# Introduction
# ISO 27001

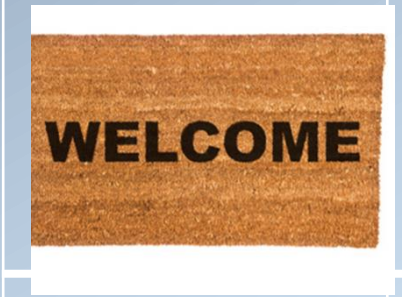
Universitas Lambung Mangkurat
Kalimantan Selatan
13 Februari 2018


Welcome to Our Classroom
Introduction an Information Security Management System

# Course Purpose

- To understand the concepts of fundamental contained within ISO/IEC 27001:2013 and its role in defining an Information Security Management System
- To develops the skills needed to implement an ISMS based on the ISO/IEC 27001:2013 Information Security Management Systems standard.

# Let's get started

| | | | | |
|---|---|---|---|---|
|  | Get Ready! | |  | Introductions |
|  | Materials | |  | Mobiles & email |
|  | Breaks | |  | Facilities |

# INFORMATION SECURITY MANAGEMENT SYSTEMS

# Information Asset

Information can be in many forms:

- Data records: HR information, Accounts Payable records
- Hardware: Server, Laptop, Whiteboard
- Software: Windows XP, SAP, SalesForce
- People: Manager, Call centre agent, Support Engineer
- Paper: Confidentiality agreement, Memos
- Information: Credit card data, written on board, voice message
- Supporting utilities: UPS, Air Conditioner, Phone service

# Characteristics of Information Security

- Confidentiality

  *Provide access only to those who need the access.*

- Integrity

  *Keep the information accurate and complete.*

- Availability

  Make the information available when the authorised user needs it.

# Why do we need to protect information?

- Preserving competitive advantage, reputation & trust
- Avoiding legal penalties
- Protecting the organisation's (critical) information against:
  - Disclosure
  - Loss
  - Improper use
  - Unauthorised change
  - Theft
- Ensuring the continuity of the business
- Assuring business partners & customers that their confidential information is secure

# What is an Information Security Management System?

- The policies, standards, procedures, practices and planned activities that an organisation uses in order to secure its (critical) information assets, for example:
  - Risk Assessment Method
  - Documented Controls and processes
  - Security awareness, guidance, training and competencies
  - Tools and equipment, including firewalls, virus scanners, automated administration and security monitoring.

- The design of the system and how it is implemented depend on the needs and objectives of the organisation, its size and structure, and the sensitivity of information it owns or holds on behalf of others to loss, corruption, theft, disclosure or discontinuity

- The purpose of an Information Security Management System is to secure an Organisation's **Information Assets** by identifying, assessing and managing **Risks** which are presented by **Threats** and **Vulnerabilities**

# What is an ISMS Framework?

A management framework where there is:

- A clear understanding of the objectives and context of information security both within, and external to, the organisation
- Communication within and across business entities using common language, objectives, policies
- Clear understanding of the information assets and associated risks
  - Allows intangible to become tangible
  - Rationalises and prioritises risks
  - Articulates actions and achievements
- Systematic measurement and reporting of the effectiveness of controls and countermeasures
- A link to other IT, quality and business initiatives

# How to establish security requirements?

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

# What are the ISMS resources?

- All the people involved in the use and handling of information within the scope of the ISMS. This includes:
  - Management
  - Employees
  - Suppliers
  - Customers
  - Shareholders
  - Other third parties with whom information is shared (e.g. vendors, regulatory authorities, data storage companies)

- It also includes other resources, as applicable, including:
  - Infrastructure
  - Specific information security technologies
  - Firewalls
  - Virus scanners
  - Password controls, etc.

# What are the ISMS resources ?

- The information security management system extends outside the organisation to encompass suppliers, customers and other interested parties (e.g. regulators)
- There is a continuous, two-way flow of information between the organisation, its customers, suppliers and other interested parties regarding information security requirements, mutual expectations and information security management

# Why implement an ISMS?

- An organisation that establishes an effective information security management system creates confidence in the reliability of its information security.
- This can lead to increased customer confidence and trust, and to the continued success of both the organisation and its customers.
- Technical security alone is not sufficient. Many organisations that have good technical security suffer breaches. Sometimes, cost of controls is more than the benefits derived.
- The global security landscape continues to evolve and organisations must also continue to improve their approach to protecting their critical information.
- If there is no management system in place for continuous monitoring security, somewhere information will be leaked.

