INTERNATIONAL STANDARD

ISO/IEC 27005

First edition
2008-06-15

Information technology — Security techniques — Information security risk management

Technologies de l'information — Techniques de sécurité — Gestion du risque en sécurité de l'information

Reference number
ISO/IEC 27005:2008(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword ... v

Introduction ... vi

1 Scope ... 1

2 Normative references ... 1

3 Terms and definitions ... 1

4 Structure of this International Standard ... 3

5 Background ... 3

6 Overview of the information security risk management process ... 4

7 Context establishment ... 7
7.1 General considerations ... 7
7.2 Basic Criteria ... 7
7.3 The scope and boundaries ... 8
7.4 Organization for information security risk management ... 9

8 Information security risk assessment ... 9
8.1 General description of information security risk assessment ... 9
8.2 Risk analysis ... 10
8.2.1 Risk identification ... 10
8.2.2 Risk estimation ... 14
8.3 Risk evaluation ... 16

9 Information security risk treatment ... 17
9.1 General description of risk treatment ... 17
9.2 Risk reduction ... 19
9.3 Risk retention ... 20
9.4 Risk avoidance ... 20
9.5 Risk transfer ... 20

10 Information security risk acceptance ... 21

11 Information security risk communication ... 21

12 Information security risk monitoring and review ... 22
12.1 Monitoring and review of risk factors ... 22
12.2 Risk management monitoring, reviewing and improving ... 23

Annex A (informative) **Defining the scope and boundaries of the information security risk management process** ... 25
A.1 Study of the organization ... 25
A.2 List of the constraints affecting the organization ... 26
A.3 List of the legislative and regulatory references applicable to the organization ... 28
A.4 List of the constraints affecting the scope ... 28

Annex B (informative) **Identification and valuation of assets and impact assessment** ... 30
B.1 Examples of asset identification ... 30
B.1.1 The identification of primary assets ... 30
B.1.2 List and description of supporting assets ... 31
B.2 Asset valuation ... 35
B.3 Impact assessment ... 38

Annex C (informative) **Examples of typical threats** ... 39

Annex D (informative) **Vulnerabilities and methods for vulnerability assessment** ... 42

D.1 Examples of vulnerabilities **42**
D.2 Methods for assessment of technical vulnerabilities **45**

Annex E (informative) **Information security risk assessment approaches** **47**
E.1 High-level information security risk assessment **47**
E.2 Detailed information security risk assessment **48**
E.2.1 Example 1 Matrix with predefined values **48**
E.2.2 Example 2 Ranking of Threats by Measures of Risk **50**
E.2.3 Example 3 Assessing a value for the likelihood and the possible consequences of risks **51**

Annex F (informative) **Constraints for risk reduction** **53**

Bibliography **55**

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27005 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This first edition of ISO/IEC 27005 cancels and replaces ISO/IEC TR 13335-3:1998, and ISO/IEC TR 13335-4:2000, of which it constitutes a technical revision.

Introduction

This International Standard provides guidelines for Information Security Risk Management in an organization, supporting in particular the requirements of an ISMS according to ISO/IEC 27001. However, this International Standard does not provide any specific methodology for information security risk management. It is up to the organization to define their approach to risk management, depending for example on the scope of the ISMS, context of risk management, or industry sector. A number of existing methodologies can be used under the framework described in this International Standard to implement the requirements of an ISMS.

This International Standard is relevant to managers and staff concerned with information security risk management within an organization and, where appropriate, external parties supporting such activities.

Information technology — Security techniques — Information security risk management

1 Scope

This International Standard provides guidelines for information security risk management.

This International Standard supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.

Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of this International Standard.

This International Standard is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that could compromise the organization's information security.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27001, ISO/IEC 27002 and the following apply.

3.1
impact
adverse change to the level of business objectives achieved

3.2
information security risk
potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization

NOTE It is measured in terms of a combination of the likelihood of an event and its consequence.

3.3
risk avoidance
decision not to become involved in, or action to withdraw from, a risk situation

[ISO/IEC Guide 73:2002]

3.4
risk communication
exchange or sharing of information about risk between the decision-maker and other stakeholders

[ISO/IEC Guide 73:2002]

3.5
risk estimation
process to assign values to the probability and consequences of a risk

[ISO/IEC Guide 73:2002]

NOTE 1 In the context of this International Standard, the term “activity” is used instead of the term “process” for risk estimation.

