General

- Personal property
- Mobile phones, pagers, PDA’s and computers
- Smoking
- Safety
- Washrooms
- Breaks and meals

Our Class

- Workshop
- Sessions, Time, Duration
- Active Participation
- Exercises
- Home Works
- Researches and Reports

Introductions

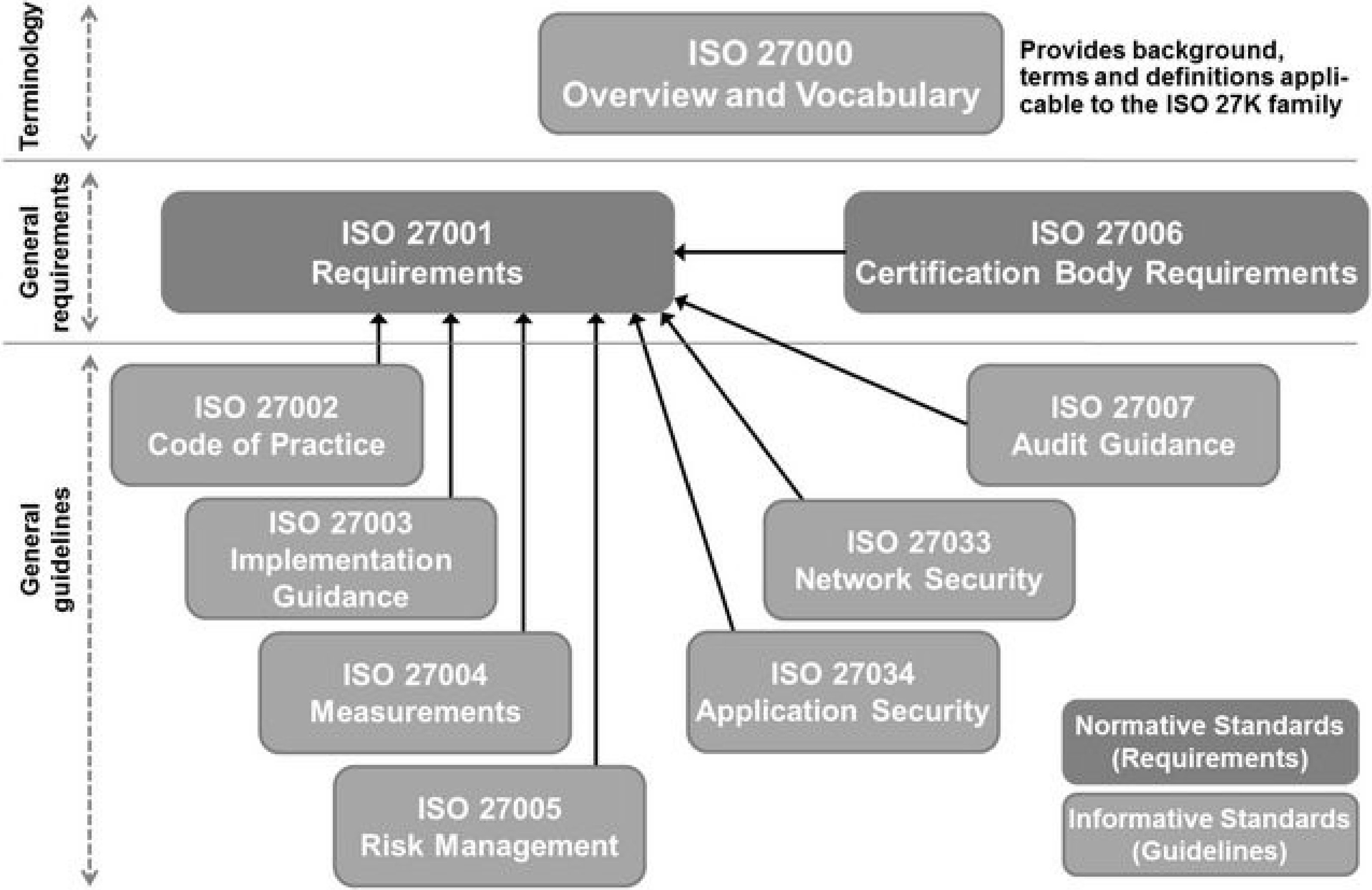
- Name
- Company/department
- Brief résumé of your career
- Information security experience
- ISMS knowledge
- Objectives of attending the course
- Hobbies