# What is an effective ISMS?

- Provides an organized approach
- Is based on security needs of
  - The Organisation
  - Customers
  - Suppliers
  - Others (e.g. regulators)
- Is clearly defined
- Helps the organisation to monitor and improve security
- Includes certain core elements, e.g. incident containment, continual risk review

A system that

- meets information security requirements
- continually monitors and improves information security effectiveness

# ISMS IN THE CONTEXT OF ISO 27001

# ISMS in the context of ISO 27001:2013 and other Standards

**HISTORY**

- 1995 BS7799 – British standard was published
- 1997 Adaptation BS7799 – Netherlands
- 1999 AS/NZS 4444 – Australia/New Zealand standard was published
- 1999 BS7799-2 Specification was published
- 2000 BS7799-1 Code of Practice was fast tracked as an ISO standard – ISO/IEC 17799
- 2005 ISO 17799 updated new technologies – e.g., email, encryption

- 2005 ISO 27001 specification was published – contains Audit Requirements,
  with Controls aligned with ISO 17799
- 2006 ISO 27006 was published – Guidelines for Certification Bodies
- 2007 ISO 17799 renumbered as ISO 27002:2005
- 2009 ISO 27000 ISMS Vocabulary was published
- 2013 ISO 27001 and 27002 updated to reflect ISO Annex SL requirements and
  changing landscape

# ISO 27001 Scope

- 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.

# ISO 27001 Scope

- Scope will include IT, it will also extend beyond IT, to other organisational objectives, for example:
  - Control of changes to financial data
  - Control of disclosure of personal data
  - Secure interconnection of customer, supplier and partner computer networks
  - Background screening of personnel with access to sensitive information
  - Personnel training in information security and disciplines

# ISO/IEC 27001:2013

1. Scope
2. Normative References
3. Terms and Definitions
4. Context of the Organisation
    - Understanding organisation and its context
    - Understanding third party needs and expectations
    - Determining the scope of the ISMS

5. Leadership
   - Commitment
   - Information security policy
   - Roles and responsibilities
6. Planning
   - Addressing risks and opportunities
   - Addressing information security objectives

# ISO/IEC 27001:2013

7. Support
   - Resources
   - Competence
   - Awareness
   - Communication
   - Documentation
8. Operation
   - Planning and control
   - Risk assessment
   - Risk treatment

9. Performance Evaluation
    - Monitoring and analysis
    - Internal audit
    - Management review
10. Improvement
    - Nonconformity and corrective action
    - Continual improvement

Annex A  Reference Control Objectives and Controls references

# DETAILS OF CLAUSES 4 TO 10

# IN ISO 27001:2013

# Details of ISO 27001:2013 General Controls

**Scope of the standard**

ISO 27001 is applicable to all types of organisations.

**Process Approach**

ISO 27001 adopts a Process Approach.

- Input
- Process – Resources – Criteria – Process steps
- Output
- Linkage to other processes

# Details of ISO 27001:2013 General Controls

**Applicability and Exclusion of processes from Scope**

Clauses 4 - 10 are mandatory.

Security requirements are determined by risk assessment and applicable legal or regulatory requirements.

Management should have accepted the risk

Exclusions that affect the organisation's ability or responsibility to provide security are NOT ACCEPTABLE.

# Details of ISO 27001:2013 General Controls

ISO 27001 gives general requirements for establishing and maintaining an ISMS.

**Clause 4 Context**

- 4.1 Understanding the organisation 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 ISO 27001:2013 General Controls

**5. Leadership**

- 5.1 Leadership and commitment
  - Demonstrable
  - Critical element
- 5.2 Information security policy
  - High level
  - Includes objectives
- 5.3 Roles and responsibilities
  - Conformance to the standard
  - Reporting on the performance of the ISMS

# Details of ISO 27001:2013 General Controls

**6. Planning**

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

# Details of ISO 27001:2013 General Controls

**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

Supports the establishment and continued operations of the ISMS.

# Details of ISO 27001:2013 General Controls

**8. Operations**

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

Required activities for an operational ISMS.

# Details of ISO 27001:2013 General Controls

**9. Performance Evaluation**

- 9.1 Monitoring, measurement, analysis and evaluation
- 9.2 Internal audit
  - At planned intervals
- 9.3 Management review
  - Also at planned intervals
  - May be part of a wider management exercise/framework

This clause covers the requirement for internal ISMS audits.

# Details of ISO 27001:2013 General Controls

**10. Improvement**

- 10.1 Nonconformity and corrective action
- 10.2 Continual improvement

The ISMS should be designed to improve itself by utilising mechanisms to detect weaknesses or failures.