NOTE 2 In the context of this International Standard, the term “likelihood” is used instead of the term “probability” for risk estimation.

3.6
risk identification
process to find, list and characterize elements of risk

[ISO/IEC Guide 73:2002]

NOTE In the context of this International Standard, the term “activity” is used instead of the term “process” for risk identification.

3.7
risk reduction
actions taken to lessen the probability, negative consequences, or both, associated with a risk

[ISO/IEC Guide 73:2002]

NOTE In the context of this International Standard, the term “likelihood” is used instead of the term “probability” for risk reduction.

3.8
risk retention
acceptance of the burden of loss or benefit of gain from a particular risk

[ISO/IEC Guide 73:2002]

NOTE In the context of information security risks, only negative consequences (losses) are considered for risk retention.

3.9
risk transfer
sharing with another party the burden of loss or benefit of gain, for a risk

[ISO/IEC Guide 73:2002]

NOTE In the context of information security risks, only negative consequences (losses) are considered for risk transfer.

4 Structure of this International Standard

This standard contains the description of the information security risk management process and its activities.

The background information is provided in Clause 5.

A general overview of the information security risk management process is given in Clause 6.

All information security risk management activities as presented in Clause 6 are subsequently described in the following clauses:

- Context establishment in Clause 7,
- Risk assessment in Clause 8,
- Risk treatment in Clause 9,
- Risk acceptance in Clause 10,
- Risk communication in Clause 11,
- Risk monitoring and review in Clause 12.

Additional information for information security risk management activities is presented in the annexes. The context establishment is supported by Annex A (Defining the scope and boundaries of the information security risk management process). Identification and valuation of assets and impact assessments are discussed in Annex B (examples for assets), Annex C (examples of typical threats) and Annex D (examples of typical vulnerabilities).

Examples of information security risk assessment approaches are presented in Annex E.

Constraints for risk reduction are presented in Annex F.

All risk management activities as presented from Clause 7 to Clause 12 are structured as follows:

Input: Identifies any required information to perform the activity.

Action: Describes the activity.

Implementation guidance: Provides guidance on performing the action. Some of this guidance may not be suitable in all cases and so other ways of performing the action may be more appropriate.

Output: Identifies any information derived after performing the activity.

5 Background

A systematic approach to information security risk management is necessary to identify organizational needs regarding information security requirements and to create an effective information security management system (ISMS). This approach should be suitable for the organization´s environment, and in particular should be aligned with overall enterprise risk management. Security efforts should address risks in an effective and timely manner where and when they are needed. Information security risk management should be an integral part of all information security management activities and should be applied both to the implementation and the ongoing operation of an ISMS.

Information security risk management should be a continual process. The process should establish the context, assess the risks and treat the risks using a risk treatment plan to implement the recommendations and decisions. Risk management analyses what can happen and what the possible consequences can be, before deciding what should be done and when, to reduce the risk to an acceptable level.

Information security risk management should contribute to the following:

- Risks being identified
- Risks being assessed in terms of their consequences to the business and the likelihood of their occurrence
- The likelihood and consequences of these risks being communicated and understood
- Priority order for risk treatment being established
- Priority for actions to reduce risks occurring
- Stakeholders being involved when risk management decisions are made and kept informed of the risk management status
- Effectiveness of risk treatment monitoring
- Risks and the risk management process being monitored and reviewed regularly
- Information being captured to improve the risk management approach
- Managers and staff being educated about the risks and the actions taken to mitigate them

The information security risk management process can be applied to the organization as a whole, any discrete part of the organization (e.g. a department, a physical location, a service), any information system, existing or planned or particular aspects of control (e.g. business continuity planning).

6 Overview of the information security risk management process

The information security risk management process consists of context establishment (Clause 7), risk assessment (Clause 8), risk treatment (Clause 9), risk acceptance (Clause 10), risk communication (Clause 11), and risk monitoring and review (Clause 12).