ISMS Road Map

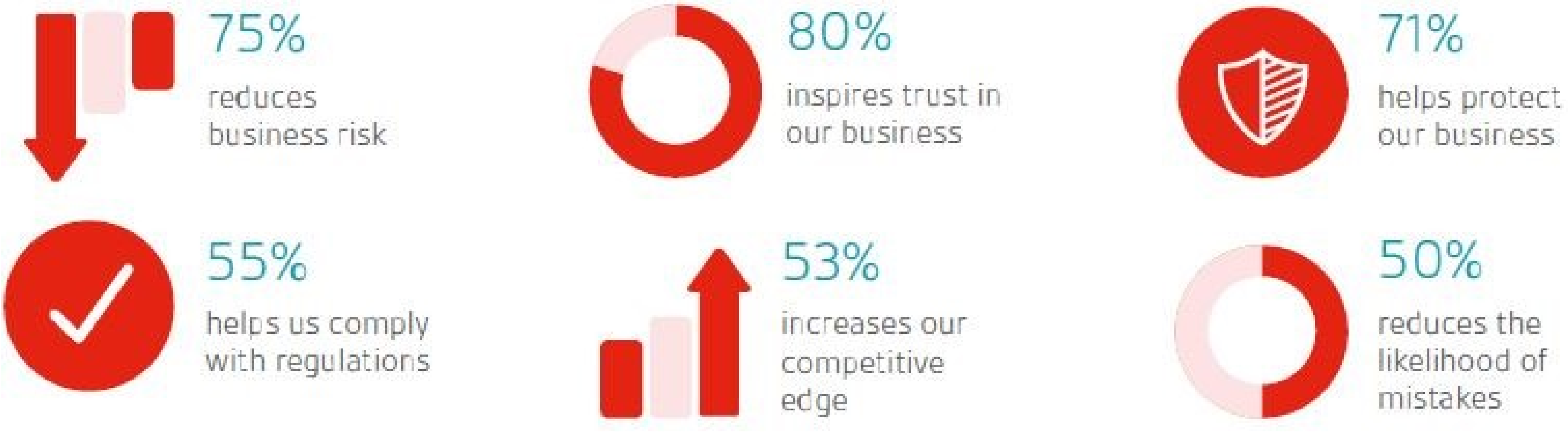
- Introduction and Implementation
- Internal Audit
- Lead Audit

By implementing information security, you help both your company and yourself

ISO 27000 Family



Benefits of ISO 27001:2013



75%
reduces business risk

80%
inspires trust in our business

71%
helps protect our business

55%
helps us comply with regulations

53%
increases our competitive edge

50%
reduces the likelihood of mistakes

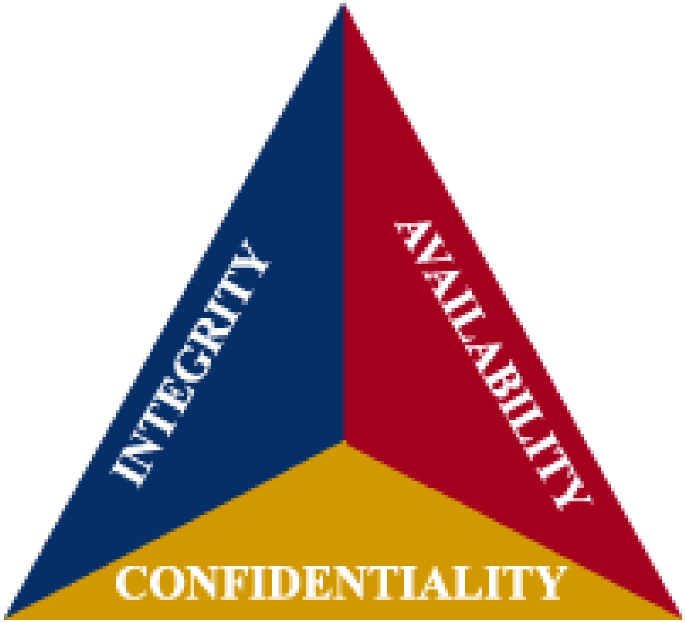
Basic information about ISO 27001

- International standard, published by ISO
- Developed by leading information security experts
- Applicable to any industry
- Applicable to any size company
- More than 20,000 companies have certified worldwide

The purpose of ISO 27001

Preservation of:

