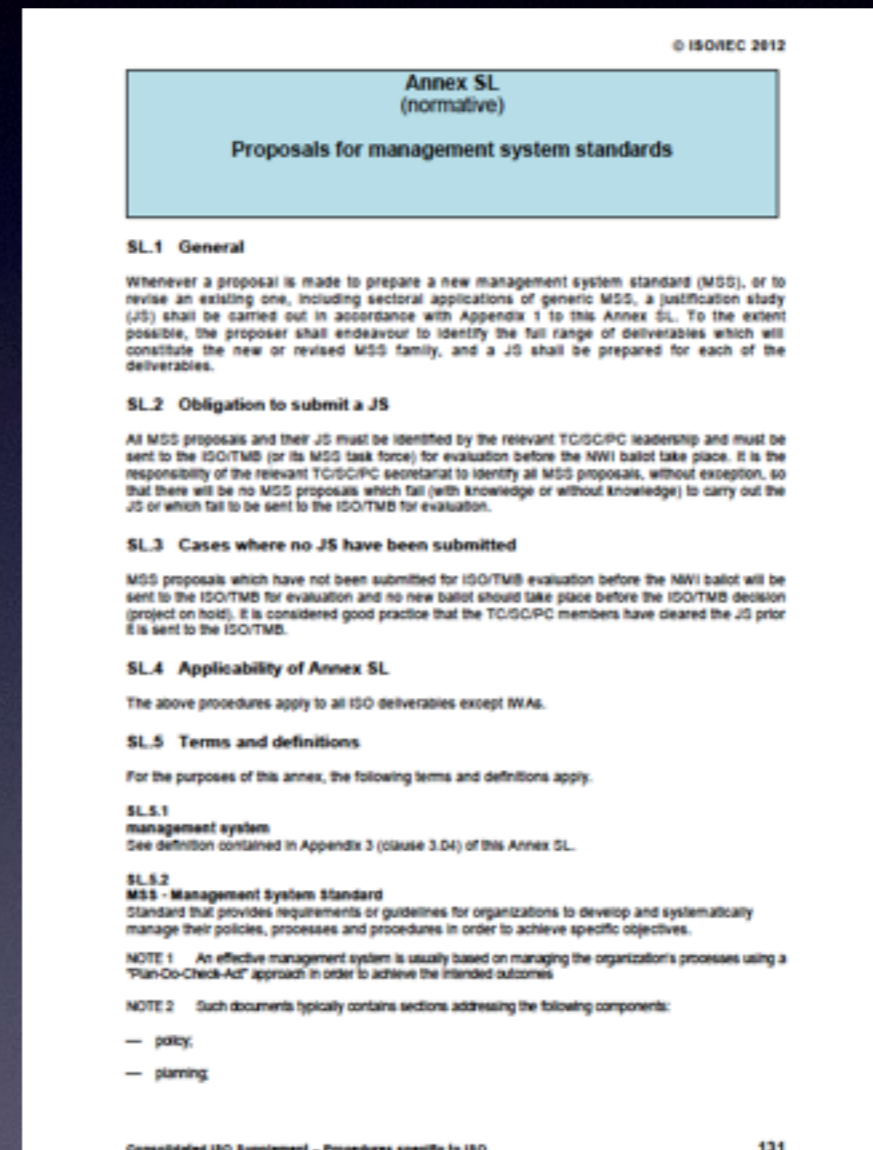


Overview of Annex SL and ISMS (ISO/ IEC 27001:2013)

Session no.: 2

Consolidated ISO Supplement – Procedures specific to ISO, Annex SL (normative)

- Previously ISO Guide 83
- Annex SL describes the requirement for proposals for ISO MSS (Management System Standards).
- To make **ALL** new MSS have the **same overall "look and feel"**



