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/IEC 2008

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2008

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

© ISO/IEC 2008 – All rights reserved

Not for Resale

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

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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**

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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).

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

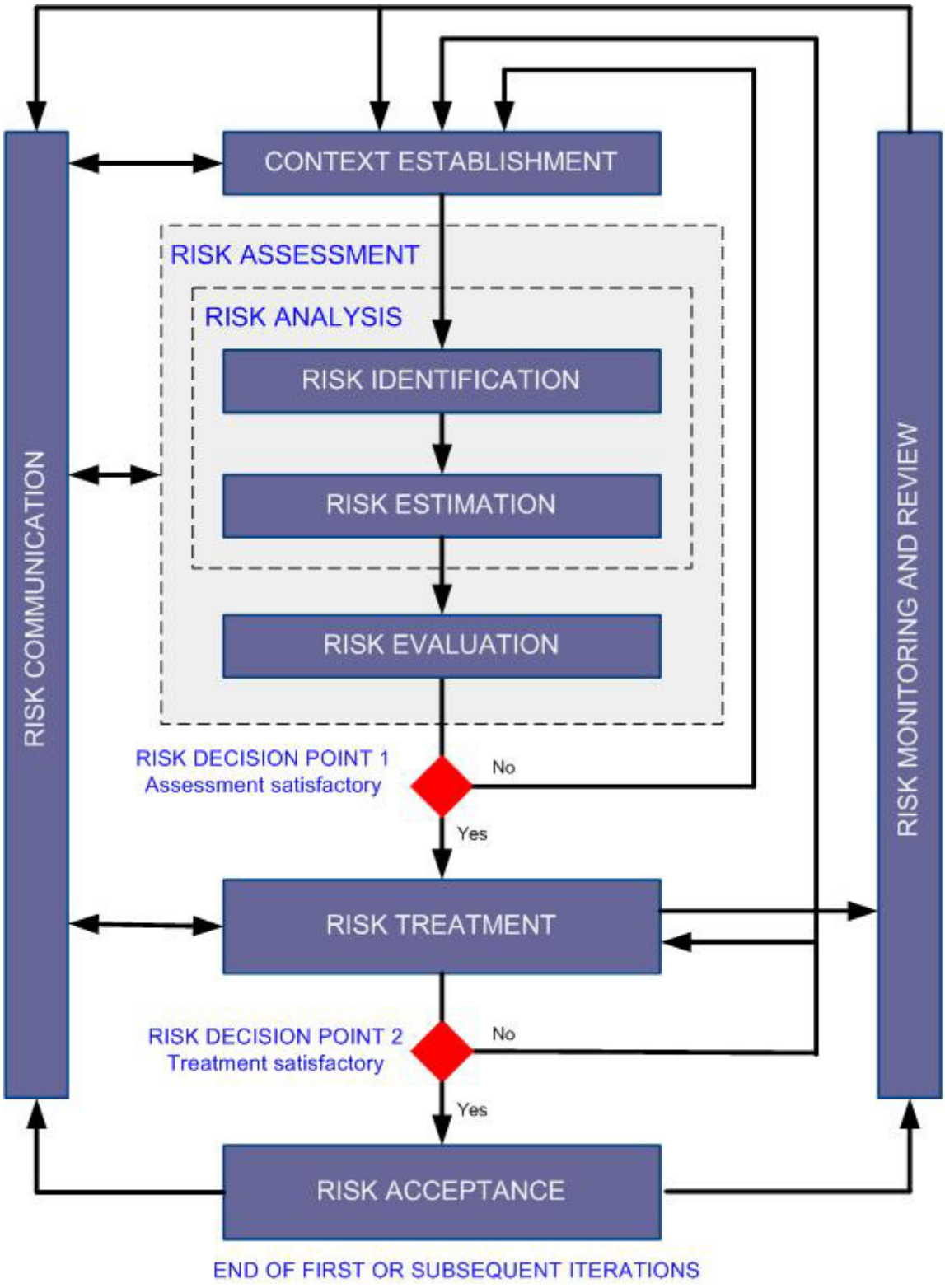

Figure 1 — Information security risk management process

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.

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Implementation guidance:

A risk is a combination of the consequences that would follow from the occurrence of an unwanted event and the likelihood of the occurrence of the event. Risk assessment quantifies or qualitatively describes the risk and enables managers to prioritize risks according to their perceived seriousness or other established criteria.

Risk assessment consists of the following activities:

- Risk analysis (Clause 8.2) which comprises:
  - Risk identification (Clause 8.2.1)
  - Risk estimation (Clause 8.2.2)
- Risk evaluation (Clause 8.3)

Risk assessment determines the value of the information assets, identifies the applicable threats and vulnerabilities that exist (or could exist), identifies the existing controls and their effect on the risk identified, determines the potential consequences and finally prioritizes the derived risks and ranks them against the risk evaluation criteria set in the context establishment.

Risk assessment is often conducted in two (or more) iterations. First a high level assessment is carried out to identify potentially high risks that warrant further assessment. The next iteration can involve further in-depth consideration of potentially high risks revealed in the initial iteration. Where this provides insufficient information to assess the risk then further detailed analyses are conducted, probably on parts of the total scope, and possibly using a different method.

It is up to the organization to select its own approach to risk assessment based on the objectives and the aim of the risk assessment.

Discussion on information security risk assessment approaches can be found in Annex E.

Output: A list of assessed risks prioritized according to risk evaluation criteria.

8.2 Risk analysis

8.2.1 Risk identification

8.2.1.1 Introduction to risk identification

The purpose of risk identification is to determine what could happen to cause a potential loss, and to gain insight into how, where and why the loss might happen. The steps described in the following subclauses of 8.2.1 should collect input data for the risk estimation activity.

NOTE Activities described in subsequent clauses may be conducted in a different order depending on the methodology applied.

8.2.1.2 Identification of assets

Input: Scope and boundaries for the risk assessment to be conducted, list of constituents with owners, location, function, etc.

Action: The assets within the established scope should be identified (relates to ISO/IEC 27001, Clause 4.2.1 d) 1)).

Implementation guidance:

An asset is anything that has value to the organization and which therefore requires protection. For the identification of assets it should be borne in mind that an information system consists of more than hardware and software.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Asset identification should be performed at a suitable level of detail that provides sufficient information for the risk assessment. The level of detail used on the asset identification will influence the overall amount of information collected during the risk assessment. The level can be refined in further iterations of the risk assessment.

An asset owner should be identified for each asset, to provide responsibility and accountability for the asset. The asset owner may not have property rights to the asset, but has responsibility for its production, development, maintenance, use and security as appropriate. The asset owner is often the most suitable person to determine the asset's value to the organization (see 8.2.2.2 for asset valuation).

The review boundary is the perimeter of assets of the organization defined to be managed by the information security risk management process.

More information on the identification and valuation of assets as related to information security can be found in Annex B.

Output: A list of assets to be risk-managed, and a list of business processes related to assets and their relevance.

8.2.1.3 Identification of threats

Input: Information on threats obtained from incident reviewing, asset owners, users and other sources, including external threat catalogues.

Action: Threats and their sources should be identified (relates to ISO/IEC 27001, Clause 4.2.1 d) 2)).

Implementation guidance:

A threat has the potential to harm assets such as information, processes and systems and therefore organizations. Threats may be of natural or human origin, and could be accidental or deliberate. Both accidental and deliberate threat sources should be identified. A threat may arise from within or from outside the organization. Threats should be identified generically and by type (e.g. unauthorized actions, physical damage, technical failures) and then where appropriate individual threats within the generic class identified. This means no threat is overlooked, including the unexpected, but the volume of work required is limited.

Some threats may affect more than one asset. In such cases they may cause different impacts depending on which assets are affected.

Input to the threat identification and estimation of the likelihood of occurrence (see 8.2.2.3) may be obtained from the asset owners or users, from human resources staff, from facility management and information security specialists, physical security experts, legal department and other organizations including legal bodies, weather authorities, insurance companies and national government authorities. Aspects of environment and culture must be considered when addressing threats.

Internal experience from incidents and past threat assessments should be considered in the current assessment. It might be worthwhile to consult other threat catalogues (maybe specific to an organization or business) to complete the list of generic threats, where relevant. Threat catalogues and statistics are available from industry bodies, national governments, legal bodies, insurance companies etc.