Section 10, coupled with Section 9, assists to ensure this occurs.

# ISMS PROGRAM INITIATION

# Planning the Project

- Identify a project champion
  - Business representative with issues that could be solved?
- Steering team
  - Which groups need to be involved?
  - HR, Risk Management, Legal?
- Implementation team
- Internal auditor candidates
- Top management commitment

# Establishing the Scope

State the objectives for the ISMS

- Who is concerned about information security?
  - Organization and its stakeholders?
  - Customers?
  - Regulators?
- What are the generic classes of information to be protected?
  - E.g. intellectual property, customer records
- What are the generic classes of loss (cost) to be secured against?
  - E.g. business continuity, market, reputation, legal penalties

# Establishing the Scope

- Include the type or nature of the business
- Define the physical scope

  i.e. locations or facilities covered by the ISMS
- Define the logical boundaries
  - Are related organisational units which process information assets that are in the scope of the ISMS included in the ISMS?
  - Are third party service providers included?

# Establishing the Scope

- A fictional company that runs on-line internet banking as an outsourced service for banks:
  - The Information Security Management System for the implementation, deployment, operations and support for On-Line Banking in accordance with the Statement of Applicability dated 1 January 2006 and ISO 27001:2013
- A fictional company that runs background checks against its databases for clients with secure connections to its data centres:
  - Management of the Information Security Management System for Hosting Operations, including the background checking service within the Orlando, FL and Phoenix, AZ Data Centres, using the Statement of Applicability dated 1 January 2006

# Establishing the Scope

- A fictional hospital:
  - The Information Management Security System covering Patient Records in accordance with the Statement of Applicability dated 1 January 2006 and ISO 27001:2013
- A fictional company that is concerned about the accuracy and integrity of its financial records:
  - The Information Security Management System for Corporate Operations including financial records and accounts at the Chicago IL facility, using the Statement of Applicability dated 1 January 2006

# Establishing the Scope

- A fictional R&D company:
  - The Information Management Security System including proprietary Patent and Design information in accordance with the Statement of Applicability dated 1 January 2006 and ISO 27001:2013
- A fictional R&D company that supplies secure databases:
  - The Information Management Security System including proprietary Patent and Design information and the Design, Provision and Support of Secure Database Products in accordance with the Statement of Applicability dated 1 January 2006 and ISO 27001:2013
- A fictional call centre:
  - Management of the Information Security Management System for high availability customer care operations and confidential customer data using the Statement of Applicability dated 1 January 2006

# Establishing the Scope

- A land development company in Australia
  - The information security of Landcom covering general information and land, internal financial and personnel information.
- A Cricket Club
  - The registration covers the Information Security Management System for the Information Systems department delivery of services to support the Melbourne Cricket Clubs' applications and systems

# Establishing the Scope

- A Department of the Government
  - The processes, assets and technology of the information security branch, including information both paper and electronic, databases and files, policies, procedures and support documentation and software platforms and applications. This is in accordance with the latest version of the Statement of Applicability.
- A Lottery agency
  - The registration covers the Information Security Management System for the provision of Enhancements to the Gaming System Application of the NSW Lotteries Corporation

# Preparing the Project Plan

- Must address all elements of Causes 4 -10
- Resourcing should include:
  - Hardware
  - Software
  - People
  - Training requirements for each phase
- Each clause in ISO 27001 is an activity/sub activity
- Work out whether certification is required
- Preferably include activities for follow up on findings of certification audit

# TOP LEVEL

# INFORMATION SECURITY POLICY

# Top Level Security Policy

- In ISO 27001:2005 this was known as the ISMS Policy
- Must be:
  - Appropriate to the purpose of the organisation
  - Include information security objectives (Clause 6.2) or provides the framework for setting information security objectives
  - Include a commitment to satisfy applicable requirements related to information security
  - Include a commitment to continual improvement of the information security management system
- Policy must be documented, communicated within the organisation and be available to interested parties, as appropriate.

# IDENTIFYING INFORMATION ASSETS

# A Reminder - Information Assets

Information can be in many forms:

- Data records: HR information, Accounts Payable records
- Hardware: Server, Laptop, Whiteboard
- Software: Windows XP, SAP, SalesForce
- People: Manager, Call centre agent, Support Engineer
- Paper: Confidentiality agreement, Memos
- Information: Credit card data, written on board, voice message
- Supporting utilities: UPS, Air Conditioner, Phone service

# Information Assets

- ISO 27001:2013 does NOT require you to identify assets BEFORE you perform risk assessments
- However, good practice to identify those in scope to provide focus for the assessments
- Annex A Control 8.1.1 still requires an inventory of assets to be complied and maintained
- Need asset owner who may also be the risk owner
- Also the “value” of the asset (determined by a defined table?)