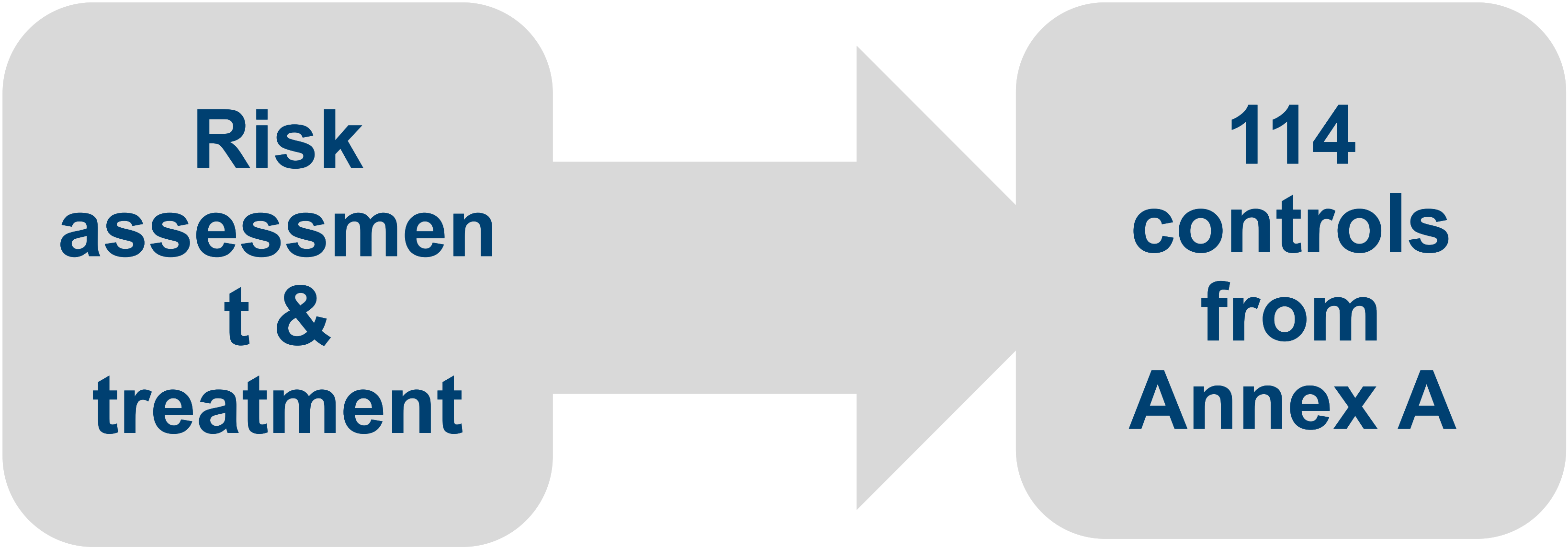
- Confidentiality
- Integrity
- Availability



What is Information

- ISO 27001 is about Information Security
- Information is an organisational asset, which has a value and needs to be appropriately protected
- Without protections information can
  - Loose confidentiality
  - Be modified, with or without our knowledge
  - Be deleted or lost irreparably
  - Be made unavailable

The ISO 27001 framework


Risk assessment & treatment

114 controls from Annex A

ISO 27001 myths

- “This is an IT job”
- “It’s all about writing policies and procedures”
- “We’ll get lost in all those documents”
- “ISO 27001 will only make our job more difficult”
- “It will be implemented in 2 months”
- “We do it only because of the certification”

Benefits for our company

Compliance

Your role in the implementation

- Suggest which processes to document
- Suggest changes in existing & new policies and procedures
- Read all the new documents and attend awareness & training sessions
- Comply with policies and procedures once they are published

Definition of ISMS

- An Information Security Management System consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets.
- An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing maintaining and improving an organization’s information security to achieve business objectives.

Definition of ISMS …

- It is based upon a risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks.

Process

- A group of repeatable and interrelated activities performed to transform a series of inputs into defined outputs

Process approach

- Management of a group of processes together as a system, where the interrelations between processes are identified and the outputs of a previous process are treated as the inputs of the following one. This approach helps ensure the results of each individual process will add business value and contribute to achieve the final desired results.

Information security

- Processes, methodologies, and technologies with the objective to preserve the confidentiality, integrity, and availability of information.

Confidentiality

- Property of the information that can be accessed or disclosed only to authorized persons, entities, or processes.

Integrity

- Property of something that is complete and free of error.