When using threat catalogues, or the results of earlier threat assessments, one should be aware that there is continual change of relevant threats, especially if the business environment or information systems change.

More information on threat types can be found in Annex C.

Output: A list of threats with the identification of threat type and source.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

8.2.1.4 Identification of existing controls

Input: Documentation of controls, risk treatment implementation plans.

Action: Existing and planned controls should be identified.

Implementation guidance:

Identification of existing controls should be made to avoid unnecessary work or cost, e.g. in the duplication of controls. In addition, while identifying the existing controls, a check should be made to ensure that the controls are working correctly – a reference to already existing ISMS audit reports should limit the time expended in this task. If a control does not work as expected, this may cause vulnerabilities. Consideration should be given to the situation where a selected control (or strategy) fails in operation and therefore complementary controls are required to address the identified risk effectively. In an ISMS, according to ISO/IEC 27001, this is supported by the measurement of control effectiveness. A way to estimate the effect of the control is to see how it reduces the threat likelihood and ease of exploiting the vulnerability, or impact of the incident. Management reviews and audit reports also provide information about the effectiveness of existing controls.

Controls that are planned to be implemented according to the risk treatment implementation plans should be considered in the same way like those already implemented.

An existing or planned control might be identified as ineffective, or not sufficient, or not justified. If not justified or not sufficient, the control should be checked to determine whether it should be removed, replaced by another, more suitable control, or whether it should stay in place, for example, for cost reasons.

For the identification of existing or planned controls, the following activities can be helpful:

- Reviewing documents containing information about the controls (for example, risk treatment implementation plans). If the processes of information security management are well documented all existing or planned controls and the status of their implementation should be available;
- Checking with the people responsible for information security (e.g. information security officer and information system security officer, building manager or operations manager) and the users as to which controls are really implemented for the information process or information system under consideration;
- Conducting an on-site review of the physical controls, comparing those implemented with the list of what controls should be there, and checking those implemented as to whether they are working correctly and effectively, or
- Reviewing results of internal audits

Output: A list of all existing and planned controls, their implementation and usage status.

8.2.1.5 Identification of vulnerabilities

Input: A list of known threats, lists of assets and existing controls.

Action: Vulnerabilities that can be exploited by threats to cause harm to assets or to the organization should be identified (relates to ISO/IEC 27001, Clause 4.2.1 d) 3)).

Implementation guidance:

Vulnerabilities may be identified in following areas:

- Organization
- Processes and procedures
- Management routines
- Personnel
- Physical environment
- Information system configuration
- Hardware, software or communications equipment
- Dependence on external parties

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The presence of a vulnerability does not cause harm in itself, as there needs to be a threat present to exploit it. A vulnerability that has no corresponding threat may not require the implementation of a control, but should be recognized and monitored for changes. It should be noted that an incorrectly implemented or malfunctioning control or control being used incorrectly could itself be a vulnerability. A control can be effective or ineffective depending on the environment in which it operates. Conversely, a threat that does not have a corresponding vulnerability may not result in a risk.

Vulnerabilities can be related to properties of the asset that can be used in a way, or for a purpose, other than that intended when the asset was purchased or made. Vulnerabilities arising from different sources need to be considered, for example, those intrinsic or extrinsic to the asset.

Examples of vulnerabilities and methods for vulnerability assessment can be found in Annex D.

Output: A list of vulnerabilities in relation to assets, threats and controls; a list of vulnerabilities that do not relate to any identified threat for review.

8.2.1.6 Identification of consequences

Input: A list of assets, a list of business processes, and a list of threats and vulnerabilities, where appropriate, related to assets and their relevance.

Action: The consequences that losses of confidentiality, integrity and availability may have on the assets should be identified (see ISO/IEC 27001 4.2.1 d) 4)).

Implementation guidance:

A consequence can be loss of effectiveness, adverse operating conditions, loss of business, reputation, damage, etc.

This activity identifies the damage or consequences to the organization that could be caused by an incident scenario. An incident scenario is the description of a threat exploiting a certain vulnerability or set of vulnerabilities in an information security incident (see ISO/IEC 27002, Clause 13). The impact of the incident scenarios is to be determined considering impact criteria defined during the context establishment activity. It may affect one or more assets or part of an asset. Thus assets may have assigned values both for their financial cost and because of the business consequences if they are damaged or compromised. Consequences may be of a temporary nature or may be permanent as in the case of the destruction of an asset.

NOTE ISO/IEC 27001 describes the occurrence of incident scenarios as “security failures".

Organizations should identify the operational consequences of incident scenarios in terms of (but not limited to):

- Investigation and repair time
- (Work)time lost
- Opportunity lost
- Health and Safety
- Financial cost of specific skills to repair the damage
- Image reputation and goodwill

Details on assessment of technical vulnerabilities can be found in B.3 Impact Assessment.

Output: A list of incident scenarios with their consequences related to assets and business processes.

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

8.2.2 Risk estimation

8.2.2.1 Risk estimation methodologies

Risk analysis may be undertaken in varying degrees of detail depending on the criticality of assets, extent of vulnerabilities known, and prior incidents involving in the organization. An estimation methodology may be qualitative or quantitative, or a combination of these, depending on the circumstances. In practice, qualitative estimation is often used first to obtain a general indication of the level of risk and to reveal the major risks. Later it may be necessary to undertake more specific or quantitative analysis on the major risks because it is usually less complex and less expensive to perform qualitative than quantitative analysis.

The form of analysis should be consistent with the risk evaluation criteria developed as part of establishing the context.

Further details of estimation methodologies are now described:

(a) Qualitative estimation:

Qualitative estimation uses a scale of qualifying attributes to describe the magnitude of potential consequences (e.g. Low, Medium and High) and the likelihood that those consequences will occur. An advantage of qualitative estimation is its ease of understanding by all relevant personnel while a disadvantage is the dependence on subjective choice of the scale.

These scales can be adapted or adjusted to suit the circumstances and different descriptions may be used for different risks. Qualitative estimation may be used:

- As an initial screening activity to identify risks that require more detailed analysis
- Where this kind of analysis is appropriate for decisions
- Where the numerical data or resources are inadequate for a quantitative estimation

Qualitative analysis should use factual information and data where available.

(b) Quantitative estimation:

Quantitative estimation uses a scale with numerical values (rather than the descriptive scales used in qualitative estimation) for both consequences and likelihood, using data from a variety of sources. The quality of the analysis depends on the accuracy and completeness of the numerical values and the validity of the models used. Quantitative estimation in most cases uses historical incident data, providing the advantage that it can be related directly to the information security objectives and concerns of the organization. A disadvantage is the lack of such data on new risks or information security weaknesses. A disadvantage of the quantitative approach may occur where factual, auditable data is not available thus creating an illusion of worth and accuracy of the risk assessment.

The way in which consequences and likelihood are expressed and the ways in which they are combined to provide a level of risk will vary according to the type of risk and the purpose for which the risk assessment output is to be used. The uncertainty and variability of both consequences and likelihood should be considered in the analysis and communicated effectively.

8.2.2.2 Assessment of consequences

Input: A list of identified relevant incident scenarios, including identification of threats, vulnerabilities, affected assets, consequences to assets and business processes.

Action: The business impact upon the organization that might result from possible or actual information security incidents should be assessed, taking into account the consequences of a breach of information security such as loss of confidentiality, integrity or availability of the assets (relates to ISO/IEC 27001, Clause 4.2.1 e) 1)).

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Implementation Guidance:

After identifying all assets under review, values assigned to these assets should be taken into account while assessing the consequences.

The business impact value can be expressed in qualitative and quantitative forms, but any method of assigning monetary value may generally provide more information for decision making and hence facilitate a more efficient decision making process.

Asset valuation begins with classification of assets according to their criticality, in terms of the importance of assets to fulfilling the business objectives of the organization. Valuation is then determined using two measures:

- the replacement value of the asset: the cost of recovery cleanup and replacing the information (if at all possible), and
- the business consequences of loss or compromise of the asset, such as the potential adverse business and/or legal or regulatory consequences from the disclosure, modification, non-availability and/or destruction of information, and other information assets

This valuation can be determined from a business impact analysis. The value, determined by the consequence for business, is usually significantly higher than the simple replacement cost, depending on the importance of the asset to the organization in meeting its business objectives.