# RISK ASSESSMENT

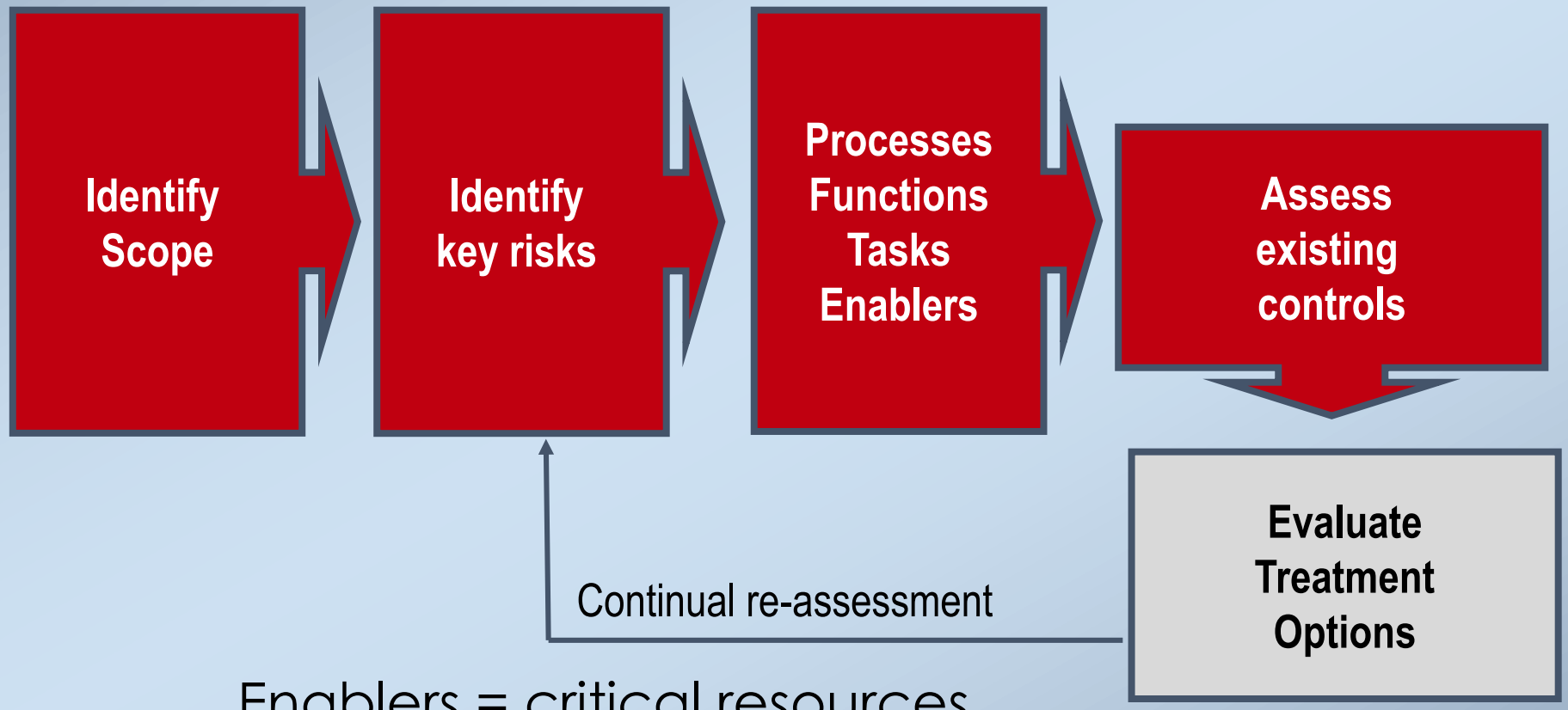
# Risk Assessment

- ISO 27001 Core Elements:
  - Risk Assessment
    - Process must be defined (6.1.2)
    - Includes criteria for accepting or treating risks (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 Management Guidelines

- ISO 27033 Information Technology – Guidelines for the management of IT Security
  - Information Security Threats & Vulnerabilities
- ISO/IEC 27005
  - Information Security Threats & Vulnerabilities
  - Scoping  guidelines
- ISO/IEC 31000
  - Addresses risks throughout the organisation

# Risk Assessment & Risk Treatment in ISMS




Enablers = critical resources

# Threats and Vulnerabilities

- Threat
  - Potential cause of an unwanted event which may result in harm to a system or organisation
  - Deliberate, Accidental or Environmental
  - E.g. Malicious software