Annex SL - Appendix 3

High level structure, identical core text, common terms and core definitions

1. Scope

2. Normative references

3. Terms and definition

4. 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 XXX management system

4.4. XXX management system

5. Leadership

5.1. Leadership and commitment

5.2. Policy

5.3. Organization roles, responsibilities and authorities

6. Planning

6.1. Actions to address risks and opportunities

6.2. XXX objectives and planning to achieve them

Annex SL - Appendix 3

High level structure, identical core text, common terms and core definitions

7. Support

7.1. Resources

7.2. Competence

7.3. Awareness

7.4. Communication

7.5. Documented information

- General
- Creating and updating
- Control of documented information

8. Operation

8.1. Operational planning and control

9. Performance evaluation

9.1. Monitoring, measurement, analysis and evaluation

9.2. Internal audit

9.3. Management review

10. Improvement

10.1. Nonconformity and corrective action

10.2. Continual improvement

Context of the ISMS, ISO/IEC 27001:2013

4 Context of the organization

“context” means the environment in which the organization operates

- 4.1 Understanding the organization and **its context**
 - The organization shall determine **external** and **internal issues** that are relevant to its purpose and that **affect** its ability to achieve the intended outcome(s) of its **information security management system**.

“issues”,
replaces
preventive
action

NOTE Determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.3 of **ISO 31000:2009**.

ISO 31000:2009

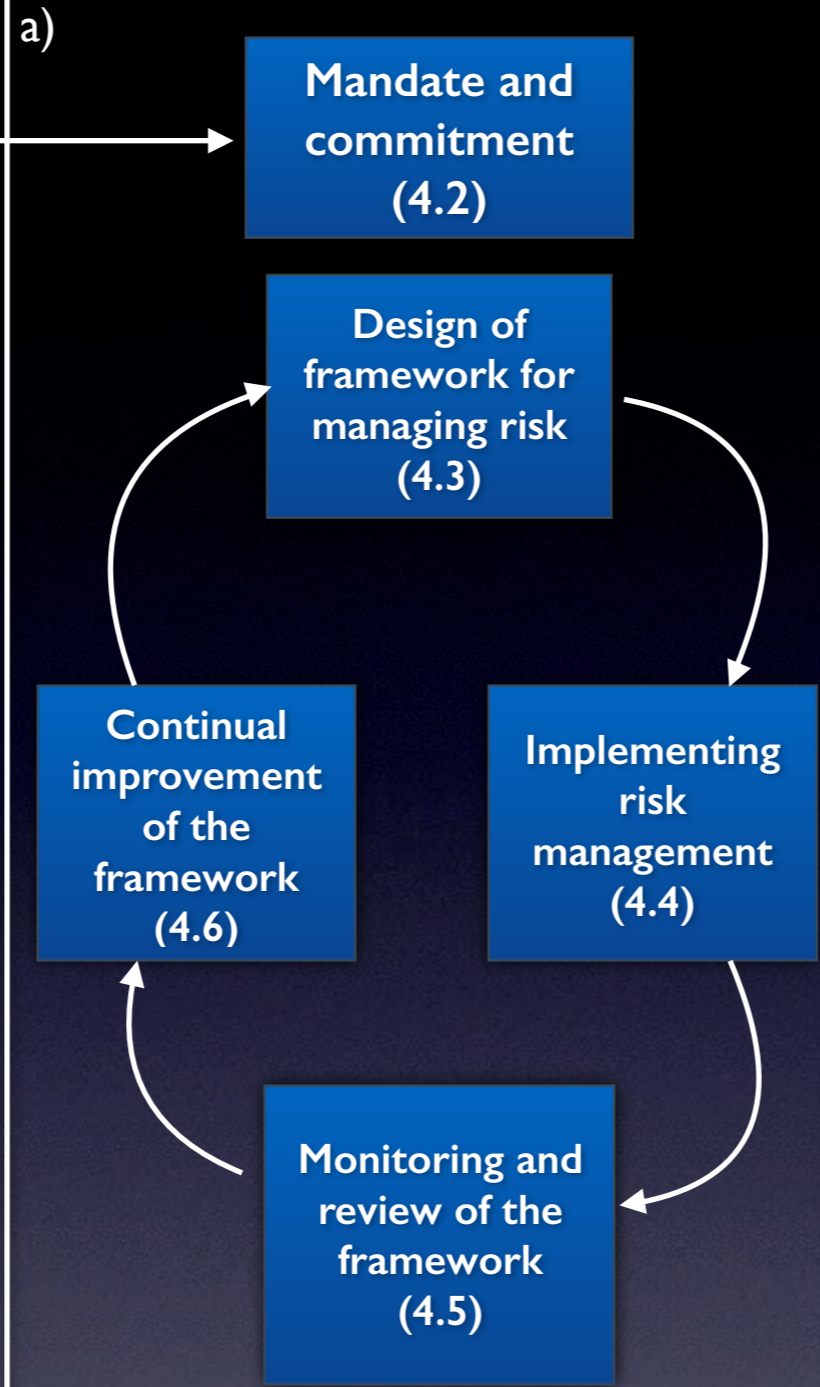
Risk Management principles and guidelines