Asset valuation is a key factor in the impact assessment of an incident scenario, because the incident may affect more than one asset (e.g. dependent assets), or only a part of an asset. Different threats and vulnerabilities will have different impacts on assets, such as a loss of confidentiality, integrity or availability. Assessment of consequences is thus related to asset valuation based on the business impact analysis.

Consequences or business impact may be determined by modelling the outcomes of an event or set of events, or by extrapolation from experimental studies or past data.

Consequences may be expressed in terms of monetary, technical or human impact criteria, or other criteria relevant to the organization. In some cases, more than one numerical value is required to specify consequences for different times, places, groups or situations.

Consequences in time and finance should be measured with the same approach used for threat likelihood and vulnerability. Consistency has to be maintained on the quantitative or the qualitative approach.

More information both on asset valuation and impact assessment can be found in Annex B.

Output: A list of assessed consequences of an incident scenario expressed with respect to assets and impact criteria.

8.2.2.3 Assessment of incident likelihood

Input: A list of identified relevant incident scenarios, including identification of threats, affected assets, exploited vulnerabilities and consequences to assets and business processes. Furthermore, lists of all existing and planned controls, their effectiveness, implementation and usage status.

Action: The likelihood of the incident scenarios should be assessed (relates to ISO/IEC 27001, Clause 4.2.1 e) 2)).

Implementation guidance:

After identifying the incident scenarios, it is necessary to assess the likelihood of each scenario and impact occurring, using qualitative or quantitative estimation techniques. This should take account of how often the threats occur and how easily the vulnerabilities may be exploited, considering:

- experience and applicable statistics for threat likelihood

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

- for deliberate threat sources: the motivation and capabilities, which will change over time, and resources available to possible attackers, as well as the perception of attractiveness and vulnerability of assets for a possible attacker
- for accidental threat sources: geographical factors e.g. proximity to chemical or petroleum plants, the possibility of extreme weather conditions, and factors that could influence human errors and equipment malfunction
- vulnerabilities, both individually and in aggregation
- existing controls and how effectively they reduce vulnerabilities

For instance, an information system may have a vulnerability to the threats of masquerading of user identity and misuse of resources. The vulnerability of masquerading of user identity may be high because of lack of user authentication. On the other hand, the likelihood of misuse of resources may be low, despite lack of user authentication, because ways to misuse resources are limited.

Depending on the need for accuracy, assets could be grouped, or it might be necessary to split assets into their elements and relate the scenarios to the elements. For example, across geographical locations, the nature of threats to the same types of assets may change, or the effectiveness of existing controls may vary.

Output: Likelihood of incident scenarios (quantitative or qualitative).

8.2.2.4 Level of risk estimation

Input: A list of incident scenarios with their consequences related to assets and business processes and their likelihood (quantitative or qualitative).

Action: The level of risk should be estimated for all relevant incident scenarios (relates to ISO/IEC 27001, Clause 4.2.1 e) 4)).

Implementation guidance:

Risk estimation assigns values to the likelihood and the consequences of a risk. These values may be quantitative or qualitative. Risk estimation is based on assessed consequences and likelihood. Additionally, it can consider cost benefit, the concerns of stakeholders, and other variables, as appropriate for risk evaluation. The estimated risk is a combination of the likelihood of an incident scenario and its consequences.

Examples of different information security risk estimation methods or approaches can be found in Annex E.

Output: A list of risks with value levels assigned.

8.3 Risk evaluation

Input: A list of risks with value levels assigned and risk evaluation criteria.

Action: Level of risks should be compared against risk evaluation criteria and risk acceptance criteria (relates to ISO/IEC 27001, Clause 4.2.1 e) 4)).

Implementation guidance:

The nature of the decisions pertaining to risk evaluation and risk evaluation criteria that will be used to make those decisions would have been decided when establishing the context. These decisions and the context should be revisited in more detail at this stage when more is known about the particular risks identified. To evaluate risks, organizations should compare the estimated risks (using selected methods or approaches as discussed in Annex E) with the risk evaluation criteria defined during the context establishment.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Risk evaluation criteria used to make decisions should be consistent with the defined external and internal information security risk management context and take into account the objectives of the organization and stakeholder views etc. Decisions as taken in the risk evaluation activity are mainly based on the acceptable level of risk. However, consequences, likelihood, and the degree of confidence in the risk identification and analysis should be considered as well. Aggregation of multiple low or medium risks may result in much higher overall risks and need to be addressed accordingly.

Considerations should include:

- *Information security properties*: if one criterion is not relevant for the organization (e.g. loss of confidentiality), then all risks impacting this criterion may not be relevant

- *The importance of the business process or activity supported by a particular asset or set of assets*: if the process is determined to be of low importance, risks associated with it should be given a lower consideration than risks that impact more important processes or activities

Risk evaluation uses the understanding of risk obtained by risk analysis to make decisions about future actions. Decisions should include:

- Whether an activity should be undertaken
- Priorities for risk treatment considering estimated levels of risks

During the risk evaluation stage, contractual, legal and regulatory requirements are factors that should be taken into account in addition to the estimated risks.

Output: A list of risks prioritized according to risk evaluation criteria in relation to the incident scenarios that lead to those risks.

9 Information security risk treatment

9.1 General description of risk treatment

Input: A list of risks prioritized according to risk evaluation criteria in relation to the incident scenarios that lead to those risks.

Action: Controls to reduce, retain, avoid, or transfer the risks should be selected and a risk treatment plan defined.

Implementation guidance:

There are four options available for risk treatment: risk reduction (see 9.2), risk retention (see 9.3), risk avoidance (see 9.4) and risk transfer (see 9.5).

NOTE ISO/IEC 27001 4.2.1. f) 2) uses the term “accepting risk” instead of “retaining risk”.

Figure 2 illustrates the risk treatment activity within the information security risk management process as presented in Figure 1.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