- Vulnerability
  - Characteristic (including weakness) of an information asset or group of information assets that can be exploited by a threat
  - E.g. Disabled firewall

# Threats and Vulnerabilities

**Analyse what threat can exploit which vulnerability**

- Examples of Threats are
  - Identity thief
  - Intellectual property thief
  - Internal Fraudster
  - Malicious hacker
  - Earthquake

- Examples of Vulnerabilities are
  - No firewall
  - Uncontrolled physical access to R&D and manufacturing facilities
  - No background checks
  - Passwords easy to guess
  - Open internal access to sensitive data
  - Transporting data disks by low security carrier
  - No file backups

# Risk Strategy Options

**STEPS IN A RISK ASSESSMENT APPROACH**

- Identify all Information Assets in Scope
- For each Information Asset identify all processes that touch it
- Identify Threats (agencies that could cause loss)
- Identify Vulnerabilities (process "holes" that one or more Threats could exploit)
- Prioritise (can't address all risks, not cost effective)
- Implement Countermeasures to reduce risks
- Implement Controls to minimise Vulnerabilities
- Monitor (e.g. audits)
- Repeat from step 1 in regular review cycle

# Risk Strategy Options

- Baseline Approach
  - Standard safeguards
  - Minimum resources for risk assessment and management
  - Standard solutions across many systems, assets
  - If baseline is too high, security may be expensive
  - If baseline is too low, exposure may be excessive
  - Difficult to assess security impact of changes

# Risk Strategy Options

- Informal Approach
  - Pragmatic, exploits knowledge and experience of individuals
  - Inexpensive risk assessment and management
  - Error prone: might miss threats, or manage non-existent threats
  - Subjective, depends on individuals: Does not "ensure that risk assessments produce consistent, valid and comparable results" (ISO 27001)

# Risk Strategy Options

- Detailed Risk Analysis
  - Identify and value information assets
  - For each asset evaluate threats and vulnerabilities
  - Systematically control or accept risks
  - Takes time (vulnerable during this time)
  - Expensive, thorough

# Risk Strategy Options

**COMBINED APPROACH**

- Initial High Level Risk Analysis
  - Identify critical information assets, values, risks
- For high value or high exposure assets
  - Detailed risk assessment in priority order
- For the rest
  - Baseline approach

# Risk Strategy Options

- Benefits of combined risk strategy
  - Initial quick simple approach gains acceptance of the risk management program
  - Strategic picture of security program emerges quickly, e.g. good for planning purposes
  - Focus time and money on high value, high risk first
- Potential disadvantage
  - High level risk assessment might miss areas that need detailed risk assessment
  - But baseline security applies and risks can be re-evaluated