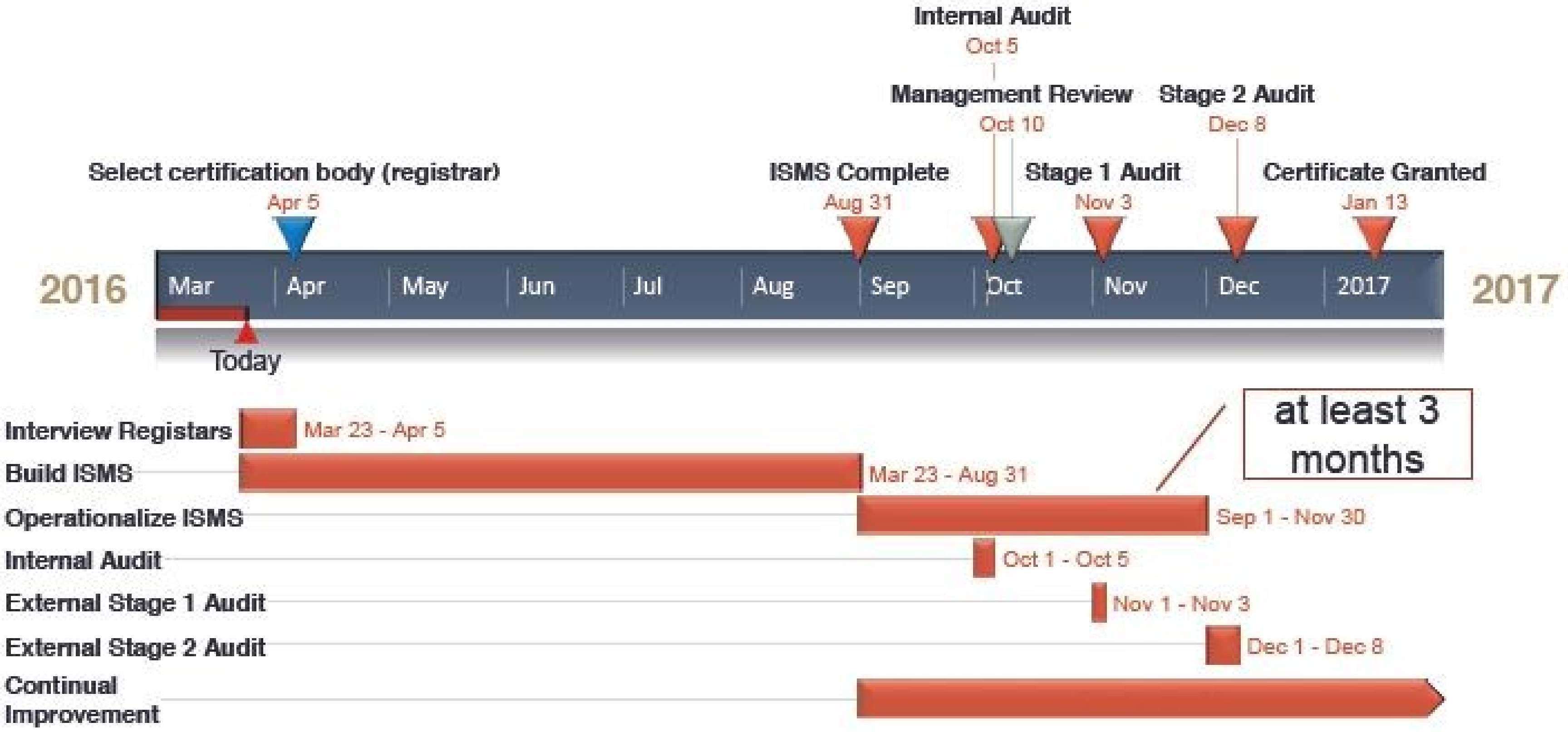
Availability

- Property of something that is accessible and usable only by an authorized person, entity, or process when demanded.

Milestones

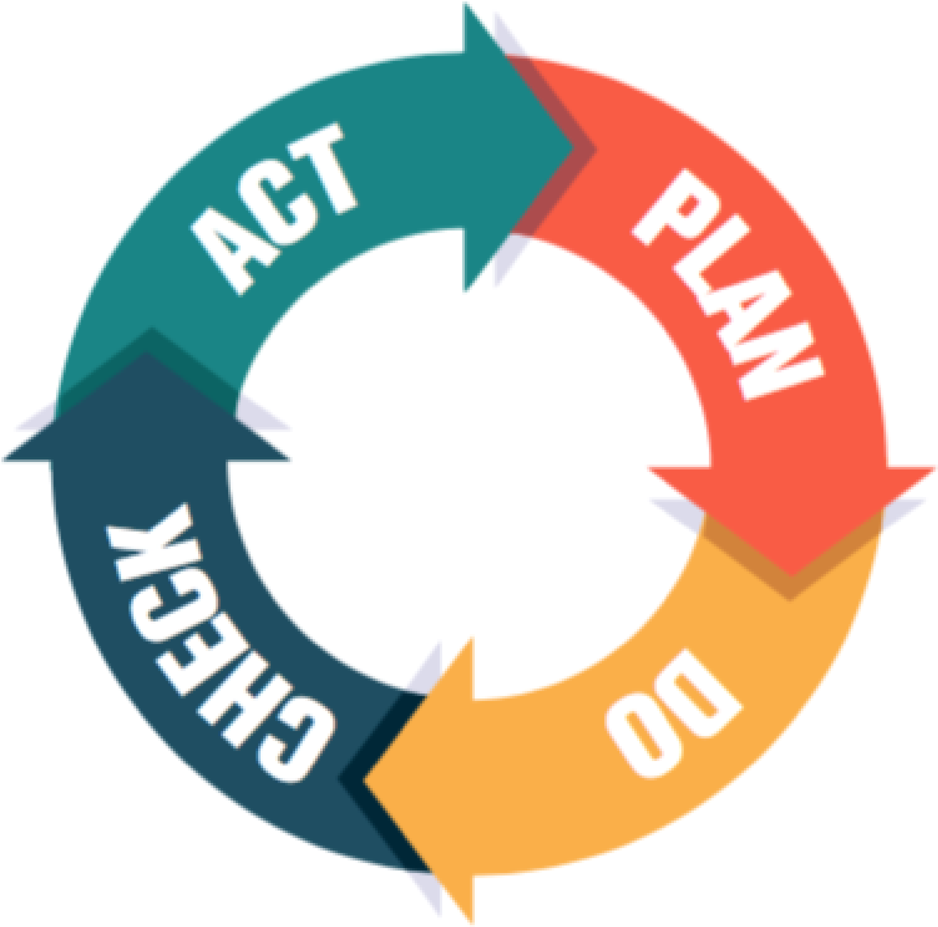
Milestone	Due date
Initiation	
Planning ISMS framework	
Risk assessment	
Implementation	
Internal Audit	
Management Review	
Corrective Actions	
Certification Audit	
Continual Improvement Setup	