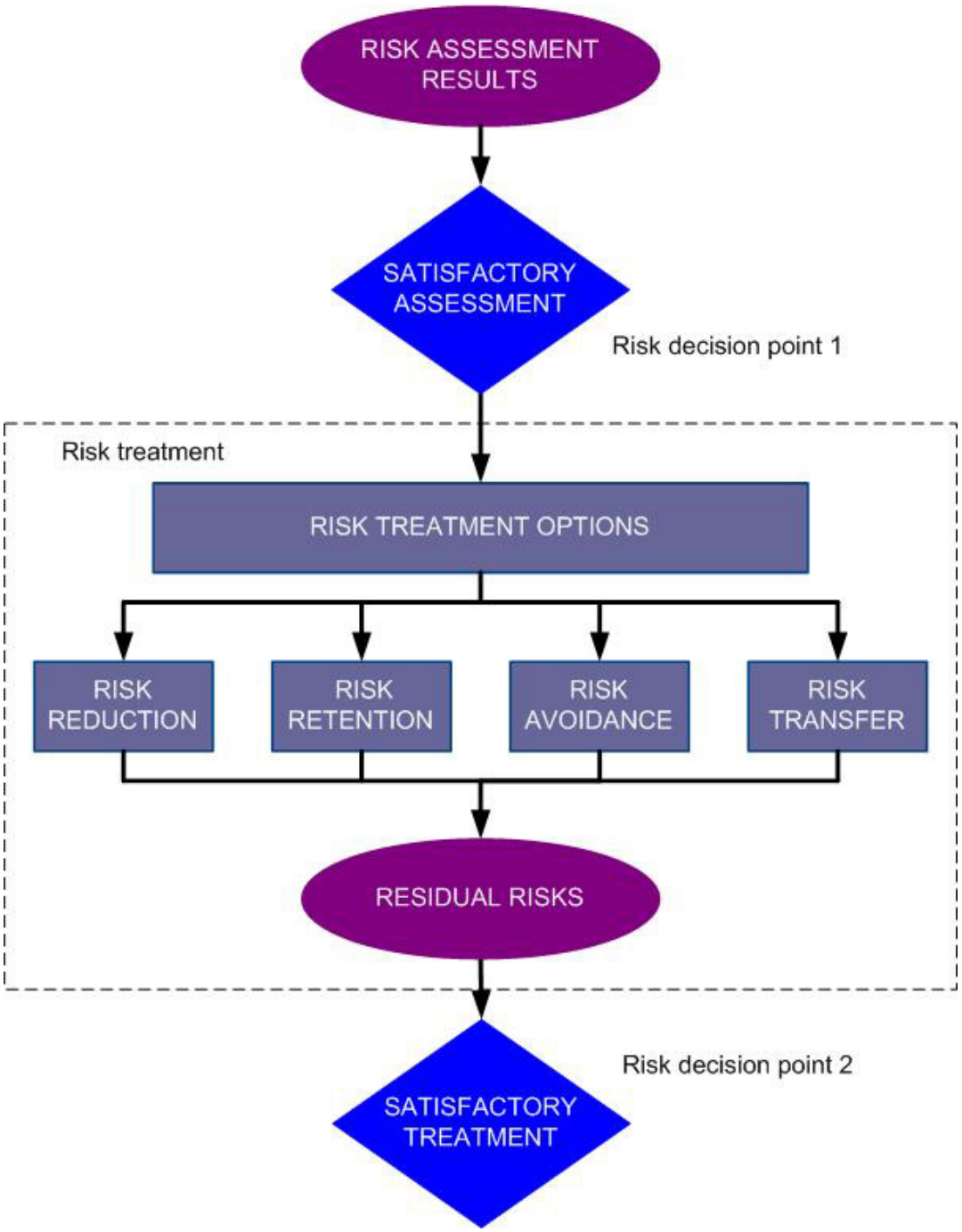

Figure 2 — The risk treatment activity

Risk treatment options should be selected based on the outcome of the risk assessment, the expected cost for implementing these options and the expected benefits from these options.

When large reductions in risks may be obtained with relatively low expenditure, such options should be implemented. Further options for improvements may be uneconomic and judgement needs to be exercised as to whether they are justifiable.

In general, the adverse consequences of risks should be made as low as reasonably practicable and irrespective of any absolute criteria. Managers should consider rare but severe risks. In such cases, controls that are not justifiable on strictly economic grounds may need to be implemented (for example, business continuity controls considered to cover specific high risks).

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The four options for risk treatment are not mutually exclusive. Sometimes the organization can benefit substantially by a combination of options such as reducing the likelihood of risks, reducing their consequences, and transferring or retaining any residual risks.

Some risk treatments can effectively address more than one risk (e.g. information security training and awareness). A risk treatment plan should be defined which clearly identifies the priority ordering in which individual risk treatments should be implemented and their timeframes. Priorities can be established using various techniques, including risk ranking and cost-benefit analysis. It is the organization's managers' responsibility to decide the balance between the costs of implementing controls and the budget assignment.

The identification of existing controls may determine that existing controls exceed current needs, in terms of cost comparisons, including maintenance. If removing redundant or unnecessary controls is considered (especially if the controls have high maintenance costs), information security and cost factors should be taken into account. Since controls may influence each other, removing redundant controls might reduce the overall security in place. In addition, it may be cheaper to leave redundant or unnecessary controls in place than to remove them.

Risk treatment options should be considered taking into account:

- How risk is perceived by affected parties
- The most appropriate ways to communicate to those parties

Context establishment (see 7.2 – Risk evaluation criteria) provides information on legal and regulatory requirements with which the organization needs to comply. The risk to organizations is failure to comply and treatment options to limit this possibility should be implemented. All constraints - organizational, technical, structural etc. - that are identified during the context establishment activity should be taken into account during the risk treatment.

Once the risk treatment plan has been defined, residual risks need to be determined. This involves an update or re-iteration of the risk assessment, taking into account the expected effects of the proposed risk treatment. Should the residual risk still not meet the organization's risk acceptance criteria, a further iteration of risk treatment may be necessary before proceeding to risk acceptance. More information can be found in ISO/IEC 27002, Clause 0.3.

Output: Risk treatment plan and residual risks subject to the acceptance decision of the organization's managers.

9.2 Risk reduction

Action: The level of risk should be reduced through the selection of controls so that the residual risk can be re-assessed as being acceptable.

Implementation guidance:

Appropriate and justified controls should be selected to meet the requirements identified by the risk assessment and risk treatment. This selection should take account of the risk acceptance criteria as well as legal, regulatory and contractual requirements. This selection should also take account of cost and timeframe for implementation of controls, or technical, environmental and cultural aspects. It is often possible to lower the total cost of ownership of a system with properly selected information security controls.

In general, controls may provide one or more of the following types of protection: correction, elimination, prevention, impact minimization, deterrence, detection, recovery, monitoring and awareness. During control selection it is important to weigh the cost of acquisition, implementation, administration, operation, monitoring, and maintenance of the controls against the value of the assets being protected. Furthermore, the return on investment in terms of risk reduction and potential to exploit new business opportunities afforded by certain controls should be considered. Additionally, consideration should be given to specialized skills that may be needed to define and implement new controls or modify existing ones.

ISO/IEC 27002 provides detailed information on controls.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

There are many constraints that can affect the selection of controls. Technical constraints such as performance requirements, manageability (operational support requirements) and compatibility issues may hamper the use of certain controls or could induce human error either nullifying the control, giving a false sense of security or even increasing the risk beyond not having the control (e.g. requiring complex passwords without proper training, leading to users writing passwords down). Moreover, it could be the case that a control would affect performance. Managers should try to identify a solution that satisfies performance requirements while guaranteeing sufficient information security. The result of this step is a list of possible controls, with their cost, benefit, and priority of implementation.

Various constraints should be taken into account when selecting controls and during implementation. Typically, the following are considered:

- Time constraints
- Financial constraints
- Technical constraints
- Operational constrains
- Cultural constraints
- Ethical constraints
- Environmental constraints
- Legal constraints
- Ease of use
- Personnel constraints
- Constraints for integrating new and existing controls

More information on the constraints for risk reduction can be found in Annex F.

9.3 Risk retention

Action: The decision on retaining the risk without further action should be taken depending on risk evaluation.

NOTE ISO/IEC 27001 4.2.1 f 2) “knowingly and objectively accepting risks, providing they clearly satisfy the organization’ policies and the criteria for accepting risks” describes the same activity.

Implementation guidance:

If the level of risk meets the risk acceptance criteria, there is no need for implementing additional controls and the risk can be retained.

9.4 Risk avoidance

Action: The activity or condition that gives rise to the particular risk should be avoided.

Implementation guidance:

When the identified risks are considered too high, or the costs of implementing other risk treatment options exceed the benefits, a decision may be made to avoid the risk completely, by withdrawing from a planned or existing activity or set of activities, or changing the conditions under which the activity is operated. For example, for risks caused by nature it may be most cost effective alternative to physically move the information processing facilities to a place where the risk does not exist or is under control.

9.5 Risk transfer

Action: The risk should be transferred to another party that can most effectively manage the particular risk depending on risk evaluation.

Implementation guidance:

Risk transfer involves a decision to share certain risks with external parties. Risk transfer can create new risks or modify existing, identified risks. Therefore, additional risk treatment may be necessary.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Transfer can be done by insurance that will support the consequences, or by sub-contracting a partner whose role will be to monitor the information system and take immediate actions to stop an attack before it makes a defined level of damage.

It should be noted that it may be possible to transfer the responsibility to manage risk but it is not normally possible to transfer the liability of an impact. Customers will usually attribute an adverse impact as being the fault of the organization.

10 Information security risk acceptance

Input: Risk treatment plan and residual risk assessment subject to the acceptance decision of the organization's managers.

Action: The decision to accept the risks and responsibilities for the decision should be made and formally recorded (this relates to ISO/IEC 27001 paragraph 4.2.1 h)).

Implementation guidance:

Risk treatment plans should describe how assessed risks are to be treated to meet risk acceptance criteria (see Clause 7.2 Risk acceptance criteria). It is important for responsible managers to review and approve proposed risk treatment plans and resulting residual risks, and record any conditions associated with such approval.

Risk acceptance criteria can be more complex than just determining whether or not a residual risk falls above or below a single threshold.

In some cases the level of residual risk may not meet risk acceptance criteria because the criteria being applied do not take into account prevailing circumstances. For example, it might be argued that it is necessary to accept risks because the benefits accompanying the risks are very attractive, or because the cost of risk reduction is too high. Such circumstances indicate that risk acceptance criteria are inadequate and should be revised if possible. However, it is not always possible to revise the risk acceptance criteria in a timely manner. In such cases, decision makers may have to accept risks that do not meet normal acceptance criteria. If this is necessary, the decision maker should explicitly comment on the risks and include a justification for the decision to override normal risk acceptance criteria.