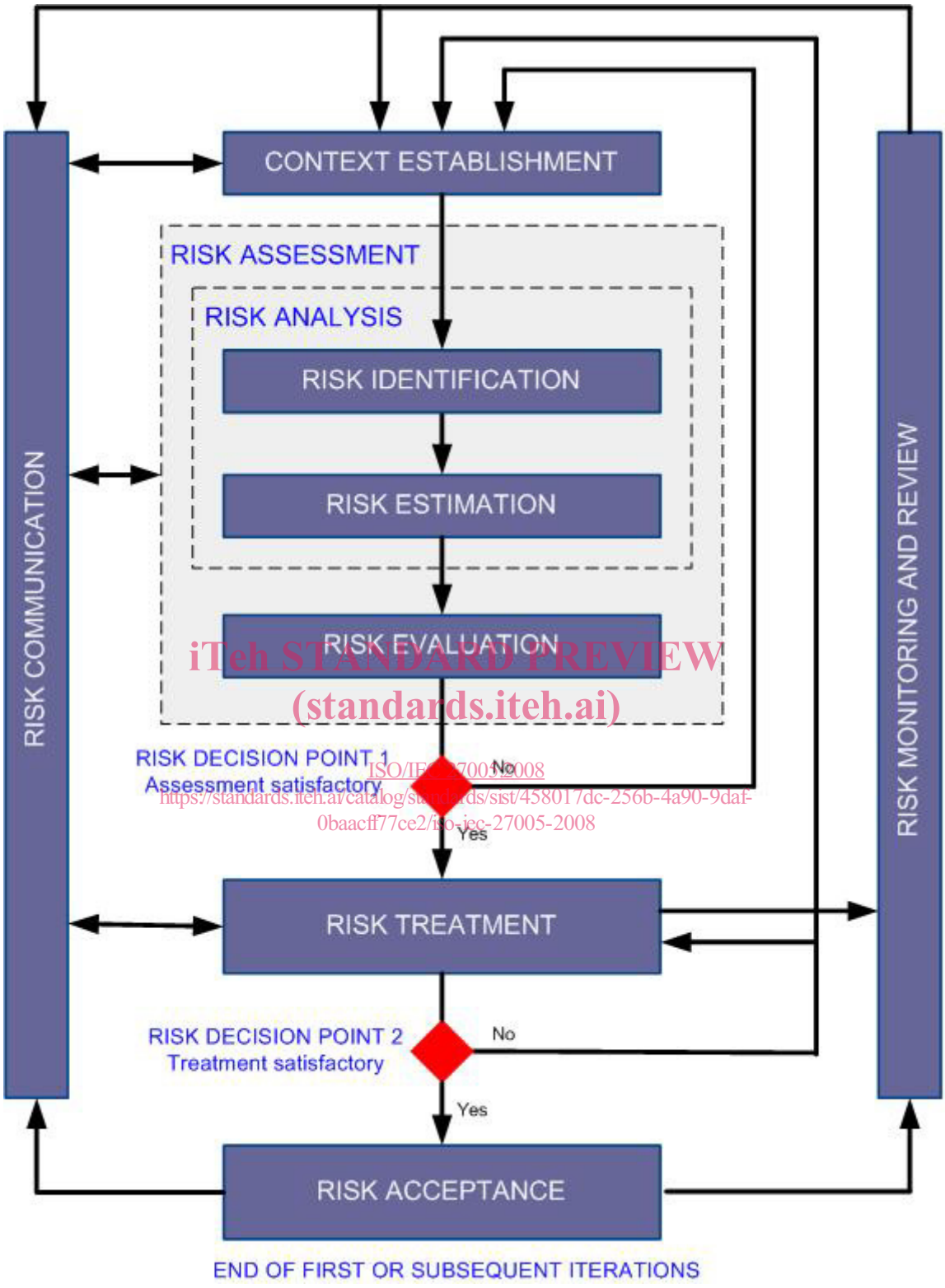

Figure 1 — Information security risk management process

As Figure 1 illustrates, the information security risk management process can be iterative for risk assessment and/or risk treatment activities. An iterative approach to conducting risk assessment can increase depth and detail of the assessment at each iteration. The iterative approach provides a good balance between minimizing the time and effort spent in identifying controls, while still ensuring that high risks are appropriately assessed.

The context is established first. Then a risk assessment is conducted. If this provides sufficient information to effectively determine the actions required to modify the risks to an acceptable level then the task is complete and the risk treatment follows. If the information is insufficient, another iteration of the risk assessment with revised context (e.g. risk evaluation criteria, risk acceptance criteria or impact criteria) will be conducted, possibly on limited parts of the total scope (see Figure 1, Risk Decision Point 1).