Certification Timeline



Surveillance Audits – annually
Recertification Audit – every 3 years

PDCA approach



Requirements for ISO 27001:2013

4.0 Context of the organization

5.0 Leadership

6.0 Planning

7.0 Support

8.0 Operation

9.0 Performance evaluation

10.0 Improvement

4.0 Context of the organization

4.1 Understanding the organization and its context

4.2 Understanding the needs and expectations of interested parties

4.3 Determining the scope of the information security management system

4.4 Information security management system

4.1 Understanding the organization and its context

- Determine external issues
- Determine internal issues
- All issues relevant to its purpose
- Consider issues that affect ability to achieve the intended outcome of ISMS.

Note: Refer Clause 5.3 of ISO 31000:2009

4.2 Understanding the needs and expectations of interested parties

Determine

1. Interested parties that are relevant to the ISMS
2. Requirements of these interested parties relevant to information security as listed below;

- Legal requirements
- Regulatory requirements
- Contractual obligations
- Other requirements identified by organization

4.3 Determining the scope of the ISMS

Determine the boundaries and applicability of the ISMS to establish its scope

For determining the scope consider:

a) **the external and internal issues**
b) **the requirements**
c) **interfaces and dependencies between activities performed**

The documented information related to scope of ISMS is kept in ISMS manual or separate scope document

4.4 Information security management system (ISMS)

- Establish ISMS
- Implement ISMS
- Maintain ISMS
- Continually improve ISMS

In accordance with the requirements of this ISO 27001:2013 standard

5.0 Leadership

5.1 Leadership and commitment

5.2 Policy

5.3 Organizational roles, responsibilities and authorities

5.1 Leadership and commitment

❖ Top Management demonstrate leadership and commitment with respect to ISMS by:

a) Ensuring the information security policy & objectives are established. It should be compatible with the strategy of the organization

b) Ensuring the integration of the ISMS requirements into the organization’s processes

c) Ensuring that the resources are available

d) Communicating the importance of effective ISMS and of conforming ISMS requirements

e) Ensuring that the ISMS achieves its intended outcome

f) Directing and supporting persons to contribute to the effectiveness of ISMS

g) Promoting continual improvement

h) Supporting other relevant management roles to demonstrate their leadership

5.2 Policy

Establish an information security policy :

- **Appropriate to the purpose of the organization**
- **Includes information security objectives**
- **Provide the framework for setting information security objectives**
- **Includes a commitment to satisfy applicable requirements**
- **Includes a commitment to continual improvement for ISMS**
- **Communicate within the organization**
- **Provide to interested parties, as appropriate**

5.3 Organizational roles, responsibilities and authorities

Ensure responsibilities and authorities for roles relevant to information security are assigned and communicated.

The responsibility and authority should cover:

a) **Ensuring ISMS conforming to ISO 27001:2013 requirements**

b) **Reporting on the performance of the information security management system to top management and within the organization.**

6.0 Planning

6 Planning

6.1 Actions to address risks and opportunities

6.2 Information security objectives and planning to achieve them

6.1 Actions to address risks and opportunities

6.1.1 General

- Consider issues, requirements to determine risks and opportunities

6.1 Actions to address risks and opportunities

6.1.2 Information security risk assessment

- Establishes and maintains information security risk criteria
- Ensure that repeated information security risk assessments produce consistent, valid and comparable results
- Evaluates the information security risks
- Identify and evaluate options for the treatment of risks
- Prepare a Statement of Applicability

Document procedure for information security risk assessment process.

