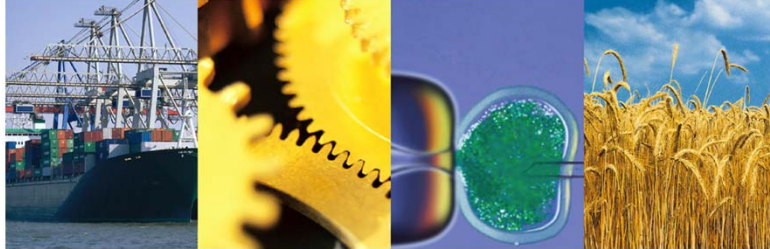


ISO/IEC 27000 Family of Standards



by Dr. Angelika Plate

07-09 June 2011, Beirut, Lebanon

June 2011



The new 27000 Family of Standards & ISO/IEC 27001



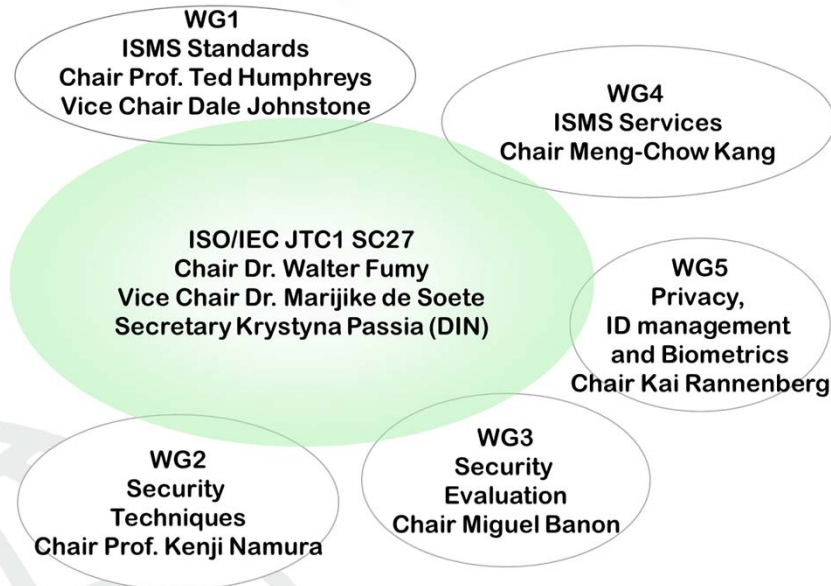
June 2011

ISO/IEC 27000 Family of Standards

2



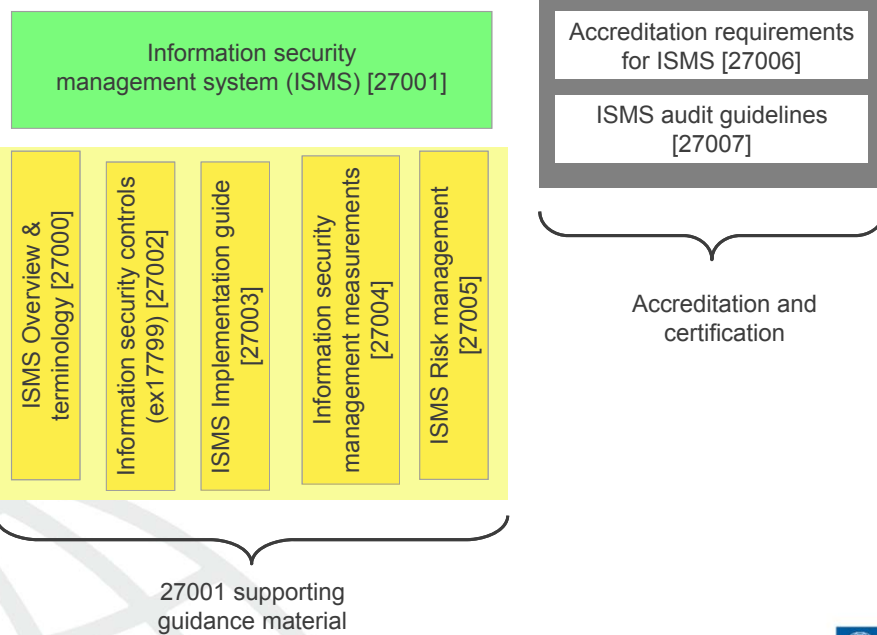
The new 27000 Family of Standards & ISO/IEC 27001



June 2011

ISO/IEC 27000 Family of Standards

3



June 2011

ISO/IEC 27000 Family of Standards

4



Standards – Title – Status

Standard	Title	Status
27000	Overview and vocabulary	WD
27001	ISMS requirements	CD
27002	Information security management Code of Practice	WD
27003	ISMS Implementation guide	Published
27004	ISM Measurements	Published
27005	ISMS Risk management	Published
27006	Accreditation requirements for certification bodies	DIS
27007	ISMS Audit guidelines	FDIS
27008	Guidance on auditing ISMS controls	Awaiting publication



Standards Development

- Study Period
- NWIP – New Work Item Proposal
- WD – Working Draft
- CD – Committee Draft
- FCD - Final CD
- DIS – Draft International Standard
- IS – International Standard



Standards – Title – Status (2)

Standard	Title	Status
27010	Sector to sector interworking and communications for industry and government	CD
27011	Information security management guidelines for telecommunications based on ISO/IEC 27002	Published
27012	ISMS guidelines for e-government	cancelled
27013	ISMS for service management	CD
27014	Information security governance framework	CD
27015	ISMS for the financial and insurance service sector	WD
27016	Information Security Management – Organizational economics	WD

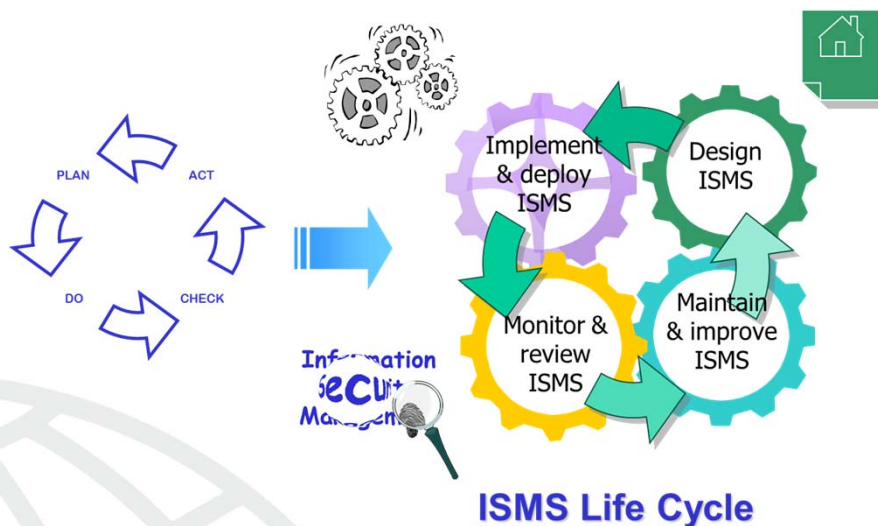
June 2011

ISO/IEC 27000 Family of Standards

7



PDCA ISMS Model



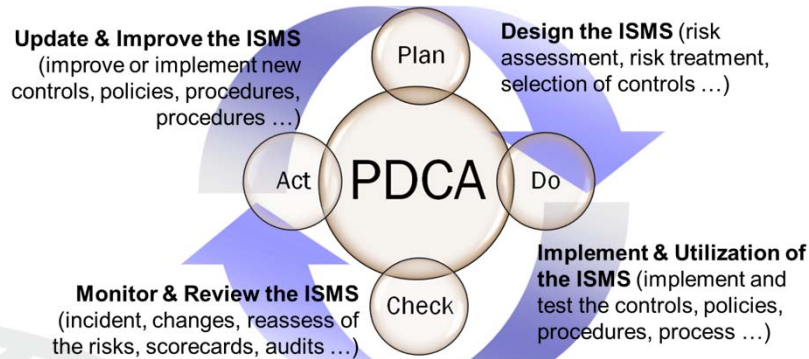
June 2011

ISO/IEC 27000 Family of Standards

8



Information Security Management System (ISMS) Process Model



Implement **risk management** processes to achieve an **effective ISMS** through a **continual improvement** process

June 2011

ISO/IEC 27000 Family of Standards

9



ISO 27001 ISMS Requirements

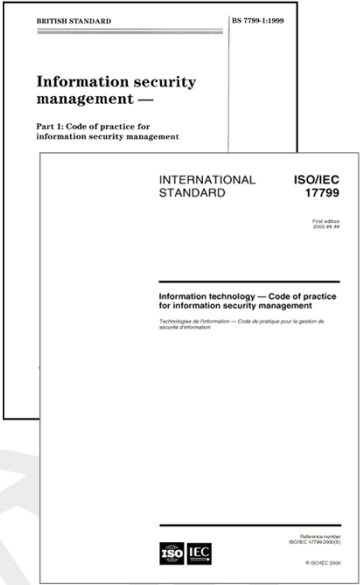
- Highlights and features
- Risk management approach
 - risk assessment
 - risk treatment
 - management decision making
- Continuous improvement model
- Measures of effectiveness
- Auditable specification (internal and external ISMS auditing)
- Now under revision

June 2011

ISO/IEC 27000 Family of Standards

10





BRITISH STANDARD
BS 7799-1:1999

Information security management —
Part 1: Code of practice for information security management

INTERNATIONAL STANDARD
ISO/IEC 17799


Information technology — Code of practice for information security management

ISO IEC

ISO/IEC 27002 Code of practice for information security management


- ❑ *A catalogue of Best Practice*
- ❑ *Suggesting a holistic set of controls*
- ❑ *Not a certification or auditable standard*

Security policy
Organising information security
Asset management
Human resources security
Physical & environmental security
Communications & operations management
Access control
Information systems acquisition, development and maintenance
Information security incident management
Business continuity management
Compliance

June 2011
ISO/IEC 27000 Family of Standards 11


ISO 27002 (prev. ISO/IEC 17799)


- Code of Practice for information security management
- In 2007 ISO/IEC 17799 was renumbered as 27002 without any content change
- The standard is now under revision



Best practice for information security

1999... TO PAY IT SAFE!

NOW, YOU CHOOSE YOUR OWN CODE!

June 2011
ISO/IEC 27000 Family of Standards 12


What is ISO/IEC 27003?

- A guide to help implementer's with taking forward the implementation requirements defined in 27001
- Scope includes implementation guidance on
 - Detailed advice and on help regarding the PDCA processes
 - ISMS Scope and policy
 - Identification of assets
 - Implementation on selected controls
 - Establishing monitoring and review processes
 - Ensuring continuous improvement
- Published in 2010

What is ISO/IEC 27004?

- Guidance on information security management measurements to support the measurement and effectiveness requirements defined in 27001
- What, how and when to measure?
- Performance, benchmarking, monitoring and review of the ISMS effectiveness to help with business decision making and improvements to the ISMS
- Published in 2009

What is ISO/IEC 27005?

- Guidance on ISMS risk management to support the risk assessment, treatment and management, and the selection of controls requirements defined in 27001
- Detailed guidance for ISMS implementers, risk managers, security officers ...
- Has been revised to align with ISO 31000
- In the process of being published

ISO/IEC 27006

- ISMS Accreditation Requirements
- Specific ISMS requirements to complement the generic requirements in ISO 17021-1
- Replaces EA 7/03
- Published January 2007 – now up for revision
- Fast revision to follow ISO 17021-1

ISO/IEC 27007

- ISMS Audit Guidelines
- Specific ISMS guidance to complement ISO 19011
- Dealing with guidance for auditors on subjects such as
 - Establishing ISMS audit trails
 - Auditing forensics
 - ISMS scopes
 - Measurements

June 2011

ISO/IEC 27000 Family of Standards

17



ISO/IEC 27008

- TR on auditing ISMS controls
- Strong focus on reviewing ISMS controls, going into some more technical details
- Scope of this standard clarifies that it relates to checking the implementation of technical controls, and that it is not suitable for ISMS audits
- Awaiting publication

June 2011

ISO/IEC 27000 Family of Standards

18



ISO/IEC 27010

- CD on sector to sector interworking and communications for industry and government
- Result of a Study Period on Critical Infrastructures
- Scope: This International Standard provides guidance for information security interworking and communications between industries in the same sectors, in different industry sectors and with governments, either in times of crisis and to protect critical infrastructure or for mutual recognition under normal business circumstances to meet legal, regulatory and contractual obligations.

Telecoms

- The ITU-T standards group Question 7/17 developed the standard X.1051 “Information security management guidelines for telecommunications based on ISO/IEC 27002”
- The aim is to support the implementation of ISO/IEC 27002 in the telecommunications sector

Telecoms

- The standard contains
 - An overview giving the framework in which it operates
 - Extended versions of the controls from ISO/IEC 27002 to address telecoms
- This standard has been adopted by SC 27 as ISO/IEC 27011 – published
- This standard was confirmed at the last meeting

ISO/IEC 27013

- Integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001
- Scope: To provide guidance on implementing an integrated information security and IT service management system
- This includes the following implementation advice:
 - Implement ISO/IEC 27001 when ISO/IEC 20000-1 is already adopted, or vice versa;
 - Implement both ISO/IEC 27001 and ISO/IEC 20000-1 together;
 - Align already existing ISO/IEC 27001 and ISO/IEC 20000-1 management systems implementations.