1. Scope
2. Terms and definitions
3. Principles
4. Framework
 - 4.1. General
 - 4.2. Mandate and commitment
 - 4.3. Design of framework for managing risk
 - 4.4. Implementing risk management
 - 4.5. Monitoring and review of the framework
 - 4.6. Continual improvement of the framework
5. Process
 - 5.1. General
 - 5.2. Communication and consultation
 - 5.3. Establishing the context
 - 5.4. Risk assessment
 - 5.5. Risk treatment
 - 5.6. Monitoring and review
 - 5.7. Recording the risk management process

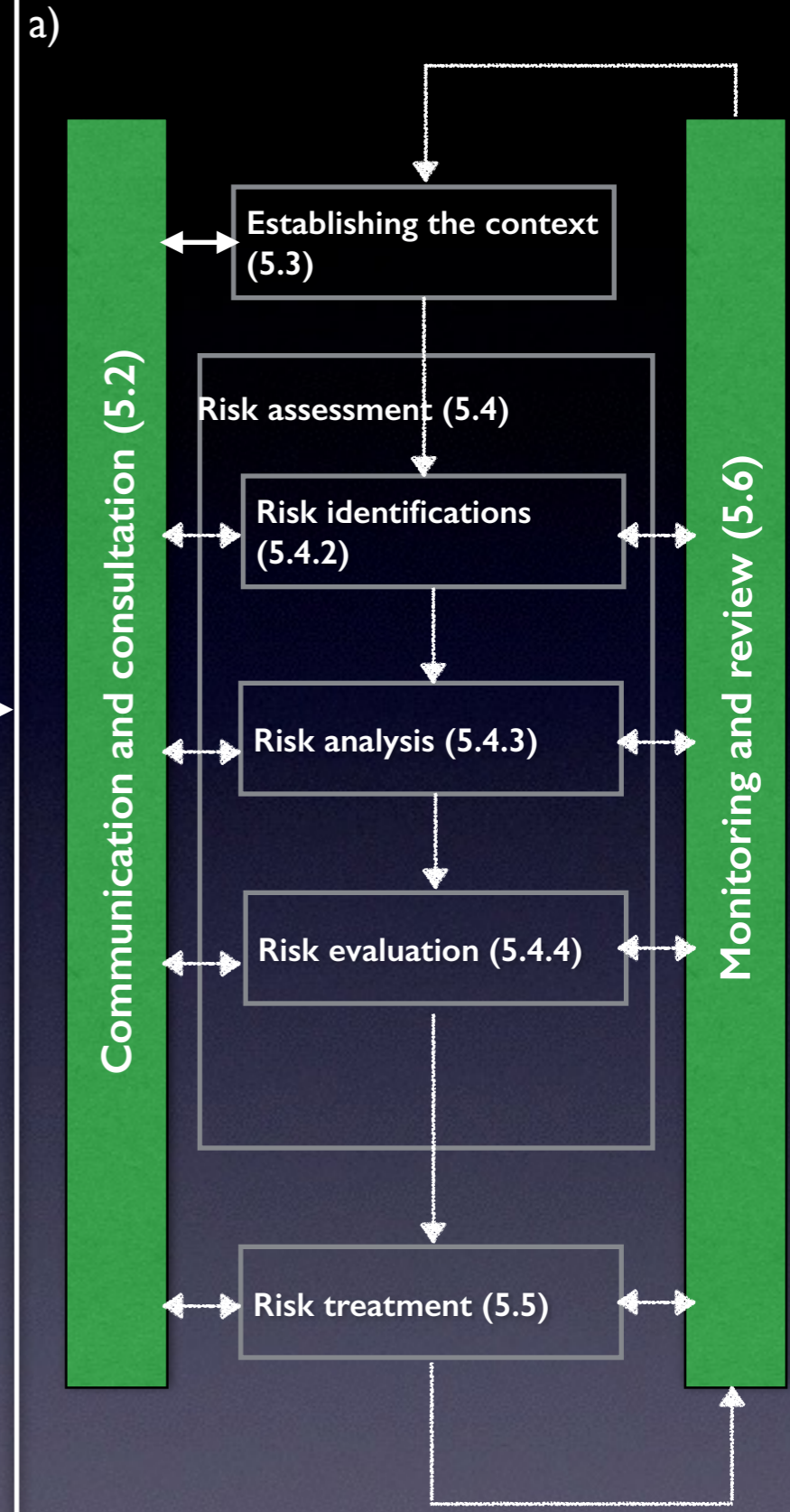


- a) Creates value
- b) Integral part of organizational process
- c) Part of decision making
- d) Explicitly addresses uncertainty
- e) Systematic, structured and timely
- f) Based on the best available information
- g) Tailored
- h) Takes human and culture factors into account
- i) Transparent and inclusive
- j) Dynamic, iterative and responsive to change
- k) Facilitates continual improvement and enhancement of the organization

Principles (Clause 3)