Output: A list of accepted risks with justification for those that do not meet the organization's normal risk acceptance criteria.

11 Information security risk communication

Input: All risk information obtained from the risk management activities (see Figure 1).

Action: Information about risk should be exchanged and/or shared between the decision-maker and other stakeholders.

Implementation guidance:

Risk communication is an activity to achieve agreement on how to manage risks by exchanging and/or sharing information about risk between the decision-makers and other stakeholders. The information includes, but is not limited to the existence, nature, form, likelihood, severity, treatment, and acceptability of risks.

Effective communication among stakeholders is important since this may have a significant impact on decisions that must be made. Communication will ensure that those responsible for implementing risk management, and those with a vested interest understand the basis on which decisions are made and why particular actions are required. Communication is bi-directional.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Perceptions of risk can vary due to differences in assumptions, concepts and the needs, issues and concerns of stakeholders as they relate to risk or the issues under discussion. Stakeholders are likely to make judgments on the acceptability of risk based on their perception of risk. This is especially important to ensure that the stakeholders' perceptions of risk, as well as their perceptions of benefits, can be identified and documented and the underlying reasons clearly understood and addressed.

Risk communication should be carried out in order to achieve the following:

- To provide assurance of the outcome of the organization's risk management
- To collect risk information
- To share the results from the risk assessment and present the risk treatment plan
- To avoid or reduce both occurrence and consequence of information security breaches due to the lack of mutual understanding among decision makers and stakeholders
- To support decision-making
- To obtain new information security knowledge
- To co-ordinate with other parties and plan responses to reduce consequences of any incident
- To give decision makers and stakeholders a sense of responsibility about risks
- To improve awareness

An organization should develop risk communication plans for normal operations as well as for emergency situations. Therefore, risk communication activity should be performed continually.

The co-ordination between major decision makers and stakeholders may be achieved by the formation of a committee where debate about risks, their prioritization and appropriate treatment, and acceptance can take place.

It is important to cooperate with the appropriate public relations or communications unit within the organization to coordinate all tasks related to risk communication. This is crucial in the event of crisis communication actions, for example, in response to particular incidents.

Output: Continual understanding of the organization's information security risk management process and results.

12 Information security risk monitoring and review

12.1 Monitoring and review of risk factors

Input: All risk information obtained from the risk management activities (see Figure 1).

Action: Risks and their factors (i.e. value of assets, impacts, threats, vulnerabilities, likelihood of occurrence) should be monitored and reviewed to identify any changes in the context of the organization at an early stage, and to maintain an overview of the complete risk picture.

Implementation guidance:

Risks are not static. Threats, vulnerabilities, likelihood or consequences may change abruptly without any indication. Therefore constant monitoring is necessary to detect these changes. This may be supported by external services that provide information regarding new threats or vulnerabilities.

Organizations should ensure that the following are continually monitored:

- New assets that have been included in the risk management scope
- Necessary modification of asset values, e.g. due to changed business requirements
- New threats that could be active both outside and inside the organization and that have not been assessed
- Possibility that new or increased vulnerabilities could allow threats to exploit these new or changed vulnerabilities
- Identified vulnerabilities to determine those becoming exposed to new or re-emerging threats

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

- Increased impact or consequences of assessed threats, vulnerabilities and risks in aggregation resulting in an unacceptable level of risk
- Information security incidents

New threats, vulnerabilities or changes in likelihood or consequences can increase risks previously assessed as low ones. Review of low and accepted risks should consider each risk separately, and all such risks as an aggregate as well, to assess their potential accumulated impact. If risks do not fall into the low or acceptable risk category, they should be treated using one or more of the options considered in Clause 9.

Factors that affect the likelihood and consequences of threats occurring could change, as could factors that affect the suitability or cost of the various treatment options. Major changes affecting the organization should be reason for a more specific review. Therefore, the risk monitoring activities should be regularly repeated and the selected options for risk treatment should be reviewed periodically.

The outcome of risk monitoring activities may be input to other risk review activities. The organization should review all risks regularly, and when major changes occur (according to ISO/IEC 27001, Clause 4.2.3)).

Output: Continual alignment of the management of risks with the organization's business objectives, and with risk acceptance criteria.

12.2 Risk management monitoring, reviewing and improving

Input: All risk information obtained from the risk management activities (see Figure 1).

Action: The information security risk management process should be continually monitored, reviewed and improved as necessary and appropriate.

Implementation guidance:

Ongoing monitoring and review is necessary to ensure that the context, the outcome of the risk assessment and risk treatment, as well as management plans, remain relevant and appropriate to the circumstances.

The organization should make sure that the information security risk management process and related activities remain appropriate in the present circumstances and are followed. Any agreed improvements to the process or actions necessary to improve compliance with the process should be notified to the appropriate managers to have assurance that no risk or risk element is overlooked or underestimated and that the necessary actions are taken and decisions are made to provide a realistic risk understanding and ability to respond.

Additionally, the organization should regularly verify that the criteria used to measure the risk and its elements are still valid and consistent with business objectives, strategies and policies, and that changes to the business context are taken into consideration adequately during the information security risk management process. This monitoring and review activity should address (but not be limited to):

- Legal and environmental context
- Competition context
- Risk assessment approach
- Asset value and categories
- Impact criteria
- Risk evaluation criteria
- Risk acceptance criteria
- Total cost of ownership
- Necessary resources

The organization should ensure that risk assessment and risk treatment resources are continually available to review risk, to address new or changed threats or vulnerabilities, and to advise management accordingly.

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Risk management monitoring can result in modifying or adding the approach, methodology or tools used depending on:

- Changes identified
- Risk assessment iteration
- Aim of the information security risk management process (e.g. business continuity, resilience to incidents, compliance)
- Object of the information security risk management process (e.g. organization, business unit, information process, its technical implementation, application, connection to the internet)

Output: Continual relevance of the information security risk management process to the organization's business objectives or updating the process.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex A
(informative)

Defining the scope and boundaries of the information security risk management process

A.1 Study of the organization

Evaluate the organization The study of the organization recalls the characteristic elements defining the identity of an organization. This concerns the purpose, business, missions, values and strategies of this organization. These should be identified together with the elements contributing to their development (e.g. subcontracting).

The difficulty of this activity lies in understanding exactly how the organization is structured. Identifying its real structure will provide an understanding of the role and importance of each division in achieving the organization's objectives.

For example, the fact that the information security manager reports to the top managers rather than IT managers may indicate top managers' involvement in information security.

The organization's main purpose The main purpose of an organization can be defined as the reason why it exists (its field of activity, its market segment, etc.).

Its business The organization's business, defined by the techniques and know-how of its employees, enables it to accomplish its missions. It is specific to the organization's field of activity and often defines its culture.

Its mission The organization achieves its purpose by accomplishing its mission. To identify its missions, the services provided and/or products manufactured should be identified in relation to the end users.

Its values Values are major principles or a well-defined code of conduct applied to the exercise of a business. This may concern the personnel, relations with outside agents (customers, etc.), the quality of products supplied or services provided.

Take the example of an organization whose purpose is public service, whose business is transport and whose missions include transporting children to and from school. Its values may be the punctuality of the service and safety during transport.

Structure of the organization There are different types of structure:

- Divisional structure: each division is placed under the authority of a division manager responsible for the strategic, administrative and operational decisions concerning his unit
- Functional structure: functional authority is exercised on the procedures, the nature of the work and sometimes the decisions or planning (e.g. production, IT, human resources, marketing, etc.)

Remarks:

- A division within an organization with divisional structure may be organised as a functional structure and vice versa
- An organization may be said to have a matrix structure if it has elements of both types of structure
- In any organizational structure the following levels can be distinguished:
    - the decision-making level (definition of strategic orientations);
    - the leadership level (co-ordination and management);
    - the operational level (production and support activities).

© ISO/IEC 2008 All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Organization chart The organization's structure is represented schematically in an organization chart. This representation should highlight the lines of reporting and delegation of authority, but should also include other relationships, which, even if they are not based on any formal authority, are nevertheless lines of information flow.

The organization's strategy This requires a formal expression of the organization's guiding principles. The organization's strategy determines the direction and development needed in order to benefit from the issues at stake and of the major changes it is planning.