ISO/IEC 27014

- ISMS Governance
- Scope: To provide guidance the development and use of an information security governance framework to direct and control the ISMS processes defined in ISO/IEC 27001.
- Addressing that part of overall IT Governance that addresses security, risk and compliance with requirements
- Acts as link between management and the ISMS
 - Assigning management responsibilities
 - Supporting well informed decision-making

ISO/IEC 27015

- 1st WD for financial and insurance services
 - Scope: This international standard provides guidance for supporting the implementation of information security management in financial and insurance services sectors
 - This standard is intended to provide guidance on how to adapt the 2700x ISMS Framework. It aims to support in fulfilling sector specific information security related legal and regulatory requirements through an internationally agreed and well-accepted framework

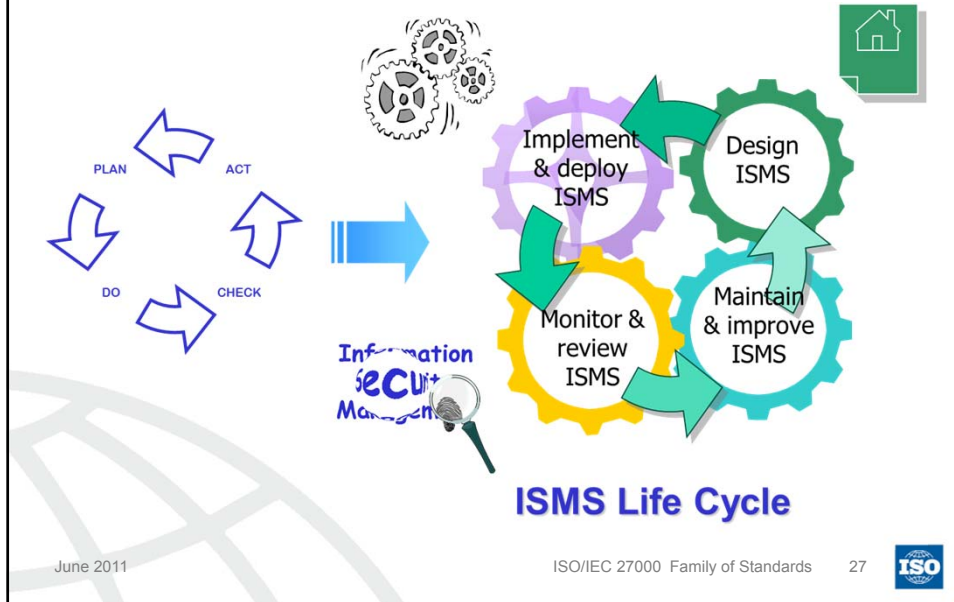
ISO/IEC 27016 and more

- 27016 deal with economical considerations for security
- Topic under research, therefore TR
- We also have a new Study Period on Cloud computing controls based on ISO/IEC 27002

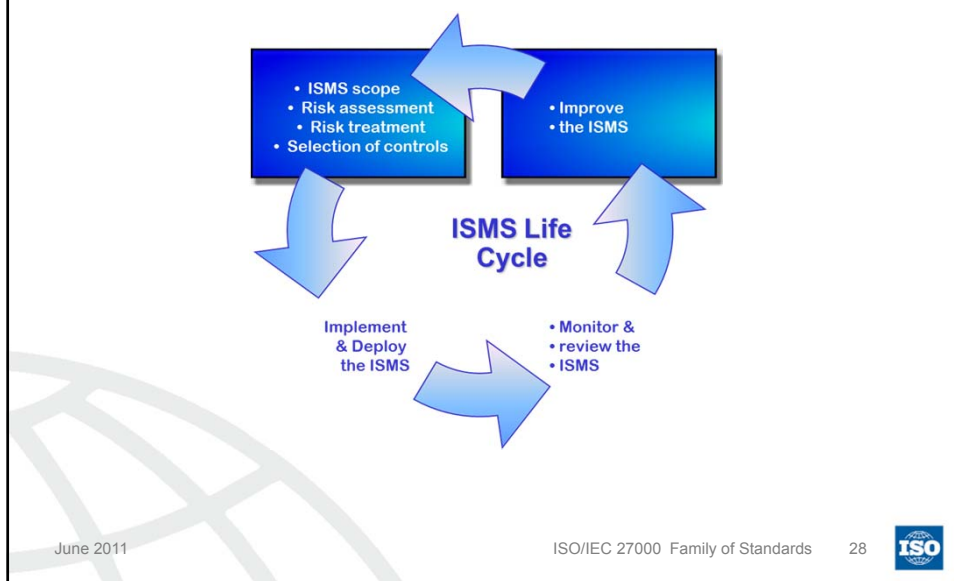
27001 ISMS



PDCA ISMS Model



27001 (PDCA) ISMS Model



27001 ISMS Scope

Design
the
ISMS

ISMS Scope (4.2.1 (a))

1. Define the scope and **boundaries** of the ISMS
2. It is entirely up to the organization to define the ISMS scope
3. Interfaces and dependencies need to be identified

ISMS Scope – Part of
the Organisation

ISMS Scope –
Whole Organisation

June 2011

ISO/IEC 27000 Family of Standards

29



27001 ISMS Scope

Design
the
ISMS

ISMS Scope (4.2.1 (a))

1. Define the scope and boundaries of the ISMS
2. It is entirely up to the organization to define the ISMS scope
3. **Interfaces and dependencies** need to be identified

External Service
Provider

ISMS Scope

Customer

IT Service Dept

June 2011

ISO/IEC 27000 Family of Standards

30



27001 ISMS Scope

Design
the
ISMS

ISMS Scope Examples

1. Sales and purchasing department
2. Outsourcing – data managed services
3. Customer repayment services
 - Insurance claims
 - Medical coverage claims
 - Return of damage goods claims
4. On-line banking
5. Internal organisational IT services

June 2011

ISO/IEC 27000 Family of Standards

31



27001 ISMS Policy

Design
the
ISMS

ISMS Policy (4.2.1 (b))

1. Define the ISMS policy that defines a framework for setting objectives and sets direction for information security:
 - Takes account of all applicable requirements, legal, contractual and business
 - Aligns with the overall risk management context of the organisation
 - Establishes criteria for risk evaluation
 - Has been approved by management

Information Security Policy	
Statement	
Objectives	
Definition of information security	
Policy requirements and rules	
.....	
.....	
.....	
Signed and approved by	
Date	

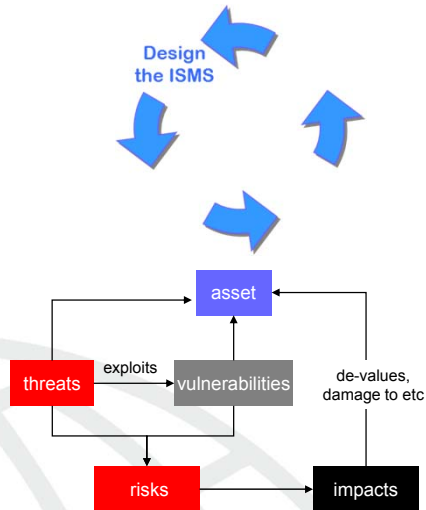
June 2011

ISO/IEC 27000 Family of Standards

32



27001 ISMS Risk Assessment



June 2011

Risk Assessment (4.2.1 (c)-(e))

1. Define the approach
2. Identify and evaluate the risks
 - Assets and their values
 - Threats and vulnerabilities
 - Risks and impacts

Example A:

Asset - customer records – commercial sensitive and value is high in financial terms

Threats – unauthorised access, leakage and modification

Vulnerabilities – lack or inappropriate control over access, lack authentication control, lack of control over processing of data

Risk – high

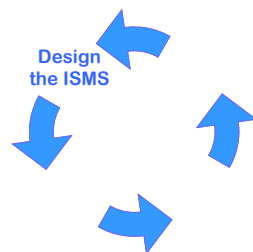
Impact - high

ISO/IEC 27000 Family of Standards

33



27001 ISMS Treatment



June 2011

Risk Treatment (4.2.1 (f))

1. Options

- **Reduce the risk** – implement controls
- **Accept the risk** – the impact the company can financially live with
- **Transfer the risk** – insurance or through contracts
- **Avoid the risk** – do not engage in a plan project cause would cause the risk

2. Management decision Making

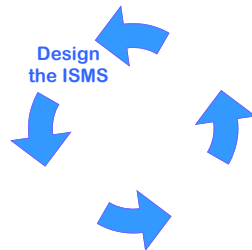
- Risk acceptance criteria and residual risks
- Business requirements
- Cost and resources

ISO/IEC 27000 Family of Standards

34



27001 ISMS Selection of Controls



Selection of controls (4.2.1 (g))

1. Controls are selected primarily from Annex A based on the risk assessment results (controls from other lists/standards could supplement what is not found in Annex A) and the decision made during the risk treatment phase
2. The selection will need to use the company criteria for accepting risk
3. The selection needs to take account of other requirements such as legal requirements

Example A continued:

- Implement better authentication and access mechanisms on the IT systems containing the customer records
- Which controls from Annex A might be applicable?

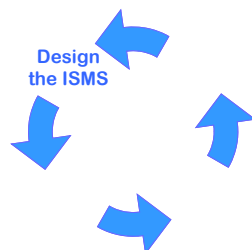
June 2011

ISO/IEC 27000 Family of Standards

35



27001 ISMS Management Approval



Management Approval (4.2.1 (h)-(i))

Approval of residual risks
Approval and authorisation to
implement ISMS controls

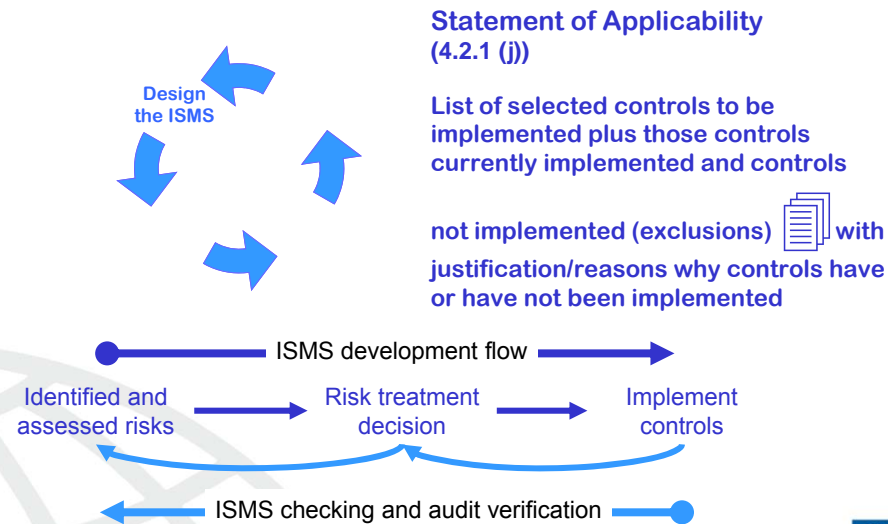
June 2011

ISO/IEC 27000 Family of Standards

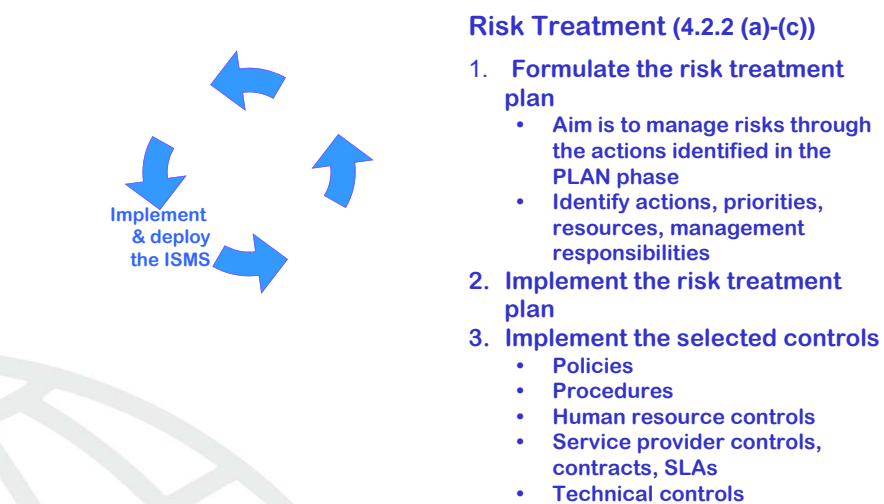
36



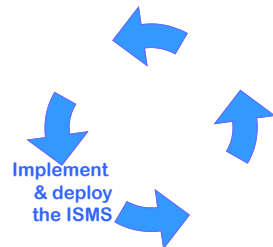
27001 ISMS Statement of Applicability



27001 Implementing ISMS Risk Treatment



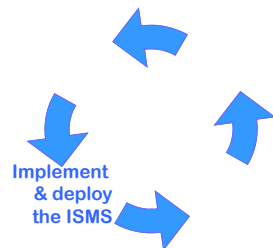
27001 Implementing ISMS Effectiveness



Effectiveness (4.2.2 (d))

1. Define a set of measurements and adopt a set methods for measuring the effectiveness of the implemented controls – after implementation and at regular periods thereafter
 - Specify how to measure the effectiveness of the selected controls or groups of controls
 - Specify how these measurements will be used to assess the effectiveness of the controls
 - Ensure comparable and reproducible results

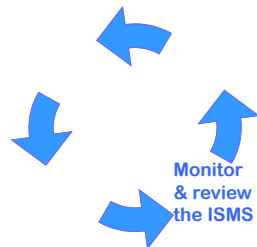
27001 ISMS Management Actions



Management Actions (4.2.2 (f)-(h))

1. Manage the resources and operations for the effective deployment of the ISMS controls
2. Ensure an effective set of procedures and resources are in place for incident handling

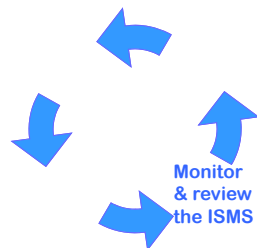
27001 (PDCA) ISMS Model



Monitor & Reviews (4.2.3)

1. Measure performance, do benchmarking etc to check the effectiveness of controls
2. Execute monitoring and review procedures to determine that everything works as expected including:
 - Access attempts
 - Use of procedures
 - Detecting errors
 - Detecting attempted breaches and incidents
 - Effectiveness
 - Risk assessment results

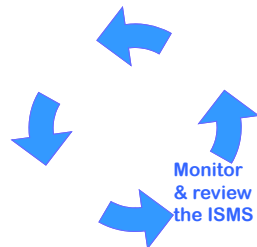
27001 (PDCA) ISMS Model



Monitor & Reviews (4.2.3)

3. Track changes
 - Risks, threats
 - Ways of doing business, new market ventures, new projects
 - Changes to workforce, clients base, business partnership
 - Technology
 - Laws and regulations
4. Undertake regular reviews (management reviews) and audits (internal and external audits) of the ISMS, taking account of:
 - Incident management reports
 - Effectiveness measurements
 - Suggestions and feedbacks
 - Audit reports
 - Management actions and their closure

27001 (PDCA) ISMS Model

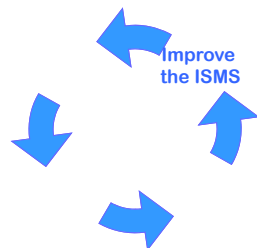


Monitor & Reviews (4.2.3)

5. Update all relevant documentation

- Policies
- Procedures
- Plans
- Test schedules
- Review and audit manuals

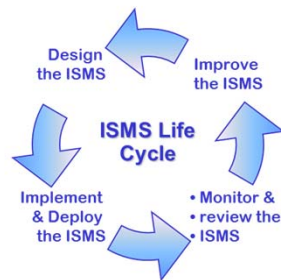
27001 (PDCA) ISMS Model



Update & improve (4.2.4 and 8.1-8.3)

1. Implement the improvements identified in the CHECK phase
2. Take corrective and preventive action (more in clause 8 ISMS Improvement)
3. Communicate actions and improvements to all interested parties
4. Ensure that the improvements work as intended
5. Retrain staff

27001 ISMS Documentation



Documentation

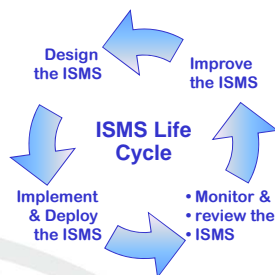
ISMS Scope and policy statement
 Risk Assessment report
 Risk Treatment Plan
 Statement of Applicability
 ISMS Procedures
 ISMS manuals
 Audit manuals