# Risk Strategy Options Type 1

Vulnerability - Very Low, Low, Moderate, High, Very High

Likelihood - Rare, Unlikely, Possible, Likely, Certain

Asset Value - Very Low, Low, Moderate, High, Very High

Measure of Risk: combination of the three

# Risk Strategy Options Type 2

Likelihood - Rare, Unlikely, Possible, Likely, Certain

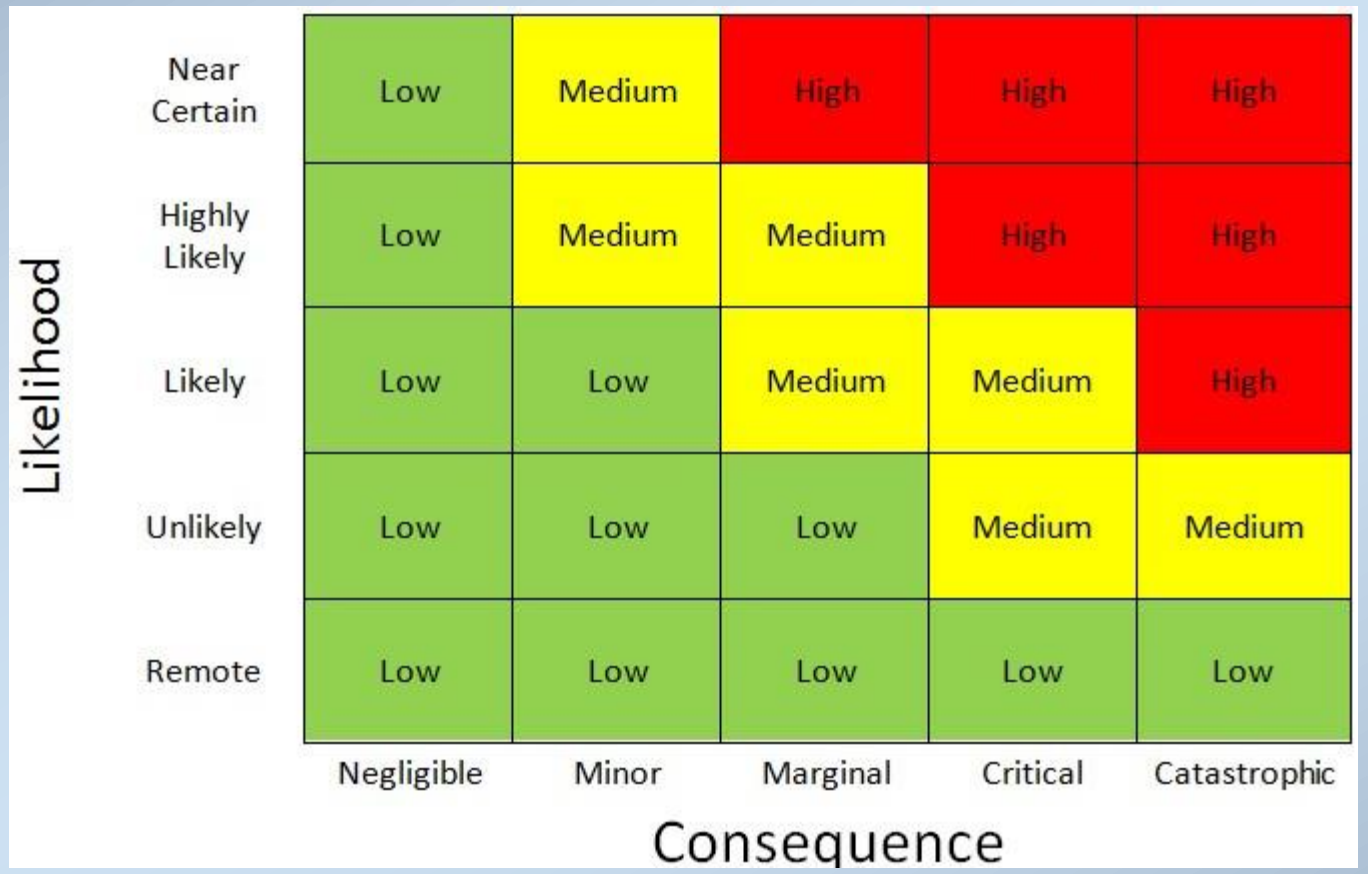
Consequence - Very Low, Low, Moderate, High, Very High

Measure of Risk: combination of the three

# A Risk Matrix

| | Likelihood | Rare(R) | Unlikely (U) | Possible (P) | Likely (L) | Certain (C) |
|---|---|---|---|---|---|---|
| **Consequence** | Very High | **6** | **8** | **10** | **12** | **14** |
| | High | **5** | **7** | **9** | **11** | **13** |
| | Moderate | **4** | **6** | **8** | **10** | **12** |
| | Low | **3** | **5** | **7** | **9** | **11** |
| | Very Low | **2** | **4** | **6** | **8** | **10** |

# Another Risk Matrix



# ANNEX A CONTROLS

# Risk Management Strategy

**Treat**

Select and implement controls to reduce the risk

**Transfer**

For example, buy an insurance policy.

For example, outsource.

**Terminate**

For example, CD Drives are disabled.

For example, physical access to data centres is restricted to IT support staff.

**Tolerate**

Accept the remaining risk

# Selecting Controls

- After identifying risks, can select controls to treat from ANY control set
  - ISO 27002
  - PCI-DSS
  - NIST
  - AG-ISM
  - Your own
- However, ISO 27001 Annex A  must still be checked after to ensure no controls have been overlooked

# STATEMENT OF APPLICABILITY

# Statement of Applicability

**Requirements in ISO/IEC 27001:2013:**

- Identify Control objectives, controls selected, reasons
- Selected controls may be additional to those listed in Annex A
- Identify Control objectives and controls currently implemented
- Include justification for Controls listed in Annex A that are excluded (cross check with the risk register)

# Statement of Applicability

**SOA is:**

- ISMS certificate is linked to SOA version number and date. So, if a control is added or removed, the ISMS certificate has to be reissued.
- Key Audit instrument for Controls
- Required for audit planning purposes
- May be integral to scope statement
- May be more than one SOA, for example, departmental SOA but a single version.

# TRAINING

# Training

- Consider training plan similar to communications plan
- NIST SP 800-50 provides guidance on building program
- Targeted training is important
- Consider audience and delivery vehicles available
- Need to establish measurement / success measures

- Build ongoing program – training is not a once off exercise!!

