and any need for changes to the ISMS.

These inputs and outputs must be documented, usually in the minutes of the Management Review meeting.

Given that the results of the ISMS Internal Audit form part of the inputs into the Management review, this means that the audit should occur before the management review is conducted.

Module 20: Corrective Actions and Improvements



IMPLEMENTING AN ISMS

Corrective Actions & Improvements

- Required by Clauses 10.1 and 10.2 of ISO 27001
- Fundamental premise of the ISMS is that it will continually improve
- Corrective actions – where a deficiency has been identified within the ISMS
- Could be raised by:
 - Internal audits
 - Management reviews
 - External audits
 - Incidents
 - Security reviews and testing



CORRECTIVE ACTIONS AND IMPROVEMENTS

ISO 27001 requires an organisation to continually improve its ISMS. These improvements come from a number of activities. Corrective action is one mechanism to drive improvements and address weaknesses within the system.

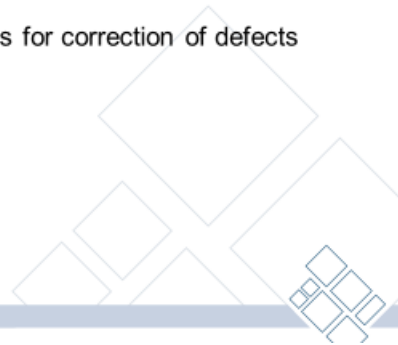
Corrective action is required by ISO 27001 when a non-conformance or deficiency is identified.

The need for corrective action can arise from a number of ISMS activities. These include:

- Internal audits;
- Management reviews;
- External audits;
- Security incidents;
- Security reviews and testing.

Corrective Actions

- Required to address any deficiencies as per agreed procedure
- Your agency specifies its timelines for response
- Only exception is issues raised by the certification bodies
 - Operate on very specific time frames for correction of defects




CORRECTIVE ACTION

The organisation's response to a need for corrective action is documented in some form of corrective action procedure. This procedure includes the requirement for root cause analysis to ensure that the non-conformance does not re-occur.

The timeframe for response and implementation of corrective action is the choice of the organisation, except for non-conformances raised by certification bodies. There are defined timeframes for the implementation of corrective action for any non-conformances raised during certification or surveillance audits.

Improvements

- Raised from a number of different sources
 - Internal audits
 - Management reviews
 - External audits
 - Suggestions from interested parties
 - Security reviews
 - Suggestions
 - Again, timeframes are up to the agency
 - The ISMS does not require you to implement all suggested improvements BUT you must improve your system
- 

IMPROVEMENTS

Organisations with operational ISMS' must continually strive to improve their management system. This is fundamental to all management systems and an ISMS is no exception.

Improvements can come from a number of sources. These include:

- Internal audits;
- The output from Management reviews;
- External audits;
- Security incidents;
- Security reviews and testing;
- Suggestions, including those from interested parties.

Suggested improvements should be considered but do not need to be implemented. The organisation selects those improvements it feels adds value to the ISMS.

Suggestions from internal and external auditors also do not need to be implemented but should be considered.

Timeframes for implementing agreed improvements are set by the organisation.

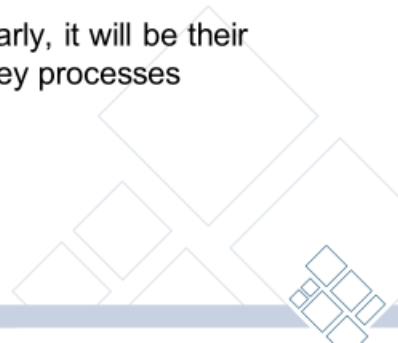
IMPLEMENTING AN ISMS

Module 21: Operationalising the ISMS



Embedding the ISMS

- As processes are developed, start using them
- Move these elements as close to BAU as possible
- Keep all processes as simple as possible
 - When you have an implementation choice, always consider the simplest alternative first
- Involve the operational groups early, it will be their responsibility to administer the key processes



EMBEDDING THE ISMS

Moving the ISMS from an implementation project to an operational system should not be a major step. One of the keys to a seamless transition is the strategy of immediately utilising the artefacts and processes as they are created. As a process is developed, it should immediately be used by the operational areas.