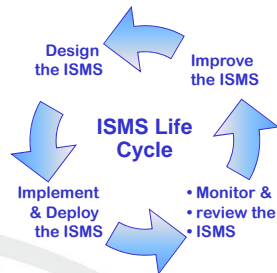
27001 ISMS Documentation

Controls (4.3.2)

- Control and protect the documents, using procedures for
 - Approval, review, update and re-approval
 - Change and version control
 - Ensuring documents are valid and accessible
 - Ensuring availability to all with right to access
 - Identifying origin and distribution
 - Preventing unintended use
 - Applying suitable identification and labelling



27001 ISMS Records



Records

Incident handling records
 Personnel records
 Training records
 Customer contract, sales and delivery records
 Sales records
 Financial records
 Test records
 Benchmarking records



June 2011

ISO/IEC 27000 Family of Standards

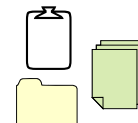
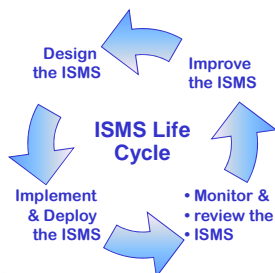
47



27001 ISMS Records

Controls (4.3.3)

- Records shall be established to provide evidence of the conformance with the standard
 - For certification, the ISMS should have been in operation for at least 4-6 months to have sufficient evidence
- Records need to be protected in the same way as all documentation
- The requirements for documentation and records are the same as for other management systems



June 2011

ISO/IEC 27000 Family of Standards

48



Management commitment

Management shall provide commitment by:

- Establishing ISMS policy, objectives and plans
- Establishing roles and responsibilities for information security
- Communicating the importance of information security
- Providing sufficient resources for the ISMS
- Deciding on criteria for risk acceptance
- Ensuring internal ISMS audits
- Conducting management reviews

Provision of resources

The organization shall determine and provide resources necessary to:

- Establish, implement, operate, monitor, review, maintain and improve an ISMS
- Ensure that information security supports the business requirements
- Identify and address legal and regulatory requirements and contractual security obligations
- Maintain adequate security by correct application of all implemented controls
- Carry out reviews and, where required, improve the effectiveness of the ISMS

Training, awareness and competence

The organization shall ensure competent personnel by

- Determining the necessary competencies for personnel in the ISMS
- Providing training or taking other actions (e.g. employing competent personnel) to satisfy these needs
- Evaluating the effectiveness of the actions taken
- Maintaining records of education, training, skills, experience and qualifications
- Ensuring awareness of the personnel in the ISMS

Internal ISMS audits

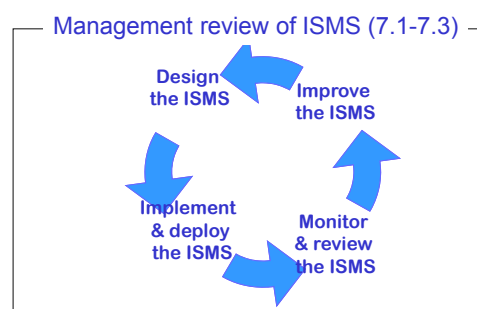
The organization shall conduct internal ISMS audits at planned intervals to ensure that the ISMS

- Conforms to the requirements of ISO/IEC 27001 and relevant legislation or regulations;
- Conforms to the identified information security requirements;
- ISMS processes and controls are effectively implemented and maintained and perform as expected

Internal ISMS audits

- The audit programme needs to be planned
- Audit criteria, scope, frequency and methods shall be defined
- Impartiality and independence of auditors needs to be ensured
- The responsibilities for planning and conducting the audit and for reporting shall be defined
- Management is responsible for the appropriate follow-up actions to react to any identified non-conformities

27001 ISMS Management Reviews

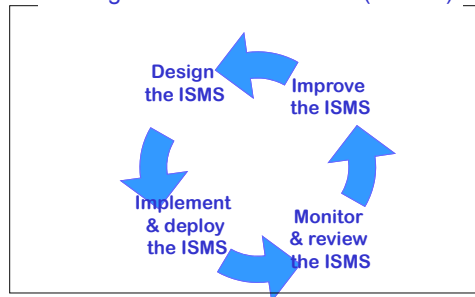


Management Review

1. At least once a year
2. Check to ensure continued ISMS suitability, adequacy and effectiveness
3. Opportunities for improvements
4. Updating of policies, procedures, plans, objectives ...
5. Results of the review are documents and meeting actions to be recorded

27001 ISMS Management Reviews

Management review of ISMS (7.1-7.3)



Review Input

1. Results of reviews, audits, effectiveness measurements, incident reports, operational records
2. Feedback from staff, customers, business partners, suppliers
3. Threat, vulnerability and risk profiles
4. New or additional controls, technology, procedures to improve ISMS
5. Follow-up actions – including status of corrective and preventive actions

June 2011

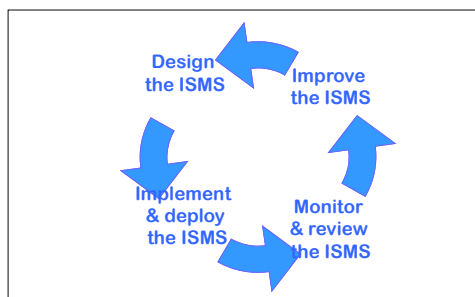
ISO/IEC 27000 Family of Standards

55



27001 ISMS Management Reviews

Management review of ISMS (7.1-7.3)



Review Output

1. Defining improvements to the ISMS
2. Effectiveness targets and improvements to methods and measures
3. Updates to risk assessment and treatment plans
4. Updates to policies, procedures, plans
5. Restating of resource needs, re-deployment and definition of roles and responsibilities

June 2011

ISO/IEC 27000 Family of Standards

56



ISMS improvements

- The organization shall continually improve the effectiveness of the ISMS
- Corrective actions
 - Identifying non-conformities and their causes
 - Determining and implementing corrective actions
- Preventive actions
 - Identifying potential non-conformities
 - Determining and implementing preventive actions
- All actions shall be recorded and reviewed

Information about the Revisions



Schedule of the Revisions

- Both revisions (27001 and 27002) are at slow progress (1st CD after 4 WDs and 4th WD)
- ISO/IEC 27002 is likely to need at least one more Working Draft – ends possibly in 2013
- ISO/IEC 27001 might end 2012
- Whether or not both revisions should be published together still needs to be discussed

Revision of 27001 - Framework

- ONLY necessary changes – no changes for the sake of change
- Clear distinction between
 - Requirements in 27001
 - Guidance in the other 2700x standards
- Guidance documents should be aligned with ISO/IEC 27001 – not the other way round
- All terms and definitions in ISO/IEC 27000
- Alignment with ISO 31000

ISMS policy and information security policy in 27002

- Considerable overlap between ISMS policy in ISO/IEC 27001 and information security policy in ISO/IEC 27002
- Decisions:
 - Keep the terms as is
 - ISMS policy in 27001 with only minor changes, addressing information security management
 - Refer only to the ISMS policy in 27001
 - The information security policy is a high level document that is issued by top management
 - Changes in ISO/IEC 27002 have been agreed to reduce the overlap between the two policies

Top Management

- It was discussed and agreed to distinguish between management and top management
- Consideration: the ISMS scope is not always the whole organisation – how “top” should “top management” be?
- Agreement: Top management denotes that level of management which is the highest within the Scope of the ISMS, i.e. the level of management that has ownership of and ultimate authority over and responsibility for the ISMS

Selection of Controls & Annex A

- The issue of Annex A and other control sets was discussed again and again
- Decisions:
 - Annex A is the recommended basis for the selection of controls
 - Other control sets can also be used, more liberty is allowed in the selection process
 - Additional controls can always be selected
 - The Statement of Applicability stays as is

JTCG Structure (1)

- In 2009, ISO TMB (Technical Management Board) started an initiative regarding the combination of management system standards in JTCG:
 - Task Force 1: Definition of a common structure and of identical text
 - Task Force 3: Terms and definitions
- Both activities should harmonize ALL management system standards
- Fast progress, the final versions are expected by the end of this year
- Great idea – but a lot of impact on existing management systems

Current Table of Contents

3	Terms and definitions.....	1
4	Context of the organization	1
4.1	Understanding the organization and its context.....	1
4.2	Understanding the needs and expectations of interested parties	2
4.3	Determining the scope of the management system.....	2
4.4	Information security management system	2
5	Leadership.....	2
5.1	General	2
5.2	Management commitment	2
5.3	Policy.....	3
5.4	Organizational roles, responsibilities and authorities	3
6	Planning	4
6.1	Actions to address risks and opportunities.....	4
6.2	Information Security objectives and plans to achieve them	4
7	Support.....	5
7.1	Resources	5
7.2	Competence	5
7.3	Awareness	5
7.4	Communication	5
7.5	Documented information	6
7.5.1	General	6
7.5.2	Create and update	6
7.5.3	Control of documented information	7
8	Operation.....	7
8.1	Operational planning and control.....	7
9	Performance Evaluation	10
9.1	Monitoring, measurement, analysis and evaluation	10
9.2	Internal Audit.....	10
9.3	Management review.....	10
10	Improvement	11
10.1	Nonconformity and corrective action	11
10.2	Continual improvement	12

June 2011

ISO/IEC 27000 Family of Standards – 65



Typical Identical Text

9.2 Internal Audit

The organization shall conduct internal audits at planned intervals to provide information to assist in the determination of whether the information security management system

- conforms to
 - the organization's own requirements for its information security management system
 - the requirements of this International Standard.
- is effectively implemented and maintained.

June 2011

ISO/IEC 27000 Family of Standards – 66



Identical Text and ISO/IEC 27001

7.1 Resources

The organization shall determine and provide the resources needed for the information security management system.

In particular, sufficient resources shall be provided to:

- ensure that information security procedures support the business requirements;
- maintain adequate information security by correct application of all implemented controls.

Revision of ISO/IEC 27002

- A lot of comments have been received, the resolution process is still ongoing
- Overview of the [changes made so far](#)
- These changes need a lot more discussion, this document is still in an intermediate state

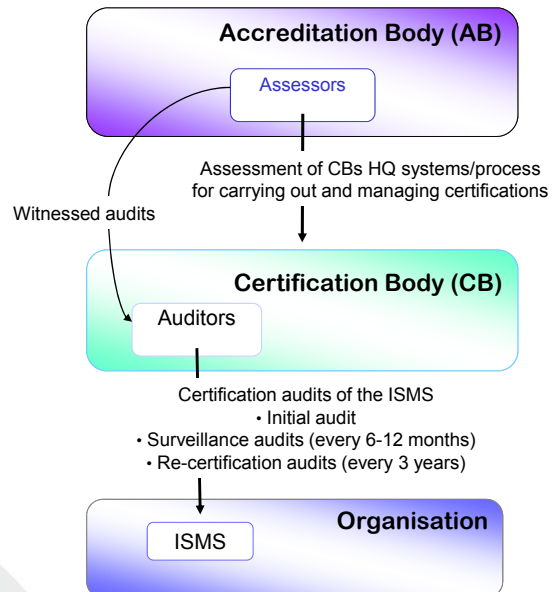
Compliance & Certification



Certification

- Stakeholders
 - Accreditation Bodies, Certification Bodies and End users
- Certification documents and standards
- Accreditation Process
- Certification Process
- Auditors
- All certificates currently registered can be viewed on www.iso27001certificates.com

Accreditation Certification



June 2011

ISO/IEC 27000 Family of Standards

71



ISMS Certification documents and standards

- Certification standard
 - ISO/IEC 27001:2005 (previously BS 7799 Part:2002)
- Accreditation Guidelines
 - ISO/IEC 17021 (prev. ISO Guide 62/EN 45012)
 - ISO/IEC 27006 (prev. EA 7/03), ISO 19011
- Supporting documents
 - ISO/IEC 27002

June 2011

ISO/IEC 27000 Family of Standards

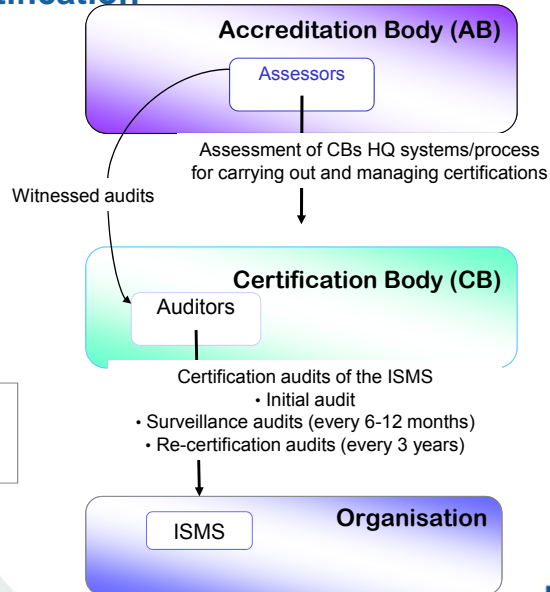
72



Accreditation Certification

Documents used:
(a) ISO/IEC 17021
(b) ISO 19011
(c) ISO/IEC 27006

Documents used:
(d) ISO/IEC 27001:2005
(c) ISO/IEC 27006



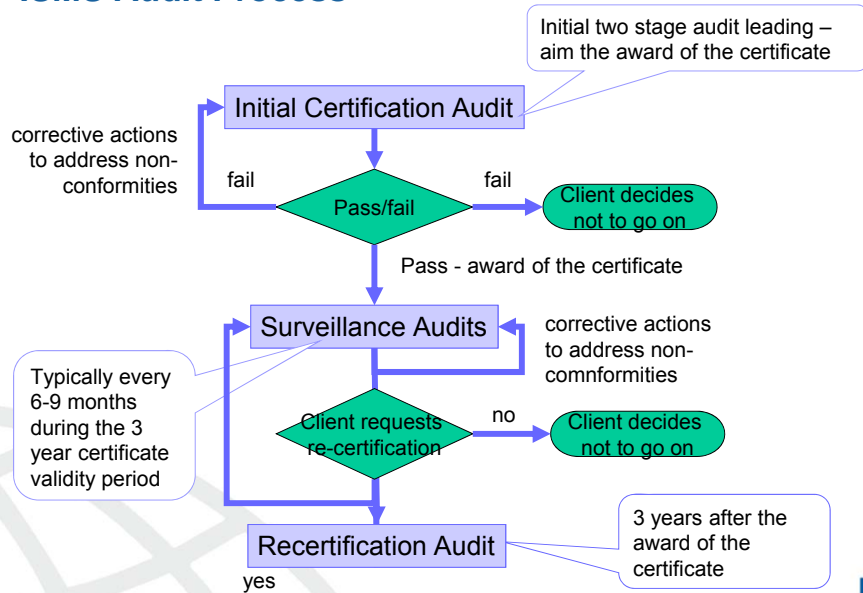
June 2011

ISO/IEC 27000 Family of Standards

73



ISMS Audit Process



June 2011

ISO/IEC 27000 Family of Standards

74



ISMS Audit Process

- Typically the initial audit process involves a two stage process
- Stage 1 Audit
 - Review of ISMS documents ...
- Stage 2 Audit
 - On-site visit
 - Meetings with management team
 - Interviews with staff
 - Observation and assessment of the ISMS in operation
 - Review and discussion of findings, documents, records, reports ...
 - Collection of objective evidence

ISMS Audit Process

- Stage 1 Audit
 - In this stage of the audit, the certification body shall obtain documentation on the design of the ISMS covering the documentation required in Clause 4.3.1 of ISO/IEC 27001.
 - The objective of the stage 1 audit is to provide a focus for planning the stage 2 audit by gaining an understanding of the ISMS in the context of the client organization's ISMS policy and objectives, and, in particular, of the client organization's state of preparedness for the audit.
 - The stage 1 audit includes, but should not be restricted to, the document review. The certification body shall agree with the client organization when and where the document review is conducted. In every case, the document review shall be completed prior to the commencement of the stage 2 audit.
 - The results of the stage 1 audit shall be documented in a written report. The certification body shall review the stage 1 audit report before deciding on proceeding with the stage 2 audit and for selecting the stage 2 audit team members with the necessary competence.
 - The certification body shall make the client organization aware of the further types of information and records that may be required for detailed examination during the stage 2 audit.