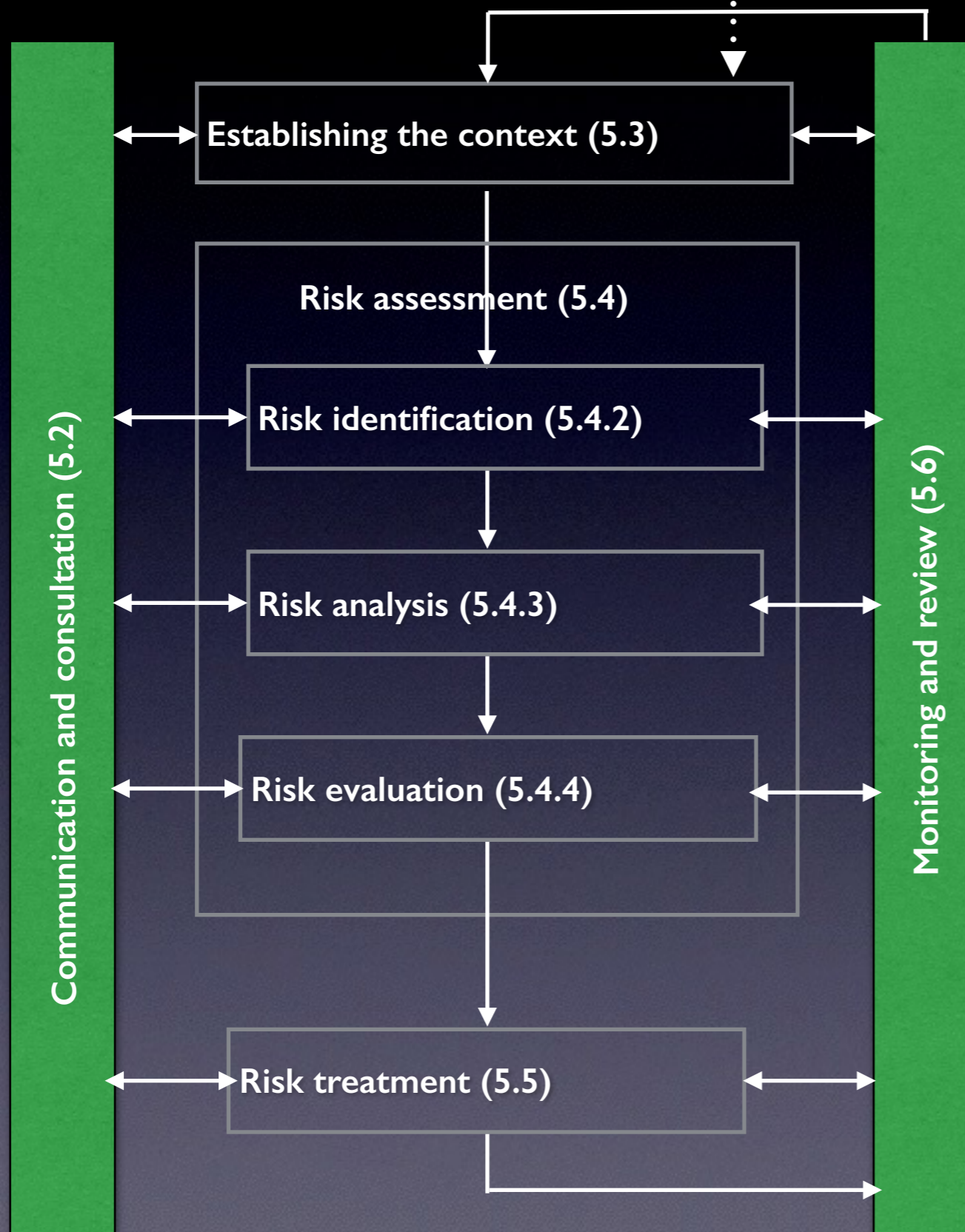


Framework (Clause 4)



Process (Clause 5)

ISO/IEC 27001:2013 Clause 4.1



ISO 31000 Clause 5.3

- 5.3.1 General
- 5.3.2 Establishing the **external** context
- 5.3.3 Establishing the **internal** context
- 5.3.4 Establishing the context of the **risk management process**
- 5.3.5 Defining **risk criteria**

4 Context of the organization



“interested parties”, replaces stakeholders

- 4.2 Understanding the **needs** and **expectations** of **interested parties**
- The organization **shall** determine:
 - (a) **interested parties** that are relevant to the information security management system; and
 - (b) the **requirements** of these interested parties relevant to information security

4 Context of the organization

- 4.3 Determining the **scope** of the information security management system
 - The organization **shall** determine the **boundaries** and **applicability** of the information security management system to establish its scope.
 - When determining this scope, the organization **shall** consider:
 - (a) the external and internal issues referred to in 4.1
 - (b) the requirements referred to in 4.2; and
 - (c) **interfaces and dependencies between activities** performed by the organization, and those that are performed by other organizations.
 - The scope shall be available as **documented information**

4 Context of the organization

- 4.4 Information security management system
 - The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard.

5 Leadership



Specific requirements to top management

- 5.1 **Leadership** and commitment
- **Top management shall demonstrate** leadership and commitment with respect to the information security management system by:
 - (a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;
 - (b) ensuring the integration of the information security management system requirements into the organization's processes;
 - (c) ensuring that the resources needed for the information security management system are available

5 Leadership

- (d) communicating the importance of effective information security management and of conforming to the information security management system requirements;**
- (e) ensuring that the information security management system achieves its intended outcome(s);**
- (f) directing and supporting persons to contribute to the effectiveness of the information security management system;**
- (g) promoting continual improvement; and**
- (h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.**

5 Leadership

- 5.2 Policy
 - Top management shall establish **an information security policy** that:
 - (a) is appropriate to the purpose of the organization
 - (b) includes information security objectives (see 6.2) or provides the framework for setting information security objectives;
 - (c) includes a commitment to satisfy applicable requirements related to information security; and
 - (d) includes a commitment to continual improvement of the information security management system.