This approach has several benefits. Firstly, the business doesn't see this as a "big bang" approach. The benefits for these new or amended processes are recognised early, building support for the ISMS. The other major benefit comes with the early collection of measures and evidence to assist in improving the ISMS.

It is important to ensure that these new and changed processes are made available to the operational teams. As much as possible, the operations of the ISMS should be as close to the front line operational teams as possible. It should become "business-as-usual".

Another key to successful transition is to ensure that the governance forum operates at a strategic and management level and does not become immersed in operational challenges. The exception is when resource or business change decisions are required.

Organisational Change

Be aware of possible barriers to change within your agency:

- Lack of top management commitment to the system
- The agency culture may be resistant to change
- Size of the agency – large agencies tend to change more slowly
- Primary role of the agency – some are more risk adverse
- Individuals may perceive conflicting priorities
 - Have too many other things to do, see this as burden

ORGANISATIONAL CHANGE

In many organisations, there are some internal barriers to change. These barriers can hinder the successful implementation of an ISMS. Such barriers may include:

- Lack of top management commitment to the system. This is particularly true when the implementation is driven by a compliance objective;
- The agency culture may be resistant to change;
- Size of the agency – large agencies tend to change more slowly;
- Primary role of the agency – some are more risk adverse;
- Individuals may perceive conflicting priorities in that they have other projects or activities and feel they are under-resourced.

Overcoming these barriers requires good and regular communications strategies, highlighting the benefits of the ISMS and “what’s in it for them”.

Keeping the system as simple as possible is another factor that can help overcome some of these challenges.

Running a Security Calendar

A security calendar:

- Provides a list of all scheduled activities within the information security domain
- Includes the specific ISMS items such as internal audit, review of risks and management review
- Can be used to plan and resource tasks



THE SECURITY CALENDAR

The concept of a security calendar is not addressed directly by the standard. However, an operating ISMS has a number of regular or planned activities relating to either clauses 4–10, or controls specified in the Statement of Applicability.

An artefact such as an ISMS Security Calendar captures all planned activities relating to the ISMS. It can then be used as part of the governance and monitoring of the system to ensure that planned activities occur on schedule.

It becomes a useful planning and resourcing tool.

The ISMS Security Calendar may form part of a larger compliance calendar.

Sample activities in the calendar may include items such as:

- ISMS internal audit;
- Review of privileged users;
- Management review;
- Review of risk register;
- Delivery of annual security awareness training.



ACTIVITY 11: The Security Calendar

OBJECTIVE

To identify key activities for inclusion in the Security Calendar.

TIME

15 minutes

TASK

As a group, discuss activities that may appear on such a calendar.

Consider:

- ISMS-specific activities
- Control effectiveness reviews
- Other security activities

For each activity, consider the frequency of the activity.

NOTES

[illegible]

Module 22: Certification



Certification Audits

- Performed by a “trusted third party”
 - Under a program overseen by JAS-ANZ
- Steps for certification generally are:
 1. Complete the application forms
 2. Undertake the certification audits
- ISMS Certification Audits are conducted in two Stages.
 - Stage 1 - Document Review
 - Stage 2 - Implementation Review



CERTIFICATION

The process of formal certification of an ISMS requires engaging an independent trusted third party to assess the conformance of the system against ISO 27001, the organisation’s own policies and procedures and the legal and regulatory environment under which it operates.

The certification audit is designed to:

- Demonstrate ISO 27001 compliance to customers and other interested parties;
- Reduce information security risks to customers and suppliers;
- Increase the confidence of customers, suppliers, regulators and others in the organisation’s information security.

The first step of the certification process involves the organisation completing an application form with a selected certification organisation.