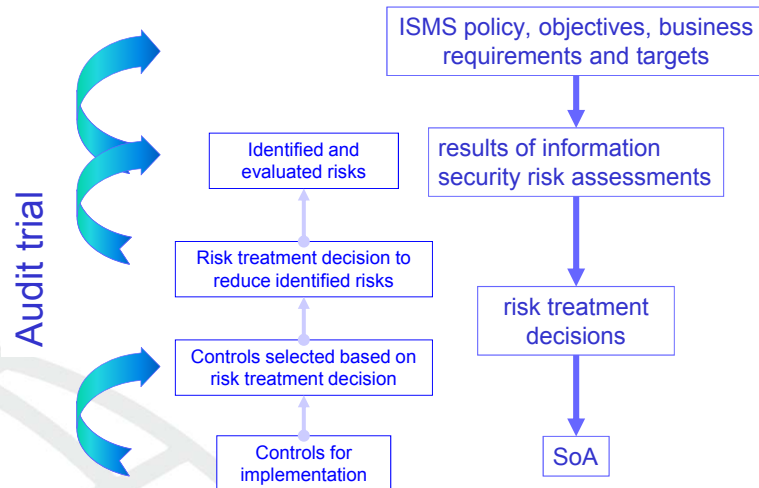
ISMS Audit Process

- Stage 2 Audit
 - Objectives of this audit are:
 - To confirm that the client organization adheres to its own policies, objectives and procedures;
 - To confirm that the ISMS conforms to all the requirements of the normative ISMS standard ISO/IEC 27001 and is achieving the client organization's policy objectives.
 - This audit always takes place at the site(s) of the organisation
 - The certification body drafts an audit plan for this stage 2 audit based on the stage 1 findings.

ISMS Audit Process

- Stage 2 Audit
 - The audit should focus on the organization's
 - Assessment of information security related risks and that the assessment produces comparable and reproducible results
 - Selection of control objectives and controls based on the risk assessment and risk treatment processes
 - Reviews of the effectiveness of the ISMS and measurements of the effectiveness of the information security controls, reporting and reviewing against the ISMS objectives
 - Correspondence between the selected and implemented controls, the Statement of Applicability, and the results of the risk assessment and risk treatment process, and the ISMS policy and objectives
 - Programmes, processes, procedures, records, internal audits, and reviews of the ISMS effectiveness to ensure that these are traceable to management decisions and the ISMS policy and objectives

ISMS Audit Process



June 2011

ISO/IEC 27000 Family of Standards

79



ISMS Audit Process

■ Stage 2 Audit (Specific Elements of the Audit)

- The role of the certification body is to establish that client organizations are consistent in establishing and maintaining procedures for the identification, examination and evaluation of information security related threats to assets, vulnerabilities and impacts on the client organization. Certification bodies shall:
 - a) Require the client organization to demonstrate that the analysis of security related threats is relevant and adequate for the operation of the client organization;
 - b) Establish whether the client organization's procedures for the identification, examination and evaluation of information security related threats to assets, vulnerabilities and impacts and the results of their application are consistent with the client organization's policy, objectives and targets.

June 2011

ISO/IEC 27000 Family of Standards

80



ISMS Audit Process

- Stage 2 Audit (Specific Elements of the Audit)
 - Regulatory Compliance
 - The maintenance and evaluation of legal and regulatory compliance is the responsibility of the client organization. The certification body shall restrict itself to checks and samples in order to establish confidence that the ISMS functions in this regard. The certification body shall verify that the client organization has a management system to achieve legal and regulatory compliance applicable to the information security risks and impacts.
 - Combining management system audits
 - ISMS audit can be combined with audits of other management systems. This combination is possible provided it can be demonstrated that the audit satisfies all requirements for certification of the ISMS. All the elements important to an ISMS shall appear clearly, and be readily identifiable, in the audit reports. The quality of the audit shall not be adversely affected by the combination of the audits.

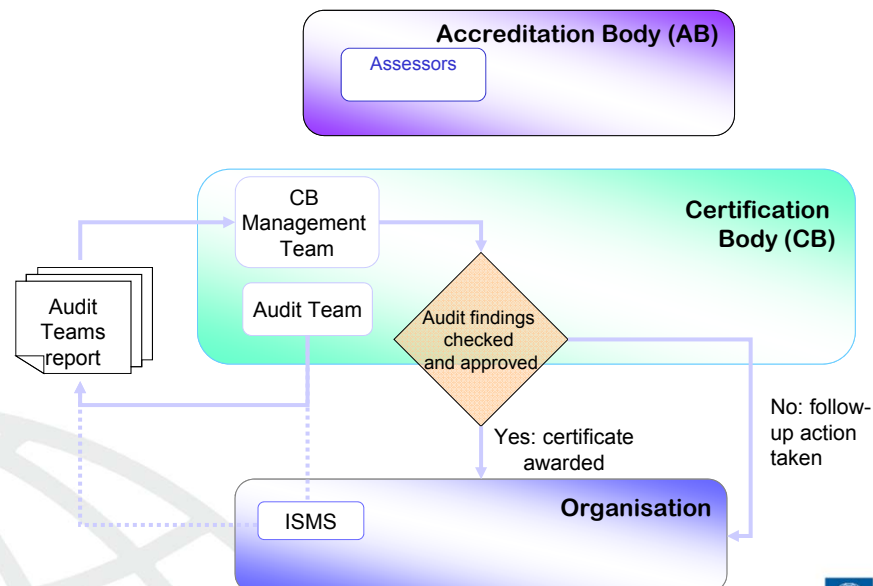
June 2011

ISO/IEC 27000 Family of Standards

81



Accreditation Certification



June 2011

ISO/IEC 27000 Family of Standards

82



ISMS Auditor Qualifications

- ISO/IEC 19011 (Audit Guidelines) (available from www.iso.org)
 - Education
 - Industrial experience
 - Training
 - Audit experience
- IRCA Certificated Auditors (www.irca.org)
 - Provisional Auditor
 - Auditor
 - Lead Auditor

ISO/IEC 27006

- ISO/IEC 27006 is the “Requirements for the accreditation of bodies providing certification of ISMSs”
 - Joint initiative from ISO, IAF and CASCO
- Based on
 - ISO/IEC 17021
 - ISO/IEC 27001
- Currently under revision to align with the new version of ISO/IEC 17021

The Use of Shall & Should

- ISO/IEC 27006 contains requirements
 - No requirements for general auditing that are additional to ISO/IEC 17021
 - “Shall” is used to indicate mandatory requirements from ISO/IEC 17021, ISO/IEC 27001, or those resulting from their combination
 - “Should” is guidance, but a recognised means to fulfil the requirements

Structure of ISO/IEC 27006

- ISO/IEC 27006 follows the structure from ISO/IEC 17021
 - A high level statement of what the clause in ISO/IEC 17021 contains
 - ISMS Guidance – if there is additional guidance necessary for the ISMS, this is included here

7 Resource requirements

7.1 Competence of management and personnel

The requirements from ISO/IEC 17021:2006, Clause 7.1 apply. In addition, the following ISMS-specific requirements and guidance apply.

7.1.1 IS 7.1 Management competence

The essential elements of competence required to perform ISMS certification are to select, provide and manage those individuals whose skills and collective competence is appropriate to the activities to be audited and the related information security issues.

7.1.1.1 Competence analysis and contract review

The certification body shall ensure that it has knowledge of the technological and legal developments relevant to the ISMS of the client organization, which it assesses.

The certification body shall have an effective system for the analysis of the competencies in information security management which it needs to have available, with respect to all the technical areas in which it operates.

For each client, the certification body shall be able to demonstrate that it has performed a competence analysis (assessment of skills in response to evaluated needs) of the requirements of each relevant sector prior to undertaking the contract review. The certification body shall then review the contract with the client organization, based on the results of this competence analysis. In particular, the certification body shall be able to demonstrate that it has the competence to complete the following activities:

- a) understand the areas of activity of the client organization and the associated business risks;
- b) define the competencies needed in the certification body to certify in relation to the identified activities, and information security related threats to assets, vulnerabilities and impacts on the client organization;
- c) confirm the availability of the required competencies.

7.1.1.2 Resources

The management of the certification body shall have the necessary processes and resources to enable it to determine whether or not individual auditors are competent for the tasks they are required to perform within the scope of certification in which they are operating. The competence of auditors may be established by verified background experience and specific training or briefing (see also Annex B). The certification body shall be able to communicate effectively with all those clients it provides services to.

What is in ISO/IEC 27006?

- Section 9 “Process Requirements”
 - 9.1.1 Specific ISMS Guidance on general ISMS audit requirements for
 - Certification audit criteria
 - Policies and procedures
 - Audit team
 - 9.1.2 Specific ISMS Guidance on the scope
 - CB shall ensure that the scope is defined as required in ISO/IEC 27001
 - CB shall ensure that the risk assessment reflects the scope
 - Special emphasis on interfaces and the need to address them

What is in ISO/IEC 27006?

- Section 9 “Process Requirements”
 - 9.1.3 Specific ISMS Guidance on audit time
 - Not(!) specifying a particular time frame
 - Listing factors that can influence the time needed for the audit
 - ISMS complexity, size of scope, type and diversity of business, number of sites,...
 - Reference to Annex A.3

What is in ISO/IEC 27006?

- Section 9 “Process Requirements”
 - 9.1.4 Multiple sites
 - Specific ISMS guidance contains the usual information
 - Representative sampling, partly random and partly risk based
 - Every site with significant risks is audited prior to certification
 - The surveillance programme should eventually cover all sites

What is in ISO/IEC 27006?

- Three annexes – all informal
 - Annex A.1 Analysis of Complexity
 - Estimating the complexity of an ISMS
 - Annex A.2 Example Areas of Auditor Competence
 - Competence needed for the different control areas and the ISMS
 - Annex A.3 Audit Time
 - Describing the process to determine the audit time
 - Example calculations based on IAFGD 2, plus additional days for ISMS/controls
 - Annex A.4 Guidance on reviewing Annex A controls



Which of the following is true?

- ISO/IEC 27002 is an auditable standard
- ISO/IEC 27001 does not mandate a specific risk assessment method
- All standards ISO/IEC 27002 – ISO/IEC 27005 contain only guidance
- Conducting internal ISMS audits is not a requirement
- It is up to the organization to define measurements for control effectiveness
- ISO/IEC 27001 requires that documents are controlled
- Continual improvement does include corrective and preventive action
- ISO/IEC 27002 contains the requirement to conduct management reviews
- Certification audits always consist of Stage 1 and Stage 2



ISO/IEC 27001 Risk Assessment & Risk Management



Risk Management Approaches

- ISO/IEC 27001 does not specify the risk assessment/management approach to be used
- It is up to the organization to specify what to use (as in 4.2.1 c))
- ISO/IEC 27001 gives the framework and ISO/IEC 27005 some more helpful information

ISO/IEC 27005

- ISO/IEC 27005 – Information security risk management
 - Provides guidance for information security risk management as laid out in ISO/IEC 27001
 - Is applicable for all organizations (size, type of business, etc.) that need to manage information security risks
- Published in 2007
- Currently considered for revision to align with ISO 31000

June 2011

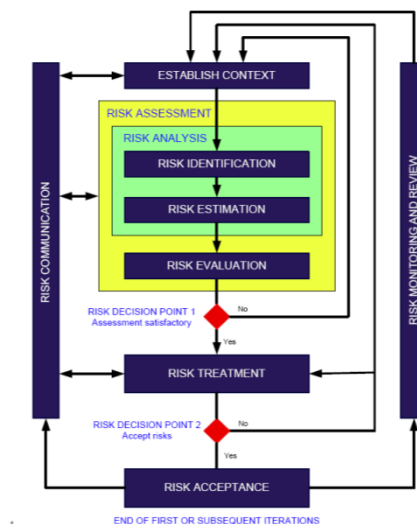
ISO/IEC 27000 Family of Standards

95



ISO/IEC 27005 - Model

- Risk management process in ISO/IEC 27005



June 2011

ISO/IEC 27000 Family of Standards

96



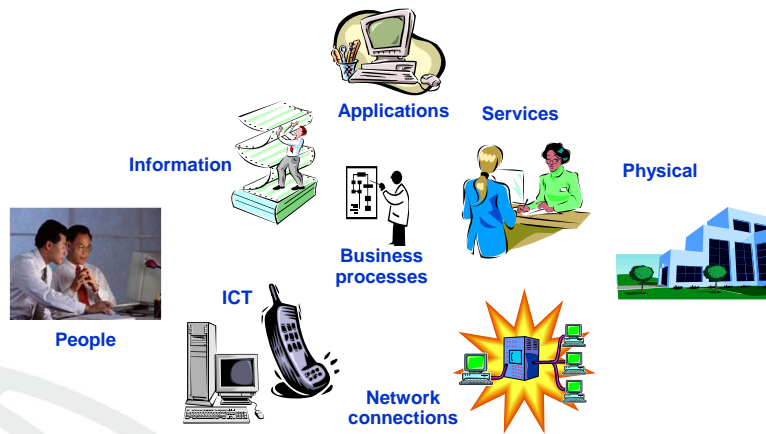
ISO/IEC 27005 - Content

- ISO/IEC 27005 does not specify a “right” risk assessment/management approach
- Considers qualitative and quantitative analyses
- Currently concentrates on risk assessment and risk treatment
- Additions on risk monitoring and risk review are still needed
- Revision ONLY to align with ISO 31000