5 Leadership

- The information security policy shall:
 - (e) be available as documented information
 - (f) be communicated within the organization; and
 - (g) be available to interested parties, as appropriate

5 Leadership

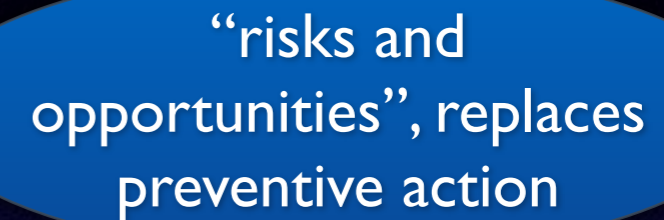
- **5.3 Organizational roles, responsibilities and authorities**
 - **Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.**
 - **Top management shall assign the responsibility and authority for**
 - (a) ensuring that the information security management system conforms to the requirements of this International Standard; and**
 - (b) reporting on the performance of the information security management system to top management**

6 Planning

- **6.1 Actions to address risks and opportunities**
 - **6.1.1 General**
 - **When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:**
 - (a) ensure the information security management system can achieve its intended outcome(s);**
 - (b) prevent, or reduce, undesired effects; and**
 - (c) achieve continual improvement**

6 Planning

- The organization shall plan:
 - (d) **actions to address these risks and opportunities;** and
 - (e) how to
 - integrate and implement the actions into its information security management system processes; and
 - evaluate the effectiveness of these actions



“risks and opportunities”, replaces preventive action

6 Planning

- 6.1.2 Information security risk assessment
- The organization shall define and apply an information security risk assessment process that:
 - (a) establishes and maintains information security risk criteria that include:
 - the risk acceptance criteria; and
 - criteria for performing information security risk assessments

6 Planning

- (b) ensures that repeated information security risk assessments produce consistent, valid and comparable results;
- (c) identifies the information security risks:
 - (1) apply the information security risk assessment process to **identify risks associated with the loss of confidentiality, integrity and availability** for information within the scope of the information security management system; and
 - (2) identify the **risk owners**



Replaces asset owner

6 Planning

(d) analyses the information security risks:

- (1) assess the **potential consequences** that would result if the risks identified in 6.1.2 c) 1) were to materialize;
- (2) assess the realistic **likelihood** of the occurrence of the risks identified in 6.1.2 c) 1); and
- (3) **determine the levels of risk**

6 Planning

- (e) evaluates the information security risks**
 - (1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and**
 - (2) prioritize the analysed risks for risk treatment**
- The organization shall retain documented information about the information security risk assessment process.**

6 Planning

- **6.1.3 Information security risk treatment**
 - The organization shall define and apply an information security risk treatment process to:
 - (a) select appropriate information security risk treatment options, taking account of the risk assessment results;
 - (b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen;
 - (c) compare the controls determined in 6.1.3 b) above with those in **Annex A** and verify that no necessary controls have been omitted;

Controls are now determined during the process of risk treatment, rather than being selected from Annex A

6 Planning

- **NOTE 1** Annex A contains a comprehensive list of control objectives and controls. Users of this International Standard are directed to Annex A to ensure that no necessary controls are overlooked.
- **NOTE 2** Control objectives are implicitly included in the controls chosen. **The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may be needed.**

6 Planning

- (d) produce a Statement of Applicability that contains the necessary controls (see 6.1.3 b) and c)) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A;
 - (e) formulate an information security risk treatment plan; and
 - (f) obtain **risk owners'** approval of the information security risk treatment plan and acceptance of the residual information security risks.
- The organization shall retain documented information about the information security risk treatment process

The effectiveness of the risk treatment plan is now regarded as being more important than the effectiveness of controls

6 Planning

Information security objectives are now to be set at relevant functions and levels

- **6.2 Information security objectives** and planning to achieve them
- The organization shall establish information security objectives **at relevant functions and levels**. The information security objectives shall:
 - (a) be consistent with the information security policy
 - (b) be measurable (if practicable);
 - (c) take into account applicable information security requirements, and results from risk assessment and risk treatment;
 - (d) be communicated; and
 - (e) be updated as appropriate