6.1 Actions to address risks and opportunities

6.1.3 Information security risk treatment

Apply and implement an information security risk treatment process

6.2 Information security objectives and planning to achieve them

Establish information security objectives at relevant functions and levels

IS Objectives:

- IS objectives consistent with the information security policy
- Measurable objectives
- Consider applicable IS requirements, and results from risk assessment and risk treatment
- Communicate IS objectives
- Update IS objectives periodically (Preferably once in a year)
- Retain Documented IS objectives

6.2 Information security objectives and planning to achieve them

Establish information security objectives at relevant functions and levels

For planning of IS objectives determine

- **what will be done;**
- **what resources will be required**
- **who will be responsible**
- **when it will be completed**
- **how the results will be evaluated**

7.0 Support

7.0 Support

7.1 Resources

7.2 Competence

7.3 Awareness

7.4 Communication

7.5 Documented information

7.1 Resources

Determine and provide the resources needed for:

- **Establishment of ISMS**
- **Implementation of ISMS**
- **Maintenance of ISMS**
- **Continual improvement of the ISMS**

Resource Management

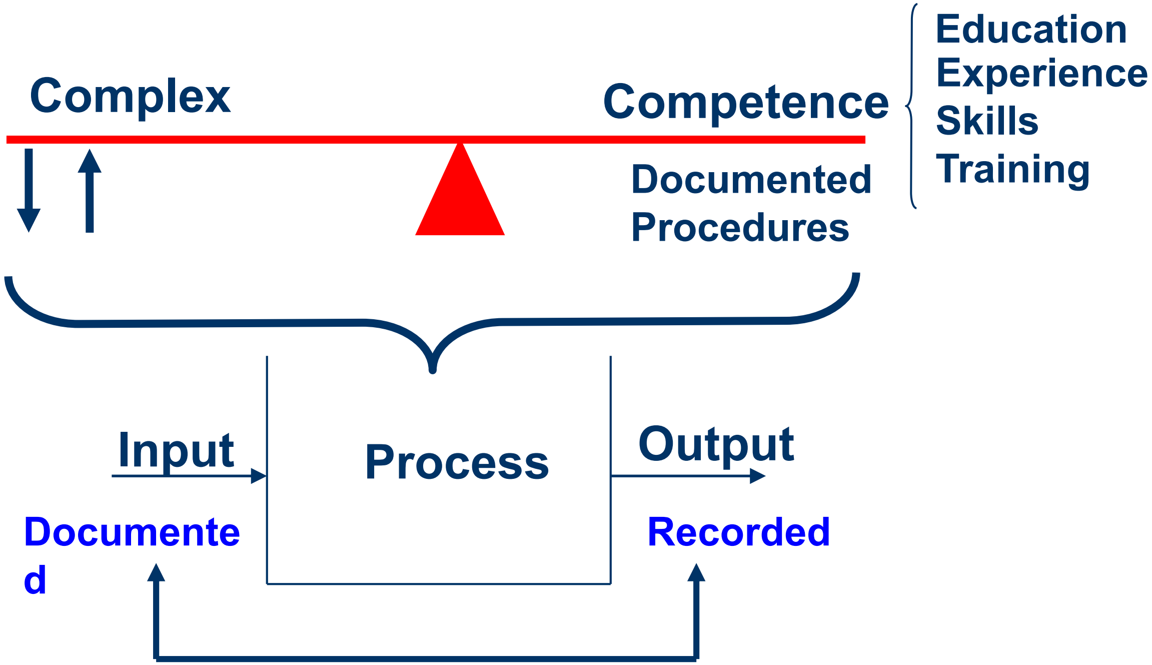
- Provide resources to:
  - Establish, operate and maintain ISMS
  - To support procedures as per business requirements
  - Address legal, regulatory and contractual obligations

7.2 Competence

- Determine the necessary competence of person that affects information security performance
- Ensure persons are competent on the basis

  1.Education 2. training 3. experience;
- Take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken
- Retain appropriate documented information as evidence of competence.
- Evaluate the effectiveness of the training provided and actions taken;
- Maintain records of education, training, skills, experience and qualifications

Competency


Complex
Competence
Education
Experience
Skills
Training
Documented
Procedures
Input
Process
Output
Documente
d
Recorded

7.3 Awareness

❖ Persons should be aware of:

- Information security policy
- Their contribution to the effectiveness of ISMS and the benefits of improved information security performance
- The implications of not conforming with the ISMS requirements

7.4 Communication

- Determine the need for internal and external communications relevant to the ISMS including:

  a) What to communicate?

  b) When to communicate?

  c) Whom to communicate?

  d) Who shall communicate?

  e) Processes by which communication is effected.