ISO/IEC 27005 - Annexes

- ISO/IEC 27005 contains a number of useful annexes
 - Asset valuation
 - Impact assessment
 - Example lists of threats
 - Example lists of vulnerabilities, related to specific information security areas
 - Discussion of several risk assessment approaches
 - A lot of information about the selection of controls (based on the old ISO/IEC 13335-4)

Risk Domains



June 2011

ISO/IEC 27000 Family of Standards

99



Assets in the ISMS

- All assets within the ISMS boundary should be identified
- To understand the assets and their role in the ISMS, it is helpful to identify them as part of the ISMS subdivisions
- This should include
 - Assets related to the ISMS via interfaces
 - Dependencies to ensure consistent protection

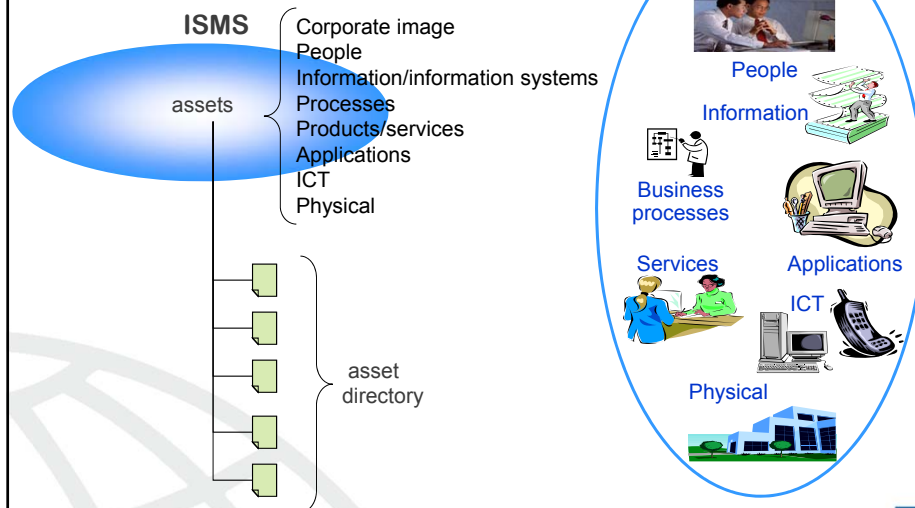
June 2011

ISO/IEC 27000 Family of Standards

100



ISMS Assets



June 2011

ISO/IEC 27000 Family of Standards

101



Measuring asset importance

- What is the most important asset in your organisation?
- Factors that influence importance:
 - What happens if the asset is damaged?
 - Is the asset useful to the organisation, how difficult is it to conduct business without it?
 - Does the asset relate to critical applications, resources etc?

June 2011

ISO/IEC 27000 Family of Standards

102



How to measure?

- Different 'values' of an asset
 - Money (e.g. replacement costs)
 - Value expressing the criticality
 - Values expressing the potential impact and damage to the business from a loss of
 - Confidentiality
 - Integrity
 - Availability
 - Values associated with other classifications (e.g. breach of legislation)

Asset valuation scale

- How many levels
 - 3, 4 or 5 or how many?
 - The difference between the levels must be easy to explain
- The meaning of these different levels should be expressed in words, for each
 - Confidentiality
 - Integrity
 - Availability
 - Potential other criteria

Identifying requirements

- Identifying requirements for the assets
 - Legal and contractual obligations that the asset (or its environment) has to fulfil
 - Business requirements that relate to the asset
- Necessary input into the valuation
- Example: information with the requirement to comply with the Data Protection Act
 - High valuation for confidentiality and integrity

Legal / Contractual requirements

- Identify all legislation and regulation applicable for the ISMS and its assets
 - See also ISO/IEC 27002, Section 12.1
- Identify contractual obligations
 - Consider all existing contracts
 - Identify the obligations in there
 - Service level agreements
 - Compliance with security policies and procedures
 - Rights to audit in third party contracts
 - IPR requirements
 - ...

Business requirements

- Identify all business requirements applicable for the ISMS and its assets resulting from
 - Specific applications such as Internet, E-Commerce etc.
 - Business issues such as joint ventures, requirements for correct business processing, requirements for timely delivery, etc.
 - Availability requirements for information and services, e.g. resulting from customer requirements

Asset classifications

Confidentiality Requirements (C)		
Asset Value	Class	Description
1 - LOW	Publicly available	Non-sensitive information and information processing facilities and system resources available to the public.
2 - MEDIUM	For internal use only or restricted use only	Non-sensitive information restricted to internal use only, i.e. not publicly available or restricted information and information processing facilities and system resources available within the organisation with varying restrictions based on business needs.
3 - HIGH	In-Confidence or Strictest-In-Confidence	Sensitive information and information processing facilities and system resources available on a need-to-know basis only, or sensitive information and information processing facilities and system resources available on a strict need-to-know basis only.

Asset classifications

Integrity Requirements (I)		
Asset Value	Class	Description
1 - LOW	Low integrity	The unauthorized damage or modification of information is not critical to business applications and business impact is negligible or minor.
2 - MEDIUM	Medium integrity	The unauthorized damage or modification of information is not critical but noticeable to business applications and business impact is significant.
3 - HIGH	High or very high integrity	The unauthorized damage or modification of information is critical to business applications and business impact is major and could lead to serious or total failure of business application.

Asset classifications

Availability Requirements (A)		
Asset Value	Class	Description
1 - LOW	Low availability	The asset (information, information processing system, system resources/network services, people etc.) can be tolerated to be not available for more than a day.
2 - MEDIUM	Medium availability	The asset (information, information processing system, system resources/network services, people etc.) can be tolerated to be not available for a at most half day to a day.
3 - HIGH	High availability	The asset (information, information processing system, system resources/network services, people etc.) cannot be tolerated to be not available for more than a few hours or even less.

Assets - Summary

- The protection of assets is the aim of information security and risk management
 - Each asset should
 - Be identified and valued to allow appropriate protection to be given
- An owner/custodian should be identified
- And an inventory/list should be produced, including
 - Classification, storage and date of entry/update
 - Owner, location, type of asset, where used,...

Exercise

- 4 Groups:
 - IT Department
 - Human Resource Department
 - Finance Department
 - Online Banking Service
- Identify 5 assets in your department
- Identify the values of these assets for
 - Confidentiality
 - Integrity
 - Availability
- Use the asset valuation scale from this course

Existing controls

- All already implemented or planned controls need to be identified
- This is necessary to
 - Identify threats and vulnerabilities in a realistic background
 - Check whether these controls are really necessary or remove them, if not
 - Identify during the risk assessment process where these controls are working correctly or need to be improved
 - Select new controls that suit to those already existing

Identifying existing controls

- Existing controls can be easily identified using a Gap Analysis, which helps to
 - Put the existing controls in relation with those in ISO/IEC 27002
 - Can be adjusted in detail, as necessary
 - Can be done through
 - Check tables/Q&A
 - Interviews
 - Walking around
 - Round table discussions

Compliance Grades



NO
PARTIAL
YES

- Grades ...
 - YES – fully implemented as described in ISO/IEC 27002
 - PARTIAL – anything from almost complete to a lot of gaps between the actual implementation and ISO/IEC 27002
 - NO – not implemented at all
 - NOT APPLICABLE – not suitable for the organization, e.g. technically not feasible to implement

High Level Gap Analysis Table

Control	Question	Y/P/ N/NA	Comments
Information Security Policy			
5.1.1	Is published policy policy document, approved by management, available to all users responsible for information security?	Partial	It has been produced and approved by management but not published yet – see CISP/001/v1.0.
5.1.2	Is the published policy reviewed regularly and appropriate?	No	But it will be after its been published.
Internal Organization			
6.1.1	Is the management committed to information security and gives clear direction and support for security initiatives?	Yes	The management fully supports the ISO/IEC 27001 initiatives.
6.1.2	Are security initiatives and measures coordinated through a cross-functional forum?	Not Applicable	This is a small business and this can be handled at a day-to-day working level.
6.1.3	Are responsibilities for the protection of individual assets and for carrying out specific processes clearly defined?	Partial	Additional responsibilities still need to be assigned in line with the security policy.

Detailed

Gap Analysis Table

Question	Y/P/ N/NA	Comments
Control 5.1.1 - Information Security Policy Document		
Is the security policy implemented?	Yes	It is published and further action for communication will be taken in the next month.
Is the policy approved by management?	Yes	Yes, it has been approved by management.
Is the policy been published and communicated to all employees and relevant external parties?	Partial	It has been published to all employees, but not yet externally.
Does everybody understand the security policy, its purpose and implications?	No	Not yet, but special training will be used to achieve that in the next month.
Does the policy contain all relevant issues mentioned in Control 5.1.1?	Yes	The policy has been developed completely in line with ISO/IEC 27002.
Is the security policy supported by more detailed policies (e.g. for software or Internet)?	Partial	There is an access control policy and incident handling guidelines, but currently no Internet policy.

Threats & vulnerabilities

- Vulnerabilities are weaknesses, e.g. security weaknesses in the system
- Threats are anything that could cause damage, harm or loss to an organisation's assets by exploiting the vulnerabilities of these assets
- Threats and vulnerabilities need to come together to cause a risk

Threats can result from ...

- Attacks from the outside, e.g. trying to break into an organisation's networks or premises
 - Hackers, spam
- Attacks from the inside using insider knowledge and opportunities
 - Example: bank in Germany where 8 mio € vanished
- Accidentally due to system failures or geographical factors
 - Floods, hurricanes, earthquakes
 - System overload

Threat examples

- Unauthorised access
- Malicious code
- Theft, by insiders or outsiders
- Misuse of information processing systems
- Fraud
- System failure
- Denial of service
- User errors
- Disasters
-

Identifying threats

- Identifying threats for the assets
 - Looking at the target of the threat
 - What could threaten this asset?
 - Insiders or outsiders
 - System failures or disasters
 - Identifying the threats
 - Who or what causes the threat?
 - Who could benefit from initiating the threat?
 - What has happened in the past?
 - How likely is this to happen (again)?

Vulnerabilities are there ...

- Due to inadequate personnel, management and administrative controls
 - Policies, procedures and guidelines
 - Compliance
- In computer software or communications equipment, in networks, systems/applications
- In the physical environment

Vulnerability examples

- Lack of awareness
- Lack of clear responsibilities
- Wrong information classification
- Inability to provide evidence
- Lack of change or version control
- Lack of maintenance
- Inappropriate identification and authentication
- Lack of media security
- Lack of physical protection
-

June 2011

ISO/IEC 27000 Family of Standards

123



Identifying vulnerabilities

- Identifying vulnerabilities of the asset
 - What are security problems of this asset?
 - Are controls missing for this asset?
 - Are flaws in the current protection mechanisms?
- Identifying vulnerabilities in the environment?
 - What is the technical environment like?
 - What about connections, networks etc.?
 - How secure is the physical environment?
 - Is the personnel well trained, aware of security and compliant with the controls?

June 2011

ISO/IEC 27000 Family of Standards

124



Incidents

- Threats and vulnerabilities only cause risks if they come together and cause incidents
- Assessing them together helps to
 - Ease the risk assessment process
 - Makes the assessment less theoretical and more realistic
- Don't combine all identified threats and vulnerabilities without thinking
- Take account of the existing controls

Sources of information

- Internal Company Resources
 - Security incident reports
 - Results of system audits & security reviews
 - Observing business processes & working/operational conditions,
 - Talking to asset/system owners & users
- Internet
 - CERT
 - SANS
 - ...

Valuation scale

- How many levels
 - 3, 4 or how many?
 - The difference between the levels must be easy to explain
- The meaning of these different levels should be expressed in words, explaining the differences in likelihood for the incidents to occur

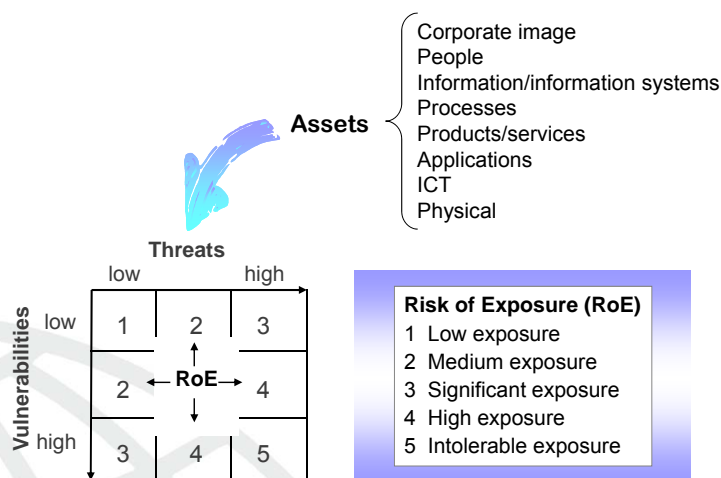
Valuation

- How likely is it that a threat/vulnerability combination occurs?
- How much could a possible attacker be attracted?
- How often has it happened in the past?
- How easy is it to exploit the vulnerabilities?
- How good are the controls in place?

T/V Valuation - Separate

- Threats
 - 1 – low likelihood
 - 2 – medium likelihood
 - 3 – likely to occur
- Vulnerability
 - 1 - Difficult to exploit, good protection
 - 2 - Possible to be exploited
 - 3 - Easy to exploit, little protection

Risk of Exposure



Exercise

- 4 Groups:
 - IT Department
 - Human Resource Department
 - Finance Department
 - Research & Development
- For the identified 3 assets:
- Identify at least 2-3 threat/vulnerability combinations that apply
- Identify how likely the T/V combinations are to occur
- Use a 3 level scale (low, medium, high)

Risk matrix

IMPACT	RISK OF EXPOSURE				
	1	2	3	4	5
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7

1 (low)	2	3	4	5	6	7	8 (very high)
---------	---	---	---	---	---	---	---------------

————— increasing severity of the risk —————→

Risk matrix

IMPACT	RISK OF EXPOSURE		
	LOW	MEDIUM	HIGH
Low	1	3	5
Medium	2	4	6
High	3	5	7
Very High	4	6	8

Risk Level

Impact	RoE			
	1	2	3	
1				
2				
3				5
				6
			5	6
				7

Risk level

- 1 Tolerable/negligible
- 2 } Minor
- 3 Significant
- 4 } Major
- 5 } Major
- 6 Intolerable
- 7

BUSINESS IMPACT

- Low** (*insignificant, inconsequential, trivial, negligible*)
- Low-Medium** (*noteworthy, considerable but not major*)
- Medium** (*significant, major*)
- Medium-High** (*serious damage, potentially disastrous*)
- High** (*devastating damage, total failure, complete shutdown*)

Relating the risk numbers

- The risk scale needs to be related to your business as its your business that faces the risks. The numbers 1 to 8 in the example below (and used in the risk matrix) may have many different meanings and interpretations. Before being able to decide how to reduce and manage the risk your business needs to specify what each number means in their business context e.g. 6 might be interpreted as a loss of £100,000 to one business and £700,000 to another.