# DOCUMENTED ISMS

# Documented ISMS

| | |
|---|---|
| • ISMS Scope | 4.3 |
| • High level information security policy | 5.2 |
| • Risk Assessment Methodology | 6.1.2 |
| • Risk Assessment Report | 6.1.2, 8.2 |
| • Statement of Applicability | 6.1.3 d) |
| • Risk Treatment process | 6.1.3, 8.3 |
| • Information security objectives | 6.2 |

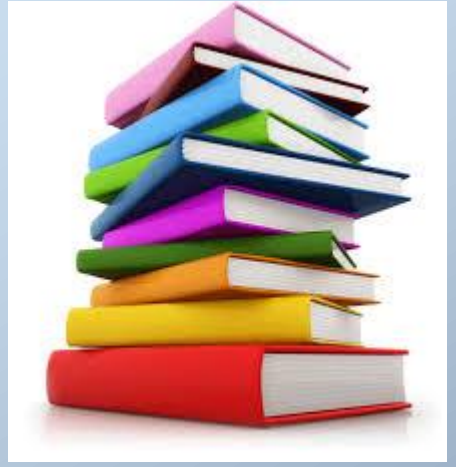
- Evidence of competencies 7.2
- Documented information as required by the ISMS 7.5.1 b)
- Documents and records required by ISO 27001 7.5.1 a)
- Monitoring and measurement results 9.1
- Internal audit programme and results 9.2
- Results of management review 9.3
- Non-conformances and results of corrective action 10.1

# Procedures

- **Procedure:**
  - "Specified way to carry out an activity or process"

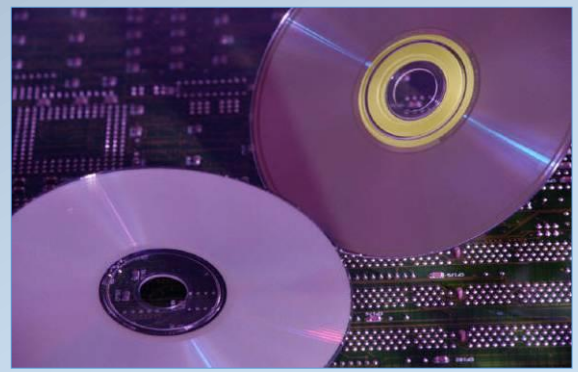
Note 1: Procedures **can be documented or not**

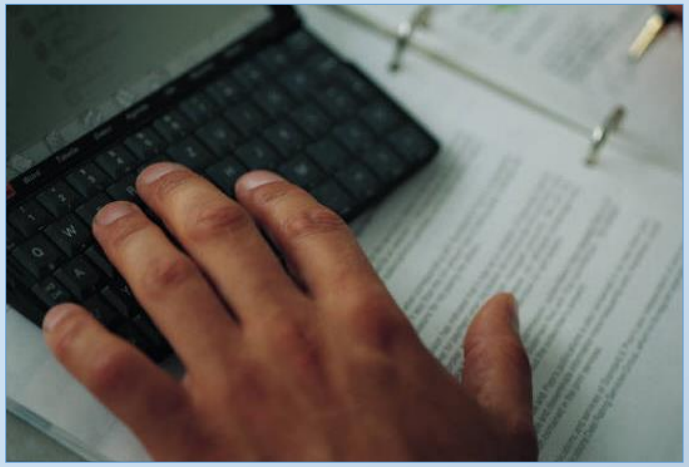
***ISO 9000:2000 3.4.5***



# Documentation

***... may exist in many forms***





# Documentation Considerations

Extent is dependent on:

- Size and type of organisation
- Complexity and interaction of processes, controls
- Competence of personnel
- Legal obligations
- Federal and local codes and regulations

….and of course associated 'Risks'

# Documentation Considerations

- To communicate the ISMS
  - Identify processes and controls needed
  - Ensure availability of resources and information
  - Identify audiences for documents
    - Write and distribute documents with audience in mind. For example:
      - Password admin might be complex document for IT administrators, probably on-line
      - Password instructions for users might be
        - Written in very simple terms,
        - Disseminated perhaps in handbooks given to employees as they join the company
        - Checked for compliance with the rules in user account management

- Monitor, measure and analyse processes and controls
  - For continued effectiveness
  - For opportunities to improve

# Documentation Considerations

**Organisations are expected to:**

- Define their processes
- Document as appropriate
- When documenting processes, controls:
  - Say what they do
  - Do what they say
- Show that the process works (effectiveness)
- Continually re-assess risks and improve controls
- Ensure changes are authorized, controlled

# Documentation Considerations

- To identify Vulnerabilities
  - Process flow diagrams
  - Process maps
  - Interactive web-based process maps
  - Written processes, paper or on-line
  - Descriptions of interactions between processes
- Essential for identifying Vulnerabilities in complex processing of Information Assets

# Undocumented Procedures

What are the characteristics of an acceptable “procedure which is not documented”?