A.2 List of the constraints affecting the organization

All the constraints affecting the organization and determining its information security orientation should be taken into account. Their source may be within the organization in which case it has some control over them or outside the organization and therefore generally non-negotiable. Resource constraints (budget, personnel) and emergency constraints are among the most important ones.

The organization sets its objectives (concerning its business, behaviour, etc.) committing it to a certain path, possibly over a long period. It defines what it wants to become and the means that will need to be implemented. In specifying this path, the organization takes into account developments in techniques and know-how, the expressed wishes of users, customers, etc. This objective can be expressed in the form of operating or development strategies with the aim, for example, of cutting operating costs, improving quality of service, etc.

These strategies probably include information and the information system (IS), which assist in their application. Consequently, characteristics concerning the identity, mission and strategies of the organization are fundamental elements in the analysis of the problem since the breach of an information security aspect could result in rethinking these strategic objectives. In addition, it is essential that proposals for information security requirements remain consistent with the rules, uses and means in force in the organization.

The list of constraints includes but is not limited to:

Constraints of a political nature

These may concern government administrations, public institutions or more generally any organization that has to apply government decisions. They are usually decisions concerning strategic or operational orientation made by a government division or decision-making body and should be applied.

For example, the computerization of invoices or administrative documents introduces information security problems.

Constraints of a strategic nature

Constraints can arise from planned or possible changes to the organization's structures or orientation. They are expressed in the organization's strategic or operational plans.

For example, international co-operation in the sharing of sensitive information may necessitate agreements concerning secure exchange.

Territorial constraints

The organization's structure and/or purpose may introduce specific constraints such as the distribution of sites over the entire national territory or abroad.

Examples include postal services, embassies, banks, subsidiaries of a large industrial group, etc.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Constraints arising from the economic and political climate

An organization's operation may be profoundly changed by specific events such as strikes or national and international crises.

For example, some services should be able to continue even during a serious crisis.

Structural constraints

The nature of an organization's structure (divisional, functional or other) may lead to a specific information security policy and security organization adapted to the structure.

For example, an international structure should be able to reconcile security requirements specific to each country.

Functional constraints

Functional constraints arise directly from the organization's general or specific missions.

For example, an organization that operates around the clock should ensure its resources are continuously available.

Constraints concerning personnel

The nature of these constraints varies considerably. They are linked to: level of responsibility, recruitment, qualification, training, security awareness, motivation, availability, etc.

For example, the entire personnel of a defence organization should have authorisation to handle highly confidential information.

Constraints arising from the organization's calendar

These constraints may result from restructuring or setting up new national or international policies imposing certain deadlines.

For example, the creation of a security division.

Constraints related to methods

Methods appropriate to the organization's know-how will need to be imposed for aspects such as project planning, specifications, development and so on.

For example, a typical constraint of this kind is the need to incorporate the organization's legal obligations into the security policy.

Constraints of a cultural nature

In some organizations work habits or the main business have led to a specific “culture” within the organization, one which may be incompatible with the security controls. This culture is the personnel's general reference framework and may be determined by many aspects, including education, instruction, professional experience, experience outside work, opinions, philosophy, beliefs, social status, etc.

Budgetary constraints

The recommended security controls may sometimes have a very high cost. While it is not always appropriate to base security investments on cost-effectiveness, economic justification is generally required by the organization’s financial department.

For example, in the private sector and some public organizations, the total cost of security controls should not exceed the cost of the potential consequences of the risks. Top management should therefore assess and take calculated risks if they want to avoid excessive security costs.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.3 List of the legislative and regulatory references applicable to the organization

The regulatory requirements applicable to the organization should be identified. These may be laws, decrees, specific regulations in the organization's field or internal/external regulations. This also concerns contracts and agreements and more generally any obligations of a legal or regulatory nature.

A.4 List of the constraints affecting the scope

By identifying the constraints it is possible to list those that have an impact on the scope and determine which are nevertheless amenable to action. They are added to, and may possibly amend, the organization's constraints determined above. The following paragraphs present a non-exhaustive list of possible types of constraints.

Constraints arising from pre-existing processes

Application projects are not necessarily developed simultaneously. Some depend on pre-existing processes. Even though a process can be broken down into sub-processes, the process is not necessarily influenced by all the sub-processes of another process.

Technical constraints

Technical constraints, relating to infrastructure, generally arise from installed hardware and software, and rooms or sites housing the processes:

- Files (requirements concerning organization, media management, management of access rules, etc.)
- General architecture (requirements concerning topology (centralised, distributed, client-server), physical architecture, etc.)
- Application software (requirements concerning specific software design, market standards, etc.);
- Package software (requirements concerning standards, level of evaluation, quality, compliance with norms, security, etc.)
- Hardware (requirements concerning standards, quality, compliance with norms, etc.)
- Communication networks (requirements concerning coverage, standards, capacity, reliability, etc.)
- Building infrastructure (requirements concerning civil engineering, construction, high voltages, low voltages, etc.)

Financial constraints

The implementation of security controls is often restricted by the budget that the organization can commit. However, the financial constraint should still to be the last to be considered as the budget allocation for security can be negotiated on the basis of the security study.

Environmental constraints

Environmental constraints arise from the geographical or economic environment in which the processes are implemented: country, climate, natural risks, geographical situation, economic climate, etc.

Time constraints

The time required for implementing security controls should be considered in relation to the ability to upgrade the information system; if the implementation time is very long, the risks for which the control was designed may have changed. Time is a determining factor for selecting solutions and priorities.

Constraints related to methods

Methods appropriate to the organization's know-how should be used for project planning, specifications, development and so on.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Organizational constraints

Various constraints may follow from organizational requirements:

- Operation (requirements concerning lead-times, supply of services, surveillance, monitoring, emergency plans, degraded operation, etc.)
- Maintenance (requirements for incident troubleshooting, preventive actions, rapid correction, etc.)
- Human resources management (requirements concerning operator and user training, qualification for posts such as system administrator or data administrator, etc.)
- Administrative management (requirements concerning responsibilities, etc.)
- Development management (requirements concerning development tools, computer-aided software engineering, acceptance plans, organization to be set up, etc.)
- Management of external relations (requirements concerning organization of third-party relations, contracts, etc.)

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex B
(informative)

Identification and valuation of assets and impact assessment

B.1 Examples of asset identification

To perform asset valuation, an organization first needs to identify its assets (at an appropriate level of detail). Two kinds of assets can be distinguished:

- The primary assets:
  - Business processes & activities
  - Information

- The supporting assets (on which the primary elements of the scope rely) of all types:
  - Hardware
  - Software
  - Network
  - Personnel
  - Site
  - Organization's structure

B.1.1 The identification of primary assets

To describe the scope more accurately, this activity consists in identifying the primary assets (business processes and activities, information). This identification is carried out by a mixed work group representative of the process (managers, information systems specialists and users).

The primary assets are usually the core processes and information of the activity in the scope. Other primary assets such as the organization's processes can also be considered, which will be more appropriate for drawing up an information security policy or a business continuity plan. Depending on the purpose, some studies will not require an exhaustive analysis of all the elements making up the scope. In such cases, the study boundaries can be limited to the key elements of the scope.

Primary assets are of two types:

1 - Business processes (or sub-processes) and activities, for example:

- Processes whose loss or degradation make it impossible to carry out the mission of the organization
- Processes that contain secret processes or processes involving proprietary technology
- Processes that, if modified, can greatly affect the accomplishment of the organization's mission
- Processes that are necessary for the organization to comply with contractual, legal or regulatory requirements

2 – Information:

More generally, primary information mainly comprises:

- Vital information for the exercise of the organization's mission or business
- Personal information, as can be defined specifically in the sense of the national laws regarding privacy
- Strategic information required for achieving objectives determined by the strategic orientations
- High-cost information whose gathering, storage, processing and transmission require a long time and/or involve a high acquisition cost

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Processes and information that are not identified as sensitive after this activity will have no defined classification in the remainder of the study. This means that even if such processes or information are compromised, the organization will still accomplish the mission successfully.

However, they will often inherit controls implemented to protect the processes and information identified as sensitive.

B.1.2 List and description of supporting assets

The scope consists of assets that should be identified and described. These assets have vulnerabilities that are exploitable by threats aiming to impair the primary assets of the scope (processes and information). They are of various types:

Hardware

The hardware type consists of all the physical elements supporting processes.