6 Planning

- **The organization shall retain documented information on the information security objectives. When planning how to achieve its information security objectives, the organization shall determine:**
 - (f) what will be done;**
 - (g) what resources will be required;**
 - (h) who will be responsible;**
 - (i) when it will be completed; and**
 - (j) how the results will be evaluated.**

7 Support

- **7.1 Resources**
 - **The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.**

7 Support

- **7.2 Competence**
 - (a) determine the necessary competence of person(s) doing work under its control that affects its information security performance;**
 - (b) ensure that these persons are competent on the basis of appropriate education, training, or experience;**
 - (c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken;
and**
 - (d) retain appropriate documented information as evidence of competence.**

7 Support

- **7.3 Awareness**
 - **Persons doing work under the organization's control shall be aware of:**
 - (a) the information security policy**
 - (b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and**
 - (c) the implications of not conforming with the information security management system requirements.**

7 Support

There are explicit requirements for both internal and external communications

- **7.4 Communication**
- The organization shall determine the need for **internal and external communications** relevant to the information security management system including:
 - (a) on what to communicate;
 - (b) when to communicate;
 - (c) with whom to communicate;
 - (d) who shall communicate; and
 - (e) the processes by which communication shall be effected.

7 Support

Replaces
documents and records

- **7.5 Documented information**
- **7.5.1 General**
 - The organization's information security management system shall include
 - (a) documented information required by this International Standard; and
 - (b) documented information determined by the organization as being necessary for the effectiveness of the information security management system.

Documented information

| | |
|---|---|
| 4.3 Scope of the ISMS | 8.1 Operational planning and control |
| 5.2 Information security policy | 8.2 Results of the information security risk assessments |
| 6.1.2 Information security risk assessment process | 8.3 Results of the information risk treatment |
| 6.1.3 Information security risk treatment process | 9.1 Evidence of the monitoring and measurement results |
| 6.1.3 (d) Statement of Applicability | 9.2 (g) Evidence of the audit programs and the audit results |
| 6.2 Information security objectives | 9.3 Evidence of the results of the management reviews |
| 7.2 (d) Evidence of competence | 10.1 (f) Evidence of the nature of the nonconformities and subsequent actions taken |
| 7.5.1 (b) Documented information determined by the organization as being necessary for the effectiveness of the ISMS | 10.2 (g) Evidence of the results of any correction action |

7 Support

- **7.5.2 Creating and updating**
- **When creating and updating documented information the organization shall ensure appropriate:**
 - (a) identification and description (e.g. a title, date, author, or reference number);
 - (b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and
 - (c) review and approval for suitability and adequacy.

7 Support

- **7.5.3 Control of documented information**
- **Documented information required by the information security management system and by this International Standard shall be controlled to ensure:**
 - (a) it is available and suitable for use, where and when it is needed; and**
 - (b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).**

7 Support

- For the control of documented information, the organization shall address the following activities, as applicable:
 - (c) distribution, access, retrieval and use;
 - (d) storage and preservation, including the preservation of legibility;
 - (e) control of changes (e.g. version control); and
 - (f) retention and disposition.
- Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.

8 Operation

- **8.1 Operational planning and control**
 - **The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information security objectives determined in 6.2.**
 - **The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.**
 - **The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.**
 - **The organization shall ensure that outsourced processes are determined and controlled.**

8 Operation

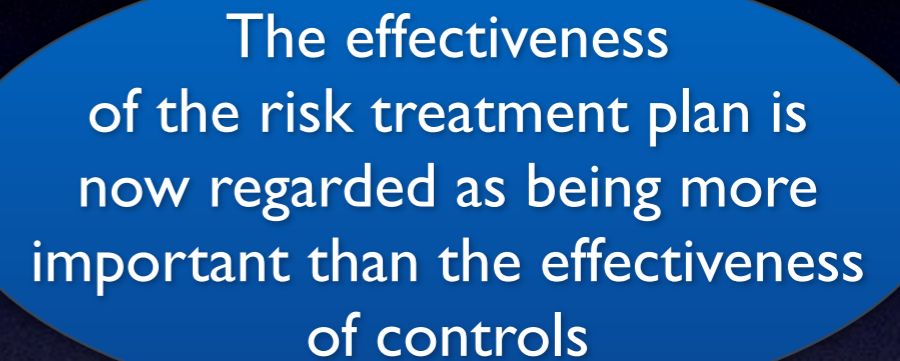
- **8.2 Information security risk assessment**
 - The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a).
 - The organization shall retain documented information of the results of the information security risk assessments.