IMPACT	RISK OF EXPOSURE		
	LOW	MEDIUM	HIGH
Low	1	3	5
Medium	2	4	6
High	3	5	7
Very High	4	6	8

Risk & impact

Impact	Risk of Exposure		
	LOW	MEDIUM	HIGH
Low	1	3	5
Medium	2	4	6
High	3	5	7
Very High	4	6	8

1 = Negligible loss or damage

2 = Some loss or damage

3 = Minor loss or damage

4 = Noticeable loss or damage

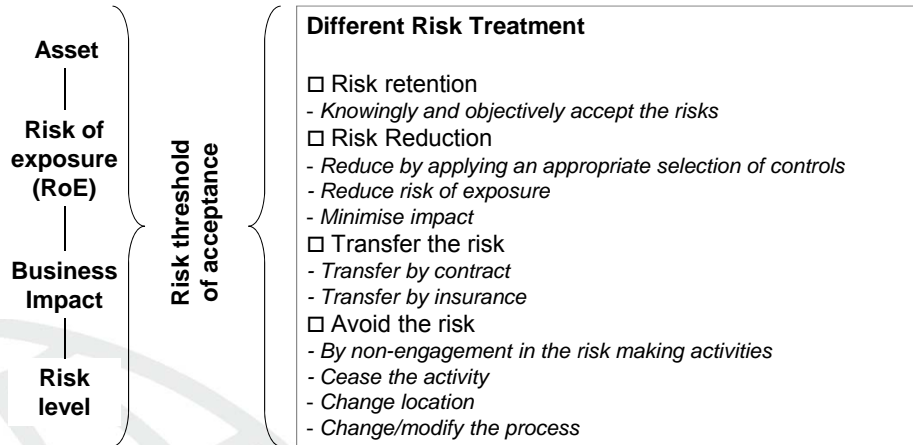
5 = Major loss or damage

6 = Significant loss or damage

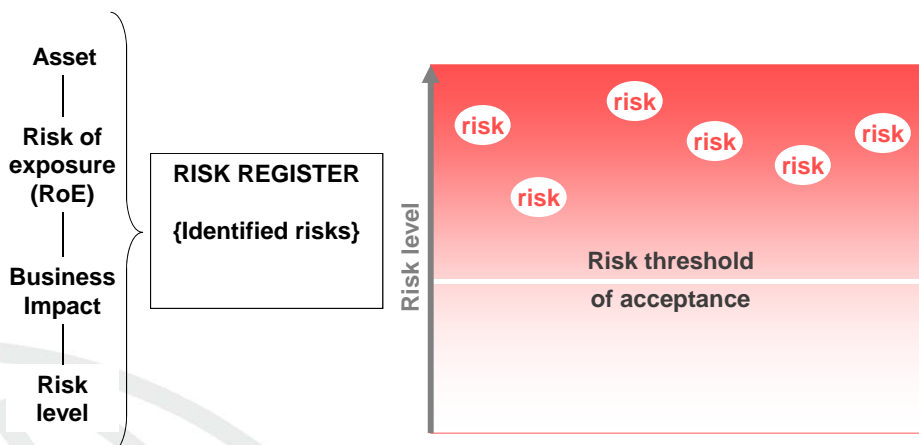
7 = Serious loss or damage

8 = Total loss or damage

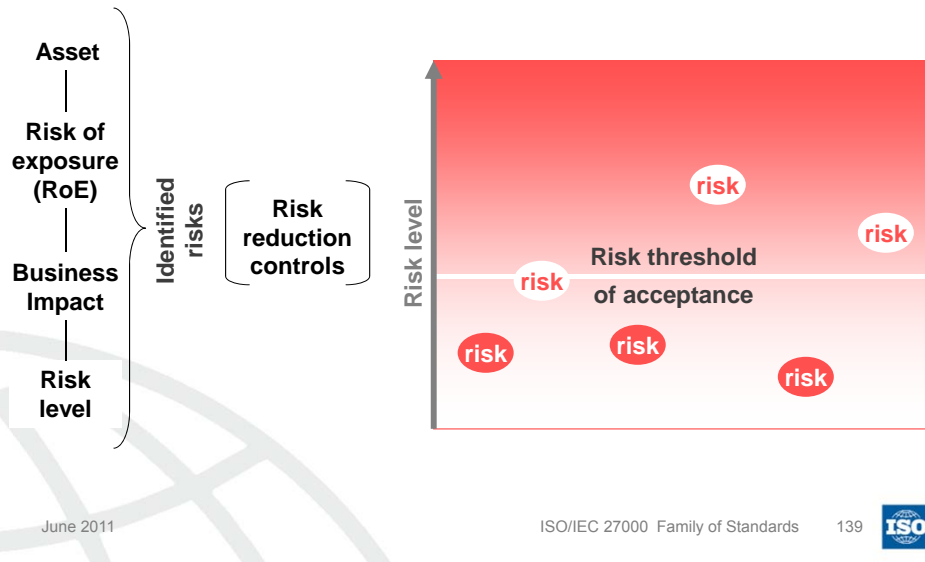
Risk Treatment



Risk Threshold



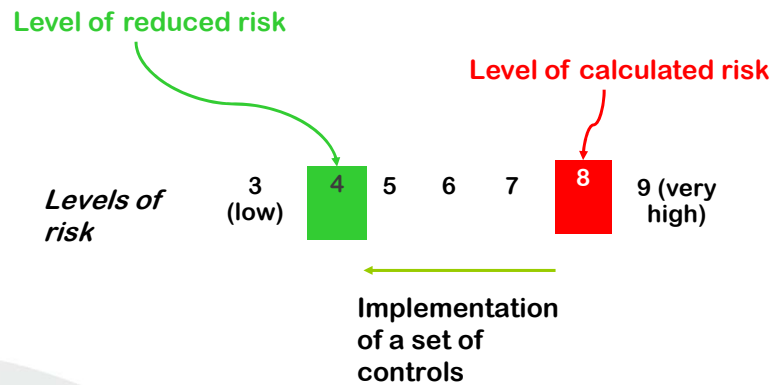
Risk Reduction



Risk Reduction by Controls

- The identified risks should be reduced to an acceptable level
- Risk reduction through
 - reducing the vulnerability – e.g. improving the user identification and authentication procedures
 - reducing the threat – e.g. putting a well configured and managed firewall in place to protect against attacks from the outside
 - protecting against the risk effects – e.g. using encryption to protect against any attacks that still might occur

Risk Reduction



For example this reduction may have been possible through the combination of improvements in operational procedures, training in their use and better technical access control mechanisms

June 2011

ISO/IEC 27000 Family of Standards

141



Risk Reduction – How does it work?

- Risk reduction is always difficult to assess
 - Controls help to reduce the risk
 - How much does a particular control reduce the likelihood of a threat/vulnerability combination to occur?
- ISO/IEC 27001 requires that risk reduction is considered
- The best way to do this is to identify over time how well controls manage the risks

June 2011

ISO/IEC 27000 Family of Standards

142



Statement of Applicability

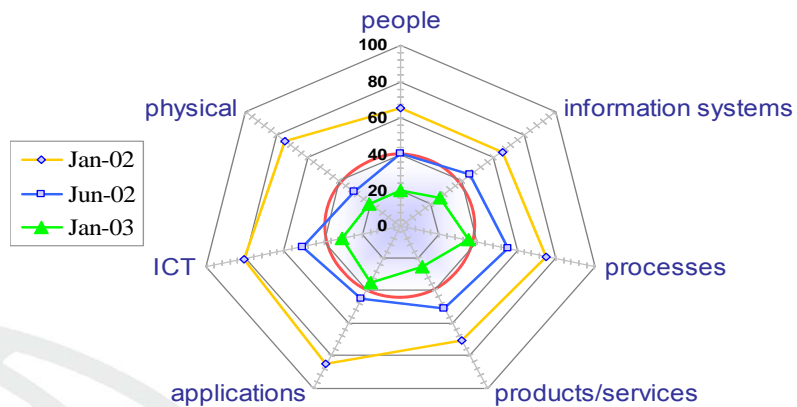
- The Statement of Applicability should contain
 - The selected control objectives and controls, and the reasons for their selection
 - All currently implemented controls (see results of the Gap Analysis)
 - Any exclusion of control objectives or controls from ISO/IEC 27001 Annex A and the reason for the exclusion

Statement of Applicability – Example

	Control Objective & Control	Y/P/ N/NA	Comments and Reasons
Information Security Policy			
A.5.1	To provide management direction and support for information security ...	Yes	This needs to be in place for the whole ISMS (see RAR Page 4).
A.5.1.1	Information security policy document	Yes	The policy needs to be completed to cover all elements as in ISO/IEC 27002, 5.1.1 .
A.5.1.2	Review of the information security policy	Yes	The policy will be reviewed in accordance with the ISP Review Procedure .
Internal Organization			
A.6.1	To manage information security within the organization	Yes	This needs to be in place for the whole ISMS (see RAR Page 6).
A.6.1.1

RAR = Risk Assessment Report

Risk Control



June 2011

ISO/IEC 27000 Family of Standards

145



Risk Assessment Tools

- There are plenty of tools available for risk assessment and risk management
- To select a tool the following should be considered
 - The tool needs to cover the risk assessment/management process as in ISO/IEC 27001
 - The tool should suit to the organization
 - The tool should cover all control areas in ISO/IEC 27002

June 2011

ISO/IEC 27000 Family of Standards

146



RA2 art of risk

- RA2 art of risk has been specially designed for ISO/IEC 27001 and ISO/IEC 27002
- It goes through the whole risk assessment process from identifying the ISMS scope to the Statement of Applicability
- It includes all controls from
 - ISO/IEC 27002:2000 and
 - ISO/IEC 27002:2005

Exercise

- 4 Groups:
 - IT Department
 - Online Service
 - Human Resource Department
 - Finance Department
- For the identified risks:
- Select controls to reduce the risk
- Use the controls from Annex A, and additional controls, where necessary

ISO/IEC 27002 Code of Practice For Information Security Management



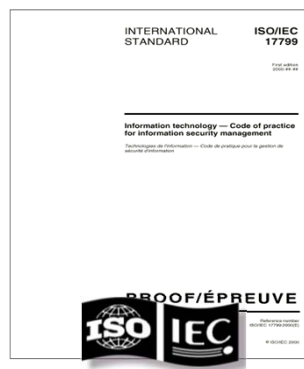
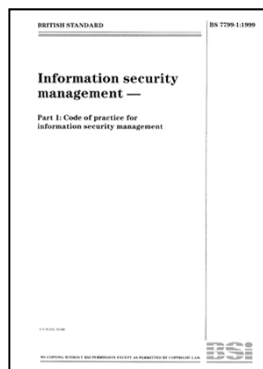
June 2011

ISO/IEC 27000 Family of Standards

149



ISO/IEC 27002 – Development over time



1995-1998

BS 7799 Part 1
Code of practice
BS 7799 Part 2
ISMS specification

June 2011

1999

Revisions of
Parts 1 & 2
published

2000

BS 7799 Part 1
published as
ISO/IEC 17799

15th June
2005

First revision
of ISO/IEC
17799

ISO/IEC 27000 Family of Standards

150



OLD & NEW

2000 edition	2005 edition
Security policy	Security policy
Security organisation	Organising information security
Asset classification & control	Asset management
Personnel security	Human resources security
Physical & environmental security	Physical & environmental security
Communications & operations management	Communications & operations management
Access control	Access control
Systems development & maintenance	Information systems acquisition, development and maintenance
	Information security incident management
Business continuity management	Business continuity management
Compliance	Compliance

June 2011

ISO/IEC 27000 Family of Standards

151



Clause 4 Risk Assessment & Treatment

- Introduction to information security risk assessment and treatment
- Alignment with ISO/IEC 27001 and ISO/IEC 27005 (the revised version of ISO/IEC 13335)
- Inclusion of risk assessment in the scope
- Emphasising the importance of risk assessment

June 2011

ISO/IEC 27000 Family of Standards

152



5.1 Information Security Policy

- 5.1.1 Information security policy document
 - An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties.
- 5.1.2 Review of the information security policy
 - The information security policy should be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

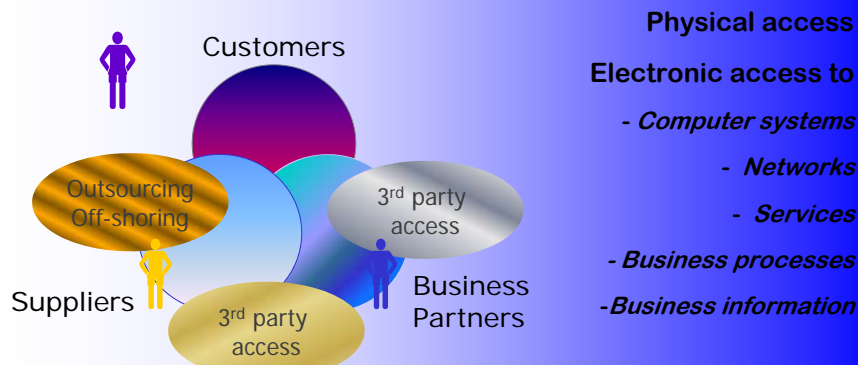
6.1 Internal Organization

- 6.1.1 Management commitment to information security
 - Management should actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.
- 6.1.2 Information security co-ordination
 - Information security activities should be co-ordinated by representatives from different parts of the organization with relevant roles and job functions.
- 6.1.3 Allocation of information security responsibilities
 - All information security responsibilities should be clearly defined.

6.1 Internal Organization

- 6.1.4 Authorization process for information processing facilities
- 6.1.5 Confidentiality agreements
- 6.1.6 Contact with authorities
- 6.1.7 Contact with specialist interest groups
- 6.1.8 Independent review of information security

IMPROVING the management of EXTERNAL RISKS



6.2 External Parties

- 6.2.1 Identification of risks related to external parties
- 6.2.2 Addressing security when dealing with customers
- 6.2.3 Addressing security in third party agreements

7 Asset Management

Responsibility for assets

- 7.1.1 Inventory of assets
- 7.1.2 Ownership of assets
- 7.1.3 Acceptable use of assets

Information classification

- 7.2.1 Classification guidelines
- 7.2.2 Information labelling and handling

Example Asset Inventory

Asset ID	Asset Type	Owner & Location	Value		
			C	I	A
XS1	Operating system A				
XS2	Operating system B				
XS3	Application S/W & Utilities				
...			
XH1	Server	System Administrator			
XH2	Desktop machines				
...			
XIS1	Information System A	Head of Human Resources			
XIS2	Information System B	Head of Finance Group			
...			
XC1	Communications Equip.	Communications Manager			
...			
XP1	CCTV	Head of Property & Office Management			
...			