# Undocumented Procedures

- Procedure is systematically:
  - Communicated
  - Understood
  - Applied
  - Effective
- A ‘procedure’ can be a ‘statement’ recognized as part of the formal ISMS

**There is no requirement to document every procedure.**

# MONITOR AND MEASURE

# Metrics

- Need to determine “best” measures
- What needs to be measured
- How this is done – methods
  - Needs to ensure valid results
- When should it be done
- Who shall do this
- What happens to these results – when are the analysed?
- Who shall analyse the results

# Other Measures

- Internal audit
- Regular review of risks
- Management review
- Legal and regulatory assessment
- How do we improve the ISMS?

# Auditing an ISMS

ISMS Certification Audits are conducted in two Stages.

***Stage 1*** - Document Review

***Stage 2*** - Implementation Review

Audit need to do, for:

- Confirm ISMS arrangements comply with organisational requirements, both internal and external **(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**

**Provide a service to the auditee**

# Auditing an ISMS

- Used effectively can be a most powerful management process
- Poorly implemented by untrained personnel adds little or no value to the organisation
- If used in a threatening and judgmental way, can be destructive
- Auditors want people to talk about security strengths and weaknesses – not hide them

**Look out, here come the auditors!**

# Auditing an ISMS

- "A person with competence to conduct an audit"
- Complies with ISO 19011:2011
- Non-judgmental, objective
- Reference is the Standard, not own opinions
- Provides objective assessment of ISMS effectiveness
- Reports fairly without bias
- Not right … Not wrong … Independent reviewer
- Might offer consultancy but without taking ownership of the process, e.g.
  - Identifying solutions that work elsewhere in the organisation
  - Offering options and ways to evaluate them

# The Security Calendar

- Not explicitly required by ISO 27001
- But can be a key artefact for oversight of activities
- Used by ISMS governance and operational teams to ensure core activities are completed

# MAINTAIN AND IMPROVE THE ISMS

# Continual Improvement

The need for continual improvement

- Customer perceptions of security
- Competitors
- Business development
- New technology
- Control costs

# Institutionalisation

**Moving from Implementation to Maintenance**

- Position close to front line
- Look to expand into other management systems
- Seek benefits

# Continual Improvement

The organisation shall continually improve the suitability, adequacy and effectiveness of the information security management system*

** (ISO 27001:2013 Clause 10.2)*

Continual improvement ...

the race without a finish line!

# Managing Change

- Barriers to change:
  - Business culture may resist change
  - Size of business may inhibit change/ decisions necessary to effect change
  - Individuals may perceive conflicting priorities
  - Lack of top management commitments, and communication of that commitment
  - Lack of clearly defined plan for change

# CERTIFICATION

# Certification

- Generally two stage process
- Stage 1 – “Say what you do”  Documentation review
- Stage 2 – “Do what you say”  Evidence of effectiveness

- Three year cycle – Triennial audits
- Annual surveillance audits – only look ay elements of the system, not the entire ISMS

- Need to allow the ISMS to operate (and collect evidence) before **Stage 2 audit**

- Application form collects data on security initiatives and posture

# Course Summary

# What Have We Learned

- Information Security Management System Framework
- ISO 27001:2013
  - Required Documentation
  - Risk Management
- Annexure A Controls
  - Excellent guidance for implementation

# Documenting

**What have we learned:**

- To make ‘documentation’ appropriate to the business
- Integrate with existing management system where possible
- Keep simple and manageable!

# Implementing

## What have we learned:

- To identify a ‘champion’
- To plan out the implementation program
- To strictly monitor progress
- To keep everyone informed
- To set realistic goals

# Risk Management

**What have we learned:**

- Adopt accepted criteria
- Define acceptable risk
- Ensure repeatable results
- Perform ongoing assessments

# Monitoring

**What have we learned:**

- Monitor the ISMS
- Prepare the annual Internal ISMS Audit Program
- Conduct Internal ISMS Audits
- Conduct Management Reviews

# Improving

## What have we learned:

- To welcome suggestions
- To welcome change
- To involve everybody
- To set meaningful measurements
- To always ‘think’ improvement