The next step is the conduct of a Stage 1 certification audit. This is followed up by the final Stage 2 audit. At the completion of this Stage 2 audit a recommendation for certification will be made assuming no major non-conformances has been identified.

Certification Audits

Are performed to:

- Confirm the ISMS meets internal and external organisational requirements (**intent**)
 - usually in Stage 1
- Assess that the stated requirements and controls are being used (**implementation**)
 - usually in Stage 2
- Evaluate that processes and controls effectively manage information security (**effectiveness**)
 - only in Stage 2

CERTIFICATION AUDITS

During the Stage 1 certification audit, the auditor examines the documentation from the system to ensure that it meets the requirements of the standard. From a control perspective, this review focusses on the “intent”, that is, the organisation has or will implement this control. This assessment of intent is driven by those controls included in the SoA.

The auditor will also examine all mandatory documentation required by the standard.

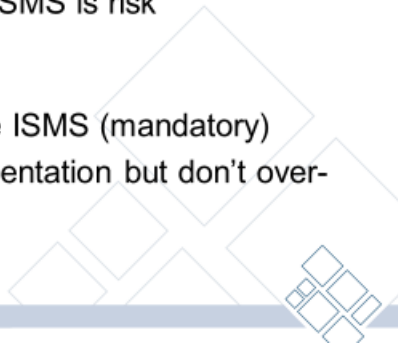
During a Stage 2 audit, the auditor is looking for evidence that the processes and controls have been implemented and are effective.

Note that most Queensland Government agencies do not currently have the requirement to seek certification for their ISMS.

Summary



Summary

- ISMS implementation and operations is not complicated
 - Good implementation planning generally gets a good outcome
 - Clear definition of the scope is important
 - The fundamental purpose of an ISMS is risk management
 - Get that right
 - Clauses 4-10 are the heart of the ISMS (mandatory)
 - The system requires core documentation but don't over-document!
- 

SUMMARY

Implementing an ISMS seems scary but it is a relatively straightforward process. At its heart, an ISMS is a formal way of identifying and managing risks to information that is important to the organisation.

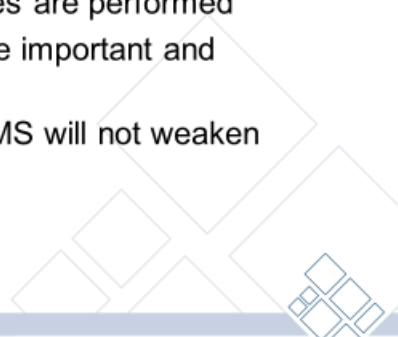
Implementation is quite linear, and once the scope is well-defined, the rest of the implementation steps is straightforward.

Like all larger programs of work, good planning generally leads to a good outcome.

Try not to over-engineer the processes, particularly risk management, and don't over-document. Make sure the documentation is "fit for purpose" and targeted at the desired audience.

Remember clauses 4-10 are the heart of the ISMS and are mandatory. You must address all requirements in these clauses.

Summary

- The ongoing governance is critical
 - The Statement of Applicability documents your control objectives and controls
 - Security calendars are a good tool to ensure all relevant and necessary processes are performed
 - Training and communications are important and ongoing
 - Replacing existing IS 18 with ISMS will not weaken security
 - Keep it simple!
- 

SUMMARY

Ongoing and regular governance of the ISMS is very important. Visible executive commitment is required to enforce the importance of the system and the benefits it can bring.

Remember the Statement of Applicability documents the organisation's control objectives and controls. It will reference all 114 controls contained in Annex A but may also include controls from other sources.

The use of security calendars has proven beneficial for most ISMS implementations and is strongly recommended.

The deployment of an ISMS is a shift from the IS18 compliance model to a risk-based model, taking into account the differences between agencies. The ISMS provides a platform for a proactive security environment and acts as a driver to strengthen security culture.

The parting message however, is keep it as simple as you can. It has to be practical and pragmatic, otherwise pockets of resistance form and impact the effectiveness of the management system and the organisation's security.