June 2011

ISO/IEC 27000 Family of Standards

159



8 Human Resources Security Before, during & termination of employment

8.1 Prior to Employment

8.1.1 Roles and responsibilities

8.1.2 Screening

8.1.3 Terms and conditions of employment

8.2 During Employment

8.2.1 Management responsibilities

8.2.2 Information security awareness, education & training

8.2.3 Disciplinary process

8.3 Termination or Change of Employment

8.3.1 Termination responsibilities

8.3.2 Return of assets

8.3.3 Removal of access rights

June 2011

ISO/IEC 27000 Family of Standards

160



9 Physical Security

Secure areas

- 9.1.1 Physical security perimeter
- 9.1.2 Physical entry controls
- 9.1.3 Securing offices, rooms and facilities
- 9.1.4 Protecting against external and environmental threats
- 9.1.5 Working in secure areas
- 9.1.6 Public access, delivery and loading areas

9 Physical Security

Equipment security

- 9.2.1 Equipment siting and protection
- 9.2.2 Supporting utilities
- 9.2.3 Cabling security
- 9.2.4 Equipment maintenance
- 9.2.5 Security of equipment off premises
- 9.2.6 Secure disposal or re-use of equipment
- 9.2.7 Removal of property

10.1 Operational Procedures and Responsibilities

- 10.1.1 Documented operating procedures
- 10.1.2 Change management
- 10.1.3 Segregation of duties
- 10.1.4 Separation of development, test and operational facilities

10.2 Third Party Service Delivery Management

- 10.2.1 Service delivery
- 10.2.2 Monitoring and review of third party services
- 10.2.3 Managing changes to third party services
- Based on BS 15000/ISOIEC 20000

10.3 System Planning and 10.4 Malicious Code

System planning and acceptance

- 10.3.1 Capacity management
- 10.3.2 System acceptance

Protection against Malicious & Mobile Code

- 10.4.1 Controls against malicious code
- 10.4.2 Controls against mobile code

Back-Up, Network Management and Information Handling

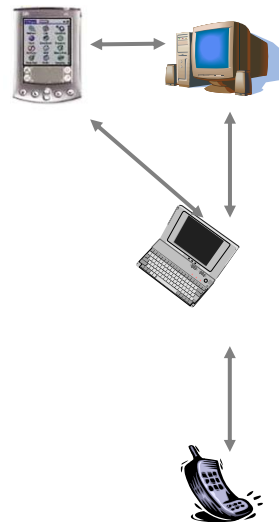
- 10.5 Back-up
 - 10.5.1 Information back-up
- 10.6 Network management
 - 10.6.1 Network controls
 - 10.6.2 Security of network services
- 10.7 Information handling
 - 10.7.1 Management of removable media
 - 10.7.2 Disposal of media
 - 10.7.3 Information handling procedures
 - 10.7.4 Security of system documentation

10.8 Exchange of Information

- 10.8.1 Information exchange policies and procedures
- 10.8.2 Exchange agreements
- 10.8.3 Physical media in transit
- 10.8.4 Electronic messaging
- 10.8.5 Business information systems

10.9 Electronic Commerce Services

- 10.9.1 Electronic commerce
- 10.9.2 On-line transactions
- 10.9.3 Publicly available systems

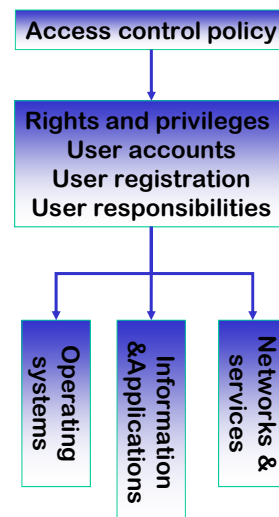


10.10 Monitoring

- 10.10.1 Audit logging
- 10.10.2 Monitoring system use
- 10.10.3 Protection of log information
- 10.10.4 Administrator and operator logs
- 10.10.5 Fault logging
- 10.10.6 Clock synchronization

11.1 Business Requirement for Access Control

- 11.1.1 Access control policy
 - An access control policy should be established, documented, and reviewed based on business and security requirements for access



11.2 User Access Management

- 11.2.1 User registration
- 11.2.2 Privilege management
- 11.2.3 User password management
- 11.2.4 Review of user access rights

11.3 User Responsibilities

- 11.3.1 Password use
- 11.3.2 Unattended user equipment
- 11.3.3 Clear desk and clear screen policy

11.4 Network Access Control

- 11.4.1 Policy on use of network services
- 11.4.2 User authentication for external connections
- 11.4.3 Equipment identification in the network
- 11.4.4 Remote diagnostic and configuration port protection
- 11.4.5 Segregation in networks
- 11.4.6 Network connection control
- 11.4.7 Network routing control

11.5 Operating System Access Control

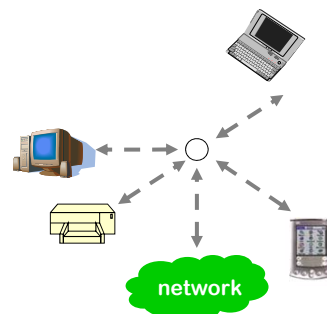
- 11.5.1 Secure log-on procedures
- 11.5.2 User identification and authentication
- 11.5.3 Password management system
- 11.5.4 Use of system utilities
- 11.5.5 Session time-out
- 11.5.6 Limitation of connection time

11.6 Application and Information Access Control

- 11.6.1 Information access restrictions
- 11.6.2 Sensitive system isolation

11.7 Mobile Computing & Teleworking

- 11.7.1 Mobile computing and communications
- 11.7.2 Teleworking



12.1 Security Requirements of Information Systems

- 12.1.1 Security requirements analysis and specification

12.2 Correct Processing in Applications

- 12.2.1 Input data validation
- 12.2.2 Control of internal processing
- 12.2.3 Message integrity
- 12.2.4 Output data validation

12.3 Cryptographic Controls

- 12.3.1 Policy on the use of cryptographic controls
 - Encryption
 - Digital signatures
 - Non-repudiation services
- 12.3.2 Key management

12.4 Security of System Files

- 12.4.1 Control of operational software
- 12.4.2 Protection of system test data
- 12.4.3 Access control to program source code

12.5 Security in Development and Support Processes

- 12.5.1 Change control procedures
- 12.5.2 Technical review of applications after operating system changes
- 12.5.3 Restrictions on changes to software packages
- 12.5.4 Information leakage
- 12.5.5 Outsourced software development

12.6 Technical Vulnerability Management

- 12.6.1 Control of technical vulnerabilities
 - Identify vulnerabilities
 - Define how to react to these vulnerabilities
 - Test carefully prior to installing patches
 - Keep and audit trail of what has been done

Link to ISO/IEC 18044

- Aligning with the definitions from ISO/IEC 18044, differentiating between
 - *Information security event* – the occurrence of any information security relevant situation is identified
 - *Information security incident* – only applies to those events that have a significant probability to cause a security problem

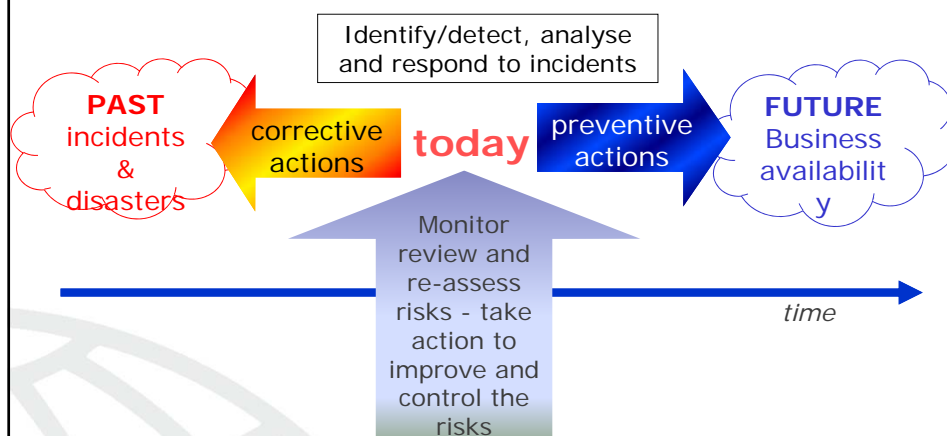
13.1 Reporting Information Security Events and Weaknesses

- 13.1.1 Reporting information security events
- 13.1.2 Reporting security weaknesses

13.2 Management of Information Security Incidents & Improvements

- 13.2.1 Responsibilities and procedures
- 13.2.2 Learning from information security incidents
- 13.2.3 Collection of evidence

Business TAKING ACTION to Control its INCIDENTS



14 Business Continuity Management

- 14.1.1 Including information security in the business continuity management process
- 14.1.2 Business continuity and impact analysis
- 14.1.3 Developing and implementing continuity plans including information security
- 14.1.4 Business continuity planning framework
- 14.1.5 Testing, maintaining and re-assessing business continuity plans

Business Continuity & Information Security

**Overall
Business
Continuity**

Business continuity framework
Risk management processes
Developing plans, guidelines and
Implementing these plans
Testing and reviewing the plans

Information
Security
Management
Process

15 Compliance

15.1 Compliance with legal requirements

- 15.1.1 Identification of applicable legislation
- 15.1.2 Intellectual property rights (IPR)
- 15.1.3 Protection of organizational records
- 15.1.4 Data protection and privacy of personal information
- 15.1.5 Prevention of misuse of information processing facilities
- 15.1.6 Regulation of cryptographic controls

15 Compliance

- 15.2 Compliance security policies and standards and technical compliance
 - 15.2.1 Compliance with security policies and standards
 - 15.2.2 Technical compliance checking
- 15.3 Information systems audit considerations
 - 15.3.1 Information systems audit controls
 - 15.3.2 Protection of information systems audit tools

More about the 27000 Family of Standards



June 2011

ISO/IEC 27000 Family of Standards

191



<http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>

June 2011

ISO/IEC 27000 Family of Standards

192



ISO/IEC 27003

ISO/IEC 27003 - Overview

- Concentration on the pure “implementation” issue, no discussion of the CHECK and ACT phase of the ISMS
- Design agreements:
 - No specification of minimal content or definition of requirements for implementation
 - No particular ways of implementing an ISMS
 - Examples, case studies

Critical Success Factors

- Management commitment
- Good governance within the organization
- Financial considerations
- Industry/sector-specific considerations
- Consideration of the overall risk situation
- Co-operation with other organisations
- Recognising the need for changes and updates

Related Issues

- Integration with other management systems
 - Identification of common elements, e.g. in the “management system” part
 - Responsibility for the other management systems
 - Clear identification of all ISMS documentation (required by ISO/IEC 27006)
- Compliance with laws and regulations
 - Important to identify all applicable laws and regulations
 - Inclusion in the requirements in the “PLAN” stage

Structure of the Chapters

- All chapters addressing the implementation workflow have the same structure
 - Overview
 - Objectives
 - Preconditions
 - Organising the work
 - Who to involve
 - How is it done?
 - Results

PLAN-Phase

The Plan Phase has several steps that should be followed for the implementation of this process. Each step provides input to the next step as a logical flow. This step-by-step procedure is exemplified by flow diagrams in this section. Each step is described in such a manner that an organisation that is not familiar with information security and/or ISO or similar management standards may understand what is intended.

Navigation area

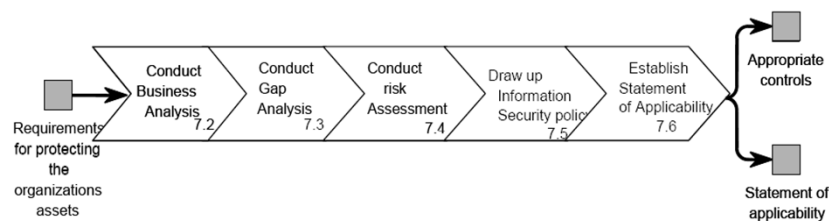
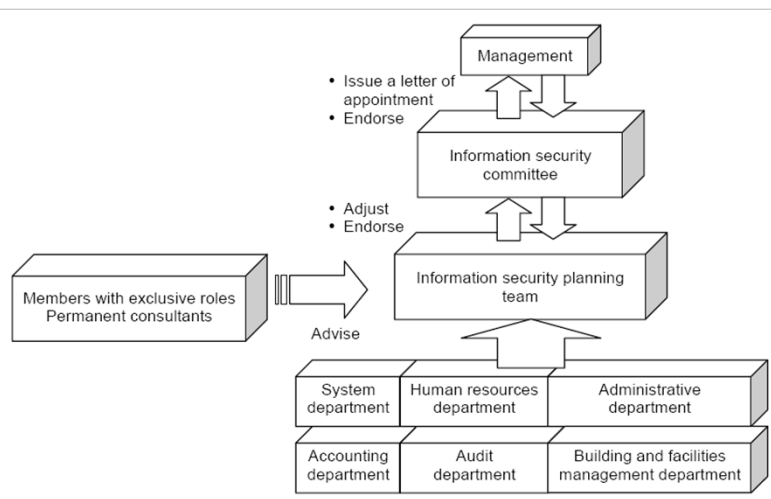


Figure 7.1: Process for Plan Phase

Business Analysis

- Collect information to establish the ISMS
- Define the scope and boundaries of the ISMS
 - Interfaces and dependencies
- Define the ISMS policy
- Planning of organisational structures
- Involvement of management
- Identification of the overall approach to information security

Organisational Structure



Gap Analysis

- Identifying the level of existing security activities and controls
- Based on
 - ISO/IEC 27001 for management system processes
 - ISO/IEC 27002 for information security controls
- Determining the grades of implementation
- Interviews, discussions, questionnaires, walking around
- Speak to different levels of personnel in the organisation

Risk Assessment

- Establishment of the business context and conduction of a gap analysis are necessary pre-conditions
- ISO/IEC 27005 explains more about how to do a risk assessment
- Who to involve
 - Senior management
 - Line management
 - Process and asset owners
 - “Normal” users

Information security policy

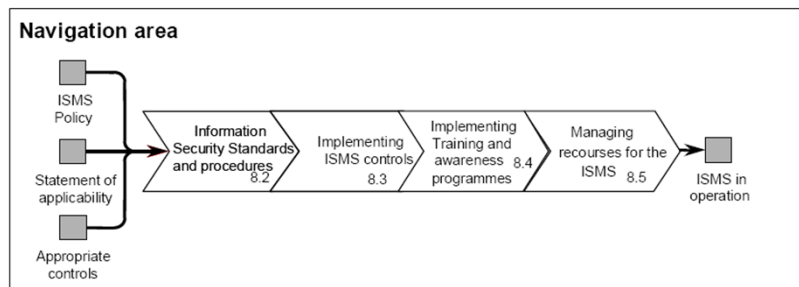
- Development of an information security policy
 - Based on the previous results
 - Content as described in ISO/IEC 27002
- Scope of the information security policy might be the same as for the ISMS, or bigger
- Recommended size: 2-4 pages
- Reference to more detailed documentation should be made
 - One way: hyperlinks

Statement of Applicability

- The Statement of Applicability includes
 - All selected controls (with reference to Annex A of ISO/IEC 27001) and the reasons for their selection
 - All existing controls (it is recommended to also link those to the identified risks)
 - All controls from Annex A of ISO/IEC 27001 that have not been selected and a justification for not selecting them
 - Controls from other sources can be included (it is recommended to also link those to the identified risks)

DO-Phase

The Do Phase has several steps that should be followed for the implementation of this process. Each step provides input to the next step as a logical flow. This step-by-step procedure is exemplified by flow diagrams. Each step is described in such a manner that an organization that is not familiar with information security and/or ISO/IEC or similar management standards may understand what is intended.