7.5 Documented Information

7.5.1 General

1. Include documented information required
2. Include documented information determined by the organization as necessary for the effectiveness of the ISMS

The extend of Documentation depends on

a. Size of organization and its type of activities, processes, products and services;
b. Complexity of processes and their interactions
c. Competence of persons.
d. Will differ from one organization to another

Documentation Type

Paper, Electronic (?)

Note: this clause include documents and records of 2 sub clauses of old standard.

Sample list of documented

Sample list of documented information required for ISMS

a) Documented statements of the security policy and ISMS objectives
b) The scope of the ISMS and procedures and controls in support of the ISMS
c) Risk assessment report
d) Risk treatment plan
e) Documented procedures for effective planning, operation and control of its information security processes
f) Records for compliance to ISO 27001:2013 requirements
g) Statement of Applicability
h) Policies and procedures to establish controls on information security as per established ISMS system

7.5 Documented Information

7.5.2 Creating and Updating

Create and update documented information

a) Identification and description (e.g. a title, date, author, or reference number)

b) Proper format (e.g. language, software version, graphics) and media (e.g. paper, electronic)

c) Review and update and re-approve for suitability and adequacy

d) Approve information for adequacy and suitability prior to issue

7.5 Documented Information

7.5.3 Control of Documented Information

Documented information control to ensure:

a) Availability and suitability for use
b) Adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).
c) Distribution, access, retrieval and use
d) storage and preservation (including the preservation of legibility)
e) Control of changes and current revision status
f) Retention and disposition
g) Ensure the recent versions are available at points of use
h) Ensure information of external origin as identified by IS head are included for same level of controls
i) Ensure distribution of information is controlled
j) Prevent unintended use of obsolete information
k) Apply suitable identification
l) Access of information for view or change

7.5 Documented Information

7.5.3 Control of Documented Information (Continue…)

- Record Control
  - Established and maintained
  - Evidence
  - Controlled
  - Legal Requirements
  - Legible, identifiable and retrievable
- Documented controls for:
  - Identification
  - Storage
  - Protection
  - Retrieval
  - Retention Time
  - Disposition

8.0 Operation

Operation

8.1 Operational planning and control

8.2 Information security risk assessment

8.3 Information security risk treatment

8.1 Operation Planning and Control

- Plan, implement and control the processes
- implement the actions from risks and opportunities
- Implement the risk treatment plan and controls to achieve the IS objectives
- Maintain documented information to establish confidence that the processes
- Control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects as necessary
- Ensure that outsourced processes are determined and controlled
- Implement procedures and other controls

8.2 Information Security Risk Assessment

- Perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established
- Retain documented information of the results of risk assessments

8.2 Information security risk treatment

- Implement the information security risk treatment plan
- Retain documented information of the results of the information security risk treatment.

9.0 Performance Evaluation

9.0 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

9.2 Internal audit

9.3 Management review

9.1 Monitoring, measurement, analysis and evaluation

Evaluate the information security performance and the effectiveness of the ISMS

Determine:

a) What needs to be monitored and measured, including IS processes and controls
b) Which methods for monitoring, measurement, analysis and evaluation?
c) When the monitoring and measuring to be performed?
d) Who will monitor and measure?
e) When the results from monitoring and measurement to be analyzed and evaluated
f) Who will analyse and evaluate these results.

Retain documented information as evidence of the monitoring and measurement results.

9.2 Internal Audit

Conduct internal ISMS audits at planned intervals to determine whether the ISMS meets company requirements and ISO 27001:2013 requirements. Also to ensure ISMS is effectively implemented and maintained.

9.3 Management Review

Management shall review the organization's ISMS at planned Intervals to ensure continuing suitability, adequacy and effectiveness

- **Input**
- **Output**

10.0 Improvement

10 Improvement

10.1 Nonconformity and corrective action

10.2 Continual improvement

10.1 Nonconformity and corrective action

a) React to the nonconformity to:
   1) take action to control and correct it
   2) deal with the consequences

b) Evaluate the need for action to eliminate the causes of nonconformity
   1) reviewing the nonconformity
   2) determining the causes of the nonconformity
   3) determining if similar nonconformities exist or could potentially occur

c) Implement action needed

d) Review the effectiveness of corrective action taken

e) Make changes to the information security management system, if necessary.

Retain documented information as evidence of:

- Nature of the nonconformities and any subsequent actions taken
- Results of corrective action

10.2 Continual Improvement

Continually improve the suitability, adequacy and effectiveness of the ISMS through the use of the

- **Information security policy**
- **Security objectives**
- **Audit results**
- **Analysis of monitored events**
- **Corrective and preventive actions**
- **Management review**

Activity

Discuss within your group:

- How would you ensure that management:
  - Are committed
  - Establish roles and responsibilities for information security
  - Provide training, awareness and competency
  - Carry out reviews of the ISMS

Time - 30 minutes

Annex A (normative)

- **Reference control objectives and controls**

A.5 Information security policies

- **A.5.1 Management direction for information security**
    - One Information Security Policy, or several policies?