Data processing equipment (active)

Automatic information processing equipment including the items required to operate independently.

Transportable equipment

Portable computer equipment.

Examples: laptop computer, Personal Digital Assistant (PDA).

Fixed equipment

Computer equipment used on the organization's premises.

Examples: server, microcomputer used as a workstation.

Processing peripherals

Equipment connected to a computer via a communication port (serial, parallel link, etc.) for entering, conveying or transmitting data.

Examples: printer, removable disc drive.

Data medium (passive)

These are media for storing data or functions.

Electronic medium

An information medium that can be connected to a computer or computer network for data storage. Despite their compact size, these media may contain a large amount of data. They can be used with standard computing equipment.

Examples: floppy disc, CD ROM, back-up cartridge, removable hard disc, memory key, tape.

Other media

Static, non-electronic media containing data.

Examples: paper, slide, transparency, documentation, fax.

Software

Software consists of all the programmes contributing to the operation of a data processing set.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Operating system

This includes all the programmes of a computer making up the operational base from which all the other programmes (services or applications) are run. It includes a kernel and basic functions or services. Depending on the architecture, an operating system may be monolithic or made up of a micro-kernel and a set of system services. The main elements of the operating system are all the equipment management services (CPU, memory, disc, and network interfaces), task or process management services and user rights management services.

Service, maintenance or administration software

Software characterised by the fact that it complements the operating system services and is not directly at the service of the users or applications (even though it is usually essential or even indispensable for the global operation of the information system).

Package software or standard software

Standard software or package software are complete products commercialised as such (rather than one-off or specific developments) with medium, release and maintenance. They provide services for users and applications, but are not personalised or specific in the way that business applications are.

Examples: data base management software, electronic messaging software, groupware, directory software, web server software, etc.

Business application

Standard business application

This is commercial software designed to give users direct access to the services and functions they require from their information system in their professional context. There is a very wide, theoretically limitless, range of fields.

Examples: accounts software, machine tool control software, customer care software, personnel competency management software, administrative software, etc.

Specific business application

This is software in which various aspects (primarily support, maintenance, upgrading, etc.) have been specifically developed to give users direct access to the services and functions they require from their information system. There is a very wide, theoretically unlimited, range of fields.

Examples: Invoice management of telecom operators' customers, real time monitoring application for rocket launching.

Network

The network type consists of all telecommunications devices used to interconnect several physically remote computers or elements of an information system.

Medium and supports

Communications and telecommunications media or equipment are characterised mainly by the physical and technical characteristics of the equipment (point-to-point, broadcast) and by the communication protocols (link or network - levels 2 and 3 of the OSI 7-layer model).

Examples: Public Switching Telephone Network (PSTN), Ethernet, GigabitEthernet, Asymmetric Digital Subscriber Line (ADSL), wireless protocol specifications (e.g. WiFi 802.11), Bluetooth, FireWire.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Passive or active relay

This sub-type includes all devices that are not the logical terminations of communications (IS vision) but are intermediate or relay devices. Relays are characterised by the supported network communication protocols. In addition to the basic relay, they often include routing and/or filtering functions and services, employing communication switches and routers with filters. They can often be administrated remotely and are usually capable of generating logs.

Examples: bridge, router, hub, switch, automatic exchange.

Communication interface

The communication interfaces of the processing units are connected to the processing units but are characterised by the media and supported protocols, by any installed filtering, log or warning generation functions and their capacities and by the possibility and requirement of remote administration.

Examples: General Packet Radio Service (GPRS), Ethernet adaptor.

Personnel

The personnel type consists of all the groups of people involved in the information system.

Decision maker

Decision makers are the owners of the primary assets (information and functions) and the managers of the organization or specific project.

Examples: top management, project leader.

Users

Users are the personnel who handle sensitive elements in the context of their activity and who have a special responsibility in this respect. They may have special access rights to the information system to carry out their everyday tasks.

Examples: human resources management, financial management, risk manager.

Operation/ Maintenance staff

These are the personnel in charge of operating and maintaining the information system. They have special access rights to the information system to carry out their everyday tasks.

Examples: system administrator, data administrator, back-up, Help Desk, application deployment operator, security officers.

Developers

Developers are in charge of developing the organization's applications. They have access to part of the information system with high-level rights but do not take any action on the production data.

Examples: business application developers.

Site

The site type comprises all the places containing the scope or part of the scope, and the physical means required for it to operate.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Location

External environment

This concerns all locations in which the organization's means of security cannot be applied.

Examples: homes of the personnel, premises of another organization, environment outside the site (urban area, hazard area).

Premises

This place is bounded by the organization's perimeter directly in contact with the outside. This may be a physical protective boundary obtained by creating physical barriers or means of surveillance around buildings.

Examples: establishment, buildings.

Zone

A zone is formed by a physical protective boundary forming partitions within the organization's premises. It is obtained by creating physical barriers around the organization's information processing infrastructures.

Examples: offices, reserved access zone, secure zone.

Essential services

All the services required for the organization's equipment to operate.

Communication

Telecommunications services and equipment provided by an operator.

Examples: telephone line, PABX, internal telephone networks.

Utilities

Services and means (sources and wiring) required for providing power to information technology equipment and peripherals.

Examples: low voltage power supply, inverter, electrical circuit head-end.

Water supply

Waste disposal

Services and means (equipment, control) for cooling and purifying the air.

Examples: chilled water pipes, air-conditioners.

Organization

The organization type describes the organizational framework, consisting of all the personnel structures assigned to a task and the procedures controlling these structures.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Authorities

These are organizations from which the studied organization derives its authority. They may be legally affiliated or external. This imposes constraints on the studied organization in terms of regulations, decisions and actions.

Examples: administrating body, Head office of an organization.

Structure of the organization

This consists of the various branches of the organization, including its cross-functional activities, under the control of its management.

Examples: human resources management, IT management, purchasing management, business unit management, building safety service, fire service, audit management.

Project or system organization

This concerns the organization set up for a specific project or service.

Examples: new application development project, information system migration project.

Subcontractors / Suppliers / Manufacturers

These are organizations that provide the organization with a service or resources and bound to it by contract.

Examples: facilities management company, outsourcing company, consultancy companies.

B.2 Asset valuation

The next step after asset identification is to agree upon the scale to be used and the criteria for assigning a particular location on that scale to each asset, based on valuation. Because of the diversity of assets found within most organizations it is likely that some assets that have a known monetary value will be valued in the local unit of currency while others which have a more qualitative value may be assigned a value ranging, for example, from ”very low” to ”very high”. The decision to use a quantitative scale versus a qualitative scale is really a matter of organizational preference, but should be relevant to the assets being valued. Both valuation types could be used for the same asset.

Typical terms used for the qualitative valuation of assets include words such as: negligible, very low, low, medium, high, very high, and critical. The choice and range of terms suitable to an organization is strongly dependent on an organization's needs for security, organizational size, and other organization specific factors.

Criteria

The criteria used as the basis for assigning a value to each asset should be written out in unambiguous terms. This is often one of the most difficult aspects of asset valuation since the values of some assets may have to be subjectively determined and since many different individuals are likely to be making the determination. Possible criteria used to determine an asset’s value include its original cost, its replacement or re-creation cost or its value may be abstract, e.g. the value of an organization’s reputation.

Another basis for the valuation of assets is the costs incurred due to the loss of confidentiality, integrity and availability as the result of an incident. Non-repudiation, accountability, authenticity and reliability should also be considered, as appropriate. Such a valuation would provide the important element dimensions to asset value, in addition to replacement cost, based on estimates of the adverse business consequences that would result from security incidents with an assumed set of circumstances. It is emphasized that this approach accounts for consequences that are necessary to factor into the risk assessment.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Many assets may during the course of valuation have several values assigned. For example: a business plan may be valued based on the labour expended to develop the plan, it might be valued on the labour to input the data, and it could be valued based on its value to a competitor. Each of the assigned values will most likely differ considerably. The assigned value may be the maximum of all possible values or may be the sum of some or all of the possible values. In the final analysis, which value or values are assigned to an asset should be carefully determined since the final value assigned enters into the determination of the resources to be expended for the protection of the asset.