Typical issues in ISMS implementation

- Lack of concentration on internal ISMS audits and management reviews
- No preventive actions, only corrective actions
- Risk assessment – approach, completeness, how tailor-made it is
- Measurements – a big issue overall, organisations find it difficult
- Controls – lots of different issues

ISO/IEC 27004

ISO/IEC 27004

June 2011

ISO/IEC 27000 Family of Standards 207



ISO/IEC 27004

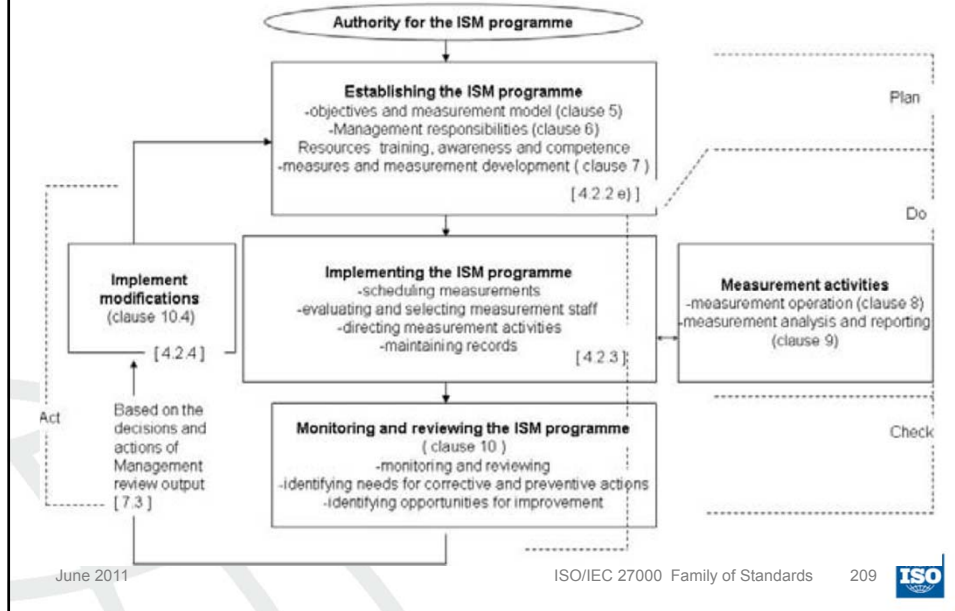
- Scope
 - Providing guidance on the development and use of measures in order to assess the effectiveness of ISMS processes, control objectives and controls as specified in ISO/IEC 27001
- Introduction explaining the main parts of the measurement programme
- Management overview to ease the understanding, especially for SMEs

June 2011

ISO/IEC 27000 Family of Standards 208



Measurement Programme



Measurement Model

- Base measures
 - Result from applying measurement methods to attributes of objects of measurement
- Derived measures
 - are defined by applying measurement function to one or more base measures
- Indicators
 - are obtained by applying an analytical model to derived measures
- Measurement results
 - are evaluated by interpretation of applicable indicators based on defined decision criteria

Base Measure

- Object of Measurement: Employee database
- Attribute: Employee records
- Measurement Method: Database query that extracts number of employees from security awareness and training tracking database
- Base measure: Number of employees who received security awareness and training

Derived Measure

- Base Measure: Number of employees who received security awareness and training, and signed user agreements
- Measurement Function: Divide number of employees who received security awareness training and signed user agreements by the number of employees who signed user agreements and multiply by 100%
- Derived Measure: Percentage of employees who received security awareness and training and signed user agreements

Indicators

- Derived Measure: Percentage of employees who received security awareness and training and signed user agreements
- Analytical model: The percentage levels at which the indicator turns into RED, YELLOW, GREEN are defined
- Example:
 - 95% or more - GREEN
 - 90% or more – YELLOW
 - Less than 90 % - RED

Measurement Results

- Indicators: Green, Yellow or Red, depending on the results of the derived measure
- Decision criteria: Describes the threshold for taking action – depending on the measure used, this can vary
- Measurement result:
 - The situation does not require changes
 - The situation should be considered for revision
 - The situation should be improved

Developing Measures

- Identifying a need for information
- Identifying the object of measurement
 - Measurement development
 - Measurement method and function
 - Attribute selection and validation
 - Analytical model
 - Indicators and reporting formats
- Decision criteria
- Measurement validation
- Data collection, analysis and reporting
- Documentation

June 2011

ISO/IEC 27000 Family of Standards

215



Measurement Template

Metric	<i>Security Management Committee meeting frequency</i>
Description	Measurement of management commitment
Metric scope	ISMS Scope
Objectives	To ensure that <i>Security Management Committee</i> meets at least every 4-6 weeks to maintain effective management of the ISMS
Measured by	ISMS Manager
Method	C = Count of meetings performed normalized, count of meeting protocols, tracking of meeting results and decisions.
Source	Meeting minutes of <i>Security Management Committee</i>
Procedure	Count meeting minutes divided by expected meetings multiplied by 100. Meeting without meeting minutes will not be counted
Frequency	Quarterly
Date	<quarterly> accumulated per calendar year
Indicators	C ≥ 90% good 70% ≤ C ≤ 90% acceptable C ≤ 70% not acceptable

June 2011

ISO/IEC 27000 Family of Standards

216



Measurement Example Group 1

Metric	
Description	
Metric scope	
Objectives	
Measured by	
Method	
Source	
Procedure	
Frequency	
Date	
Indicators	

June 2011

ISO/IEC 27000 Family of Standards

217



Measurement Example Group 2

Metric	
Description	
Metric scope	
Objectives	
Measured by	
Method	
Source	
Procedure	
Frequency	
Date	
Indicators	

June 2011

ISO/IEC 27000 Family of Standards

218



Measurement Example Group 3

Metric	
Description	
Metric scope	
Objectives	
Measured by	
Method	
Source	
Procedure	
Frequency	
Date	
Indicators	

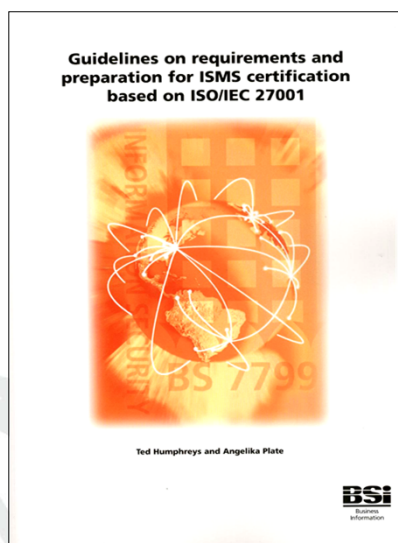
June 2011

ISO/IEC 27000 Family of Standards

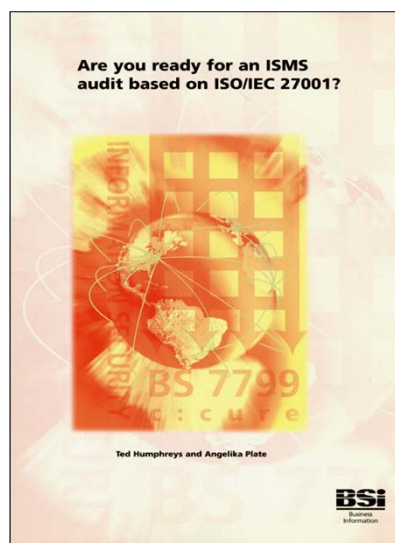
219



ISO 27001 Guidance



June 2011



ISO/IEC 27000 Family of Standards

220



Why incident handling?

- No matter how good the ISMS – errors occur...
- No matter how perfect the controls – new threats or technologies might be arriving faster than you can react
- There is no 100% security

➔ *Incidents will always happen!*

Why incident handling?

- Therefore, an organization needs to have a process in place for
 - Detection and reporting of incidents
 - Assessing the incident and reacting accordingly
 - Identify what went wrong and why the incident occurred
 - Limit the damage
 - Implement controls to improve or to prevent

Example Incident – Denial of Service

- Distributed Denial of Service Attack
- A worm similar to the Code Red
- Around 40.000 servers in Asia were brought down
- Used a MS SQL server vulnerability
- Vulnerability was known and patch available
- Patches not installed
- Panic downloads and installations caused even more network problems



Awareness Raising

- Technical information about incidents
 - CERT
 - FIRST
 - Microsoft
 - Several security software organizations
- Technical and management oriented information
 - NIST
 - SANS
- DTI Information Security Breaches Survey

ISO/IEC 18044

- Information security incident handling management
 - Supports incident handling controls in ISO/IEC 27002
 - Provides templates and more technical advice on how to implement incident handling schemes
 - Published since 2005

Incident Management Process

- There is a process for information security incident management
- Suits well into the PDCA-Model described in ISO/IEC 27001



Plan and Prepare (1)

- Gain commitment from senior management and any other important stakeholders
- Develop an incident management policy
- Develop an incident management scheme to support the policy, including
 - Detection tools and reporting forms
 - Procedures to assess incidents and make decisions
 - Procedures to respond to incidents
 - Details of an incident severity scale

Plan and Prepare (2)

- Update all other documents (policies, procedures) that should refer to the incident management policy
- Establish an organizational structure to support the incident management, e.g.
 - Information Security Incident Response Team (ISIRT)
 - All required roles and responsibilities
 - Contact points in case of an incident
- Implement awareness training for everybody
- Test the incident management scheme

Use Incident Management (1)

- If it is not possible to successfully respond to an incident, initiate crisis activities (such as a business continuity plan)
- Communicate the incident and any necessary details to all relevant people and organizations
 - Including external authorities, if needed
- Collect all important information and conduct analyses
- Produce logs of all activities
- Close the incident

Review the Incidents

- Conduct forensic analyses if more information is needed
- Identify the lessons learnt from the incidents
- Identify actions for improvement
- Identify any necessary improvements to the incident management scheme, e.g. to
 - Procedures or processes
 - Event or incident response forms
 - Organizational structures

Improve the Process

- Revise the incident management policy and scheme, based on
 - Re-assessments of risks
 - Management reviews or internal audits
 - Any other reviews that show a need for improvements
- Make all identified improvements
- Ensure that the improvements achieve their objectives
- Important: Incident management processes are iterative!

Implementing the ISIRT (1)

- Size and structure depends on the organization
 - Virtual or real team
 - With or without direct senior management involvement
- A typical set of members are
 - Business operations
 - IT/Telecoms
 - Information security
 - Human Resources
 - Audit

Implementing the ISIRT (2)

- Ensuring that points of contact and team members are available, when needed
- The ISIRT should have
 - The authority to make decisions on how to deal with incidents
 - A direct reporting line to management
 - The required skill set and knowledge
 - Procedures in place to assign tasks to the most competent member of the team

Benefits of information security management

- Improvements to information security
- Reducing damage from incidents
- Reducing recurrence of incidents
- Collection of evidence
- Contribution to further decision-making, e.g. on priorities or budgets
- Improvements to risk assessment results
- Provision of realistic awareness training material

Key Success Issues (1)

- Management commitment to incident management (as part of the overall management commitment to the ISMS)
- Awareness of everybody within the organization
 - How to report events
 - Whom to contact in case of events
 - Why reporting is important
 - Benefits from reporting events

Key Success Issues (2)

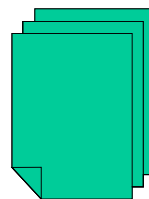
- Compliance with all relevant legal, regulatory and contractual requirements
 - Identification of all relevant legislation
 - Data protection and privacy issue
 - Legally correct monitoring
 - Fulfillment of contractual requirements
 - Contact with law enforcement
 - Adequate address of liability issues
 - Keeping of organizational records
 - Making confidentiality agreements enforceable

Key Success Issues (3)

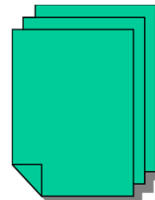
- Anonymity, e.g. when of the information that is contributed to the incident management process
- Confidentiality of any sensitive information involved in the incident management process
- Timely response that keeps people reporting informed
- Credible and trustworthy operation

Example Forms for Incident Management

- Example event reporting form



- Example incident reporting form



Overview (1)

1. Start with defining the scope and policy
2. Do a gap analysis (req. 1.)
3. Define risk assessment method (req. 1.)
 1. Scales for assets, threats , vulnerabilities
 2. Levels of acceptable risk
4. Do a risk assessment (req. 2 and 3)
 1. Identify and value assets
 2. Identify and assess threats and vulnerabilities
 3. Calculate the risks

Overview (2)

5. Define risk treatment option (req. 4)
6. Select controls objectives and controls (req. 5 & 4)
7. Obtain management approval (req. 5 & 6)
8. Produce Statement of Applicability (req. 2, 4, 5 & 6)
9. Produce risk treatment plan (req. 4, 5 & 6)
10. Define measurements (req. 4 & 6)

Overview (3)

- 11. Allocate resources (req. 9)
- 12. Implement controls (req. 9 & 10)
- 13. Do training and awareness and incident handling, produce documentation (req. 9 & 10)
- 14. Run the ISMS

ISMS Review

- There are two parts to the review
 - Regular reviews within a defined time period
 - Reviews initiated because of changes or problems
- The topic(s) of irregular reviews are depending on the problems that caused the review

Regular review activities

- General monitoring to detect incidents, changes and other problems
- Regular reviews of ISMS effectiveness
- Executing measures to determine control effectiveness
- Review of risk assessment
- Internal ISMS audits
- Management reviews

Regular outputs

- For irregular reviews: correcting the problem that caused the review and avoid re-occurrence
- For regular reviews:
 - Improvements of incident and/or change management, if necessary
 - Changes in the ISMS and control effectiveness
 - Updated risk assessment
 - Reports from internal ISMS audits and management reviews

ISMS Benefits

- Improved security, internal assurance
- Competition
- Marketing
- Compliance
- Governance
- Independent check by auditors
- Globalization, internationally agreed

Thank you for listening

Q&A

Angelika.Plate@helpag.com