8 Operation

- 8.3 Information security risk treatment

- The organization shall implement the **information security risk treatment plan**.

- The organization shall retain documented information of the results of the information security risk treatment.



The effectiveness of the risk treatment plan is now regarded as being more important than the effectiveness of controls

9 Performance evaluation

Covers the measurement of ISMS (9.1) and risk treatment plan effectiveness (9.3)

- 9.1 Monitoring, measurement, analysis and evaluation
 - The organization shall evaluate the information security performance and the effectiveness of the information security management system.
 - The organization shall determine:
 - (a) what needs to be monitored and measured, including information security processes and controls;
 - (b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;
 - NOTE The methods selected should produce comparable and reproducible results to be considered valid.

9 Performance evaluation

- (c) when the monitoring and measuring shall be performed;
 - (d) who shall monitor and measure;
 - (e) when the results from monitoring and measurement shall be analysed and evaluated; and
 - (f) who shall analyse and evaluate these results.
- The organization shall retain appropriate documented information as evidence of the monitoring and measurement results.

9 Performance evaluation

- **9.2 Internal audit**
 - **The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:**
 - (a) conforms to**
 - 1) the organization's own requirements for its information security management system; and**
 - 2) the requirements of this International Standard;**
 - (b) is effectively implemented and maintained.**

9 Performance evaluation

- The organization shall:
 - (c) plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits;
 - (d) define the audit criteria and scope for each audit;
 - (e) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;
 - (f) ensure that the results of the audits are reported to relevant management; and
 - (g) retain documented information as evidence of the audit programme(s) and the audit results.

9 Performance evaluation

- 9.3 Management review
 - Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.
 - The management review shall include consideration of:
 - a) the status of actions from previous management reviews;
 - b) changes in external and internal issues that are relevant to the information security management system;
 - c) feedback on the information security performance, including trends in:
 - (1) nonconformities and corrective actions;
 - (2) monitoring and measurement results;
 - (3) audit results; and
 - (4) fulfilment of information security objectives

9 Performance evaluation

Covers the measurement of ISMS (9.1) and risk treatment plan effectiveness (9.3)

- d) feedback from interested parties;
 - e) results of **risk assessment** and status of **risk treatment plan**; and
 - f) opportunities for continual improvement.
- The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.
 - The organization shall **retain documented information as evidence of the results of management reviews.**

10 Improvement

- 10.1 Nonconformity and corrective action
 - When a **nonconformity** occurs, the organization shall:
 - (a) react to the nonconformity, and as applicable:
 - (1) take action to control and correct it; and
 - (2) deal with the consequences;
 - (b) **evaluate the need for action to eliminate the causes of nonconformity**, in order that it does not recur or occur elsewhere, by:
 - (1) reviewing the nonconformity;
 - (2) determining the causes of the nonconformity; and
 - (3) determining if similar nonconformities exist, or could potentially occur;

I0 Improvement

- (c) implement any action needed;
 - (d) review the effectiveness of any corrective action taken; and
 - (e) make changes to the information security management system, if necessary.
- Corrective actions shall be appropriate to the effects of the nonconformities encountered.
- The organization shall retain documented information as evidence of:
 - (f) the nature of the nonconformities and any subsequent actions taken, and
 - (g) the results of any corrective action.

10 Improvement

Methodologies other than Plan-Do-Check-Act (PDCA) may be used

- **10.2 Continual improvement**
 - The organization shall continually improve the **suitability, adequacy** and **effectiveness** of the information security management system.

ISO/IEC 27001:2013, Annex A (normative)

14 categories, 114 controls

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