The effectiveness of the risk treatment depends on the results of the risk assessment. It is possible that the risk treatment will not immediately lead to an acceptable level of residual risk. In this situation, another iteration of the risk assessment with changed context parameters (e.g. risk assessment, risk acceptance or impact criteria), if necessary, may be required, followed by further risk treatment (see Figure 1, Risk Decision Point 2).

The risk acceptance activity has to ensure residual risks are explicitly accepted by the managers of the organization. This is especially important in a situation where the implementation of controls is omitted or postponed, e.g. due to cost.

During the whole information security risk management process it is important that risks and their treatment are communicated to the appropriate managers and operational staff. Even before the treatment of the risks, information about identified risks can be very valuable to manage incidents and may help to reduce potential damage. Awareness by managers and staff of the risks, the nature of the controls in place to mitigate the risks and the areas of concern to the organization assist in dealing with incidents and unexpected events in the most effective manner. The detailed results of every activity of the information security risk management process and from the two risk decision points should be documented.

ISO/IEC 27001 specifies that the controls implemented within the scope, boundaries and context of the ISMS shall be risk based. The application of an information security risk management process can satisfy this requirement. There are many approaches by which the process can be successfully implemented in an organization. The organization should use whatever approach best suits their circumstances for each specific application of the process.

In an ISMS, establishing the context, risk assessment, developing risk treatment plan and risk acceptance are all part of the “plan” phase. In the “do” phase of the ISMS, the actions and controls required to reduce the risk to an acceptable level are implemented according to the risk treatment plan. In the “check” phase of the ISMS, managers will determine the need for revisions of the risk assessment and risk treatment in the light of incidents and changes in circumstances. In the ”act” phase, any actions required, including additional application of the information security risk management process, are performed.

The following table summarizes the information security risk management activities relevant to the four phases of the ISMS process:

Table 1 — Alignment of ISMS and Information Security Risk Management Process

ISMS Process	Information Security Risk Management Process
Plan	Establishing the context Risk assessment Developing risk treatment plan Risk acceptance
Do	Implementation of risk treatment plan
Check	Continual monitoring and reviewing of risks
Act	Maintain and improve the Information Security Risk Management Process

7 Context establishment

7.1 General considerations

Input: All information about the organization relevant to the information security risk management context establishment.

Action: The context for information security risk management should be established, which involves setting the basic criteria necessary for information security risk management (7.2), defining the scope and boundaries (7.3), and establishing an appropriate organization operating the information security risk management (7.4).

Implementation guidance:

It is essential to determine the purpose of the information security risk management as this affects the overall process and the context establishment in particular. This purpose can be:

- Supporting an ISMS
- Legal compliance and evidence of due diligence
- Preparation of a business continuity plan
- Preparation of an incident response plan
- Description of the information security requirements for a product, a service or a mechanism

Implementation guidance for context establishment elements needed to support an ISMS is further discussed in Clauses 7.2, 7.3 and 7.4 below.

NOTE ISO/IEC 27001 does not use the term “context”. However, all of Clause 7 relates to the requirements “define the scope and boundaries of the ISMS” [4.2.1 a)], “define an ISMS policy” [4.2.1 b)] and “define the risk assessment approach” [4.2.1 c)], specified in ISO/IEC 27001.

Output: The specification of basic criteria, the scope and boundaries, and the organization for the information security risk management process.

7.2 Basic Criteria

Depending on the scope and objectives of the risk management, different approaches can be applied. The approach might also be different for each iteration.

An appropriate risk management approach should be selected or developed that addresses basic criteria such as: risk evaluation criteria, impact criteria, risk acceptance criteria.

Additionally, the organization should assess whether necessary resources are available to:

- Perform risk assessment and establish a risk treatment plan
- Define and implement policies and procedures, including implementation of the controls selected
- Monitor controls
- Monitor the information security risk management process

NOTE See also ISO/IEC 27001 (Clause 5.2.1) concerning the provision of resources for the implementation and operation of an ISMS.

Risk evaluation criteria

Risk evaluation criteria should be developed for evaluating the organization's information security risk considering the followings:

- The strategic value of the business information process
- The criticality of the information assets involved
- Legal and regulatory requirements, and contractual obligations
- Operational and business importance of availability, confidentiality and integrity
- Stakeholders expectations and perceptions, and negative consequences for goodwill and reputation

Additionally, risk evaluation criteria can be used to specify priorities for risk treatment.