A.6 Organization of information security

- **A.6.1 Internal organization**
- **A.6.2 Mobile devices and teleworking**
  - How to document roles and responsibilities according to ISO 27001
  - How to write an easy-to-use BYOD policy compliant with ISO 27001
  - Special interest groups: A useful resource to support your ISMS
  - How to manage security in project management according to ISO 27001 A.6.1.5

A.7 Human resource security

- **A.7.1 Prior to employment**
- **A.7.2 During employment**
- **A.7.3 Termination and change of employment**

  - What to look for when hiring a security professional, and Security Practices to Use in Your Employee Training and Awareness Program.

A.8 Asset management

- **A.8.1 Responsibility for assets**
- **A.8.2 Information classification**
- **A.8.3 Media handling**

  - How to handle Asset register (Asset inventory) according to ISO 27001
  - Secure equipment and media disposal according to ISO 27001
  - Information classification according to ISO 27001
  - Risk owners vs. asset owners in ISO 27001:2013

A.9 Access control

- **A.9.1 Business requirements of access control**
- **A.9.2 User access management**
- **A.9.3 User responsibilities**
- **A.9.4 System and application access control**

  - How to handle access control according to ISO 27001, and How two-factor authentication enables compliance with ISO 27001 access controls.

A.10 Cryptography

- **A.10.1 Cryptographic controls**
  - How to use the cryptography according to ISO 27001 control A.10.

A.11 Physical and environmental security

- **A.11.1 Secure areas**
- **A.11.2 Equipment**
  - How to implement equipment physical protection according to ISO 27001 A.11.2 – Part 1
  - How to implement equipment physical protection according to ISO 27001 A.11.2 – Part 2
  - Physical security in ISO 27001: How to protect the secure areas
  - How to protect against external and environmental threats according to ISO 27001 A.11.1.4
  - Secure equipment and media disposal according to ISO 27001
  - Clear desk and clear screen policy – What does ISO 27001 require?

A.12 Operations security

- A.12.1 Operational procedures and responsibilities
- A.12.2 Protection from malware
- A.12.3 Backup
- A.12.4 Logging and monitoring
- A.12.5 Control of operational software
- A.12.6 Technical vulnerability management
- A.12.7 Information systems audit considerations

A.12 Operations security …

- Implementing capacity management according to ISO 27001:2013 control A.12.1.3
- Logging and monitoring according to ISO 27001 A.12.4
- Implementing restrictions on software installation using ISO 27001 control A.12.6.2
- How can ISO 27001 help protect your company against ransomware?
- How to manage changes in an ISMS according to ISO 27001 A.12.1.2
- Backup policy – How to determine backup frequency
- How to manage technical vulnerabilities according to ISO 27001 control A.12.6.1
- How to use penetration testing for ISO 27001 A.12.6.1

A.13 Communications security

- **A.13.1 Network security management**
- **A.13.2 Information transfer**

    - Requirements to implement network segregation according to ISO 27001 control A.13.1.3
    - How to manage network security according to ISO 27001 A.13.1
    - How to use firewalls in ISO 27001 and ISO 27002 implementation

A.14 System acquisition, development and maintenance

- **A.14.1 Security requirements of information systems**
- **A.14.2 Security in development and support processes**
- **A.14.3 Test data**

    - How to set security requirements and test systems according to ISO 27001, and What are secure engineering principles in ISO 27001:2013 control A.14.2.5?

A.15 Supplier relationships

- **A.15.1 Information security in supplier relationships**
- **A.15.2 Supplier service delivery management**

    - step process for handling supplier security according to ISO 27001.

A.16 Information security incident management

- **A.16.1 Management of information security incidents and improvements**
  - How to handle incidents according to ISO 27001 A.16, and Using ITIL to implement ISO 27001 incident management.

A.17 Information security aspects of business continuity management

- **A.17.1 Information security continuity**
- **A.17.2 Redundancies**
  - How to use ISO 22301 for the implementation of business continuity in ISO 27001
  - How to implement business impact analysis (BIA) according to ISO 22301
  - Business continuity plan: How to structure it according to ISO 22301
  - How to perform business continuity exercising and testing according to ISO 22301
  - Understanding IT disaster recovery according to ISO 27031

A.18 Compliance

- **A.18.1 Compliance with legal and contractual requirements**
- **A.18.2 Information security reviews**

  - A list of Laws and regulations on information security and business continuity.