Impact criteria

Impact criteria should be developed and specified in terms of the degree of damage or costs to the organization caused by an information security event considering the following:

- Level of classification of the impacted information asset
- Breaches of information security (e.g. loss of confidentiality, integrity and availability)
- Impaired operations (internal or third parties)
- Loss of business and financial value
- Disruption of plans and deadlines
- Damage of reputation
- Breaches of legal, regulatory or contractual requirements

NOTE See also ISO/IEC 27001 [Clause 4.2.1 d) 4] concerning the impact criteria identification for losses of confidentiality, integrity and availability.

Risk acceptance criteria

Risk acceptance criteria should be developed and specified. Risk acceptance criteria often depend on the organization's policies, goals, objectives and the interests of stakeholders.

An organization should define its own scales for levels of risk acceptance. The following should be considered during development:

- Risk acceptance criteria may include multiple thresholds, with a desired target level of risk, but provision for senior managers to accept risks above this level under defined circumstances
- Risk acceptance criteria may be expressed as the ratio of estimated profit (or other business benefit) to the estimated risk
- Different risk acceptance criteria may apply to different classes of risk, e.g. risks that could result in non-compliance with regulations or laws may not be accepted, while acceptance of high risks may be allowed if this is specified as a contractual requirement
- Risk acceptance criteria may include requirements for future additional treatment, e.g. a risk may be accepted if there is approval and commitment to take action to reduce it to an acceptable level within a defined time period

Risk acceptance criteria may differ according to how long the risk is expected to exist, e.g. the risk may be associated with a temporary or short term activity. Risk acceptance criteria should be set up considering the following:

- Business criteria
- Legal and regulatory aspects
- Operations
- Technology
- Finance
- Social and humanitarian factors

NOTE Risk acceptance criteria correspond to “criteria for accepting risks and identify the acceptable level of risk” specified in ISO/IEC 27001 Clause 4.2.1 c) 2).

More information can be found in Annex A.

7.3 The scope and boundaries

The organization should define the scope and boundaries of information security risk management.

The scope of the information security risk management process needs to be defined to ensure that all relevant assets are taken into account in the risk assessment. In addition, the boundaries need to be identified [see also ISO/IEC 27001 Clause 4.2.1 a)] to address those risks that might arise through these boundaries.

Information about the organization should be collected to determine the environment it operates in and its relevance to the information security risk management process.

When defining the scope and boundaries, the organization should consider the following information:

- The organization's strategic business objectives, strategies and policies
- Business processes
- The organization's functions and structure
- Legal, regulatory and contractual requirements applicable to the organization
- The organization's information security policy
- The organization's overall approach to risk management
- Information assets
- Locations of the organization and their geographical characteristics
- Constraints affecting the organization
- Expectation of stakeholders
- Socio-cultural environment
- Interfaces (i.e. information exchange with the environment)

Additionally, the organization should provide justification for any exclusion from the scope.

Examples of the risk management scope may be an IT application, IT infrastructure, a business process, or a defined part of an organization.

NOTE The scope and boundaries of the information security risk management is related to the scope and boundaries of the ISMS required in ISO/IEC 27001 4.2.1 a).

Further information can be found in Annex A.

7.4 Organization for information security risk management

The organization and responsibilities for the information security risk management process should be set up and maintained. The following are the main roles and responsibilities of this organization:

- Development of the information security risk management process suitable for the organization
- Identification and analysis of the stakeholders
- Definition of roles and responsibilities of all parties both internal and external to the organization
- Establishment of the required relationships between the organization and stakeholders, as well as interfaces to the organization's high level risk management functions (e.g. operational risk management), as well as interfaces to other relevant projects or activities
- Definition of decision escalation paths
- Specification of records to be kept

This organization should be approved by the appropriate managers of the organization.

NOTE ISO/IEC 27001 requires determination and provision of the resources needed to establish, implement, operate, monitor, review, maintain and improve an ISMS [5.2.1 a)]. The organization for risk management operations may be regarded as one of the resources required by ISO/IEC 27001.

8 Information security risk assessment

8.1 General description of information security risk assessment

NOTE Risk assessment activity is referred to as process in ISO/IEC 27001.

Input: Basic criteria, the scope and boundaries, and the organization for the information security risk management process being established.

Action: Risks should be identified, quantified or qualitatively described, and prioritized against risk evaluation criteria and objectives relevant to the organization.