Reduction to the common base

Ultimately, all asset valuations need to be reduced to a common base. This may be done with the aid of criteria such as those that follow. Criteria that may be used to assess the possible consequences resulting from a loss of confidentiality, integrity, availability, non-repudiation, accountability, authenticity, or reliability of assets are:

- Violation of legislation and/or regulation
- Impairment of business performance
- Loss of goodwill/negative effect on reputation
- Breach associated with personal information
- Endangerment of personal safety
- Adverse effects on law enforcement
- Breach of confidentiality
- Breach of public order
- Financial loss
- Disruption to business activities
- Endangerment of environmental safety

Another approach to assess the consequences could be:

- Interruption of service
    - inability to provide the service
- Loss of customer confidence
    - loss of credibility in the internal information system
    - damage to reputation
- Disruption of internal operation
    - disruption in the organization itself
    - additional internal cost
- Disruption of a third party's operation:
    - disruption in third parties transacting with the organization
    - various types of injury
- Infringement of laws / regulations:
    - inability to fulfill legal obligations
- Breach of contract:
    - inability to fulfill contractual obligations
- Danger to personnel / user safety:
    - danger for the organization's personnel and / or users
- Attack on users' private life
- Financial losses
- Financial costs for emergency or repair:
    - in terms of personnel,
    - in terms of equipment,
    - in terms of studies, experts' reports
- Loss of goods / funds / assets
- Loss of customers, loss of suppliers
- Judicial proceedings and penalties
- Loss of a competitive advantage
- Loss of technological / technical lead
- Loss of effectiveness / trust
- Loss of technical reputation
- Weakening of negotiating capacity

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

- Industrial crisis (strikes)
- Government crisis
- Dismissal
- Material damage

These criteria are examples of issues to be considered for asset valuation. For carrying out valuations, an organization needs to select criteria relevant to its type of business and security requirements. This might mean that some of the criteria listed above are not applicable, and that others might need to be added to the list.

Scale

After establishing the criteria to be considered, the organization should agree on a scale to be used organization-wide. The first step is to decide on the number of levels to be used. There are no rules with regard to the number of levels that are most appropriate. More levels provide a greater level of granularity but sometimes a too fine differentiation makes consistent assignments throughout the organization difficult. Normally, any number of levels between 3 (e.g. low, medium, and high) and 10 can be used as long as it is consistent with the approach the organization is using for the whole risk assessment process.

An organization may define its own limits for asset values, like “low”, “medium”, or “high”. These limits should be assessed according to the criteria selected (e.g. for possible financial loss, they should be given in monetary values, but for considerations such as endangerment of personal safety, monetary valuation can be complex and may not be appropriate for all organizations). Finally, it is entirely up to the organization to decide what is considered as being “low” or a “high” consequence. A consequence that might be disastrous for a small organization could be low or even negligible for a very large organization.

Dependencies

The more relevant and numerous the business processes supported by an asset, the greater the value of this asset. Dependencies of assets on business processes and other assets should be identified as well since this might influence the values of the assets. For example, the confidentiality of data should be kept throughout its life-cycle, at all stages, including storage and processing, i.e. the security needs of data storage and processing programmes should be directly related to the value representing the confidentiality of the data stored and processed. Also, if a business process is relying on the integrity of certain data being produced by a programme, the input data of this programme should be of appropriate reliability. Moreover, the integrity of information will be dependent on the hardware and software used for its storage and processing. Also, the hardware will be dependent on the power supply and possibly air conditioning. Thus information about dependencies will assist in the identification of threats and particularly vulnerabilities. Additionally, it will help to assure that the true value of the assets (through the dependency relationships) is given to the assets, thereby indicating the appropriate level of protection.

The values of assets on which other assets are dependent may be modified in the following way:

- If the values of the dependent assets (e.g. data) are lower or equal to the value of the asset considered (e.g. software), its value remains the same

- If the values of the dependent asset (e.g. data) is greater, then the value of the asset considered (e.g. software) should be increased according to:

    - The degree of dependency
    - The values of the other assets

An organization may have some assets that are available more than once, like copies of software programmes or the same type of computer used in most of the offices. It is important to consider this fact when doing the asset valuation. On one hand, these assets are overlooked easily, therefore care should be taken to identify all of them; on the other hand, they could be used to reduce availability problems.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Output

The final output of this step is a list of assets and their values relative to disclosure (preservation of confidentiality), modification (preservation of integrity, authenticity, non-repudiation and accountability), non-availability and destruction (preservation of availability and reliability), and replacement cost.

B.3 Impact assessment

An information security incident can impact more than one asset or only a part of an asset. Impact is related to the degree of success of the incident. As a consequence, there is an important difference between the asset value and the impact resulting from the incident. Impact is considered as having either an immediate (operational) effect or a future (business) effect that includes financial and market consequences.

Immediate (operational) impact is either direct or indirect.

Direct:

a) The financial replacement value of lost (part of) asset

b) The cost of acquisition, configuration and installation of the new asset or back-up

c) The cost of suspended operations due to the incident until the service provided by the asset(s) is restored

d) Impact results in a information security breach

Indirect:

a) Opportunity cost (financial resources needed to replace or repair an asset would have been used elsewhere)

b) The cost of interrupted operations

c) Potential misuse of information obtained through a security breach

d) Violation of statutory or regulatory obligations

e) Violation of ethical codes of conduct

As such, the first assessment (with no controls of any kind) will estimate an impact as very close to the (combination of the) concerned asset value(s). For any next iteration for this (these) asset(s), the impact will be different (normally much lower) due to the presence and the effectiveness of the implemented controls.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex C
(informative)

Examples of typical threats

The following table gives examples of typical threats. The list can be used during the threat assessment process. Threats may be deliberate, accidental or environmental (natural) and may result, for example, in damage or loss of essential services. The following list indicates for each threat type where D (deliberate), A (accidental), E (environmental) is relevant. D is used for all deliberate actions aimed at information assets, A is used for all human actions that can accidentally damage information assets, and E is used for all incidents that are not based on human actions. The groups of threats are not in priority order.

Type	Threats	Origin
Physical damage	Fire	A, D, E
	Water damage	A, D, E
	Pollution	A, D, E
	Major accident	A, D, E
	Destruction of equipment or media	A, D, E
	Dust, corrosion, freezing	A, D, E
Natural events	Climatic phenomenon	E
	Seismic phenomenon	E
	Volcanic phenomenon	E
	Meteorological phenomenon	E
	Flood	E
Loss of essential services	Failure of air-conditioning or water supply system	A, D
	Loss of power supply	A, D, E
	Failure of telecommunication equipment	A, D
Disturbance due to radiation	Electromagnetic radiation	A, D, E
	Thermal radiation	A, D, E
	Electromagnetic pulses	A, D, E
Compromise of information	Interception of compromising interference signals	D
	Remote spying	D
	Eavesdropping	D
	Theft of media or documents	D
	Theft of equipment	D
	Retrieval of recycled or discarded media	D
	Disclosure	A, D
	Data from untrustworthy sources	A, D
	Tampering with hardware	D
	Tampering with software	A, D
	Position detection	D

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Type	Threats	Origin
Technical failures	Equipment failure	A
	Equipment malfunction	A
	Saturation of the information system	A, D
	Software malfunction	A
	Breach of information system maintainability	A, D
Unauthorised actions	Unauthorised use of equipment	D
	Fraudulent copying of software	D
	Use of counterfeit or copied software	A, D
	Corruption of data	D
	Illegal processing of data	D
Compromise of functions	Error in use	A
	Abuse of rights	A, D
	Forging of rights	D
	Denial of actions	D
	Breach of personnel availability	A, D, E

Particular attention should be paid to human threat sources. These are specifically itemized in the following table:

Origin of threat	Motivation	Possible consequences
Hacker, cracker	Challenge Ego Rebellion Status Money	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	• Computer crime (e.g. cyber stalking) • Fraudulent act (e.g. replay, impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge Political Gain Media Coverage	• Bomb/Terrorism • Information warfare • System attack (e.g. distributed denial of service) • System penetration • System tampering

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale
© ISO/IEC 2008 – All rights reserved

Origin of threat	Motivation	Possible consequences
Industrial espionage (Intelligence, companies, foreign governments, other government interests)	Competitive advantage Economic espionage	• Defence advantage • Political advantage • Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g. data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g. virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex D
(informative)

Vulnerabilities and methods for vulnerability assessment

D.1 Examples of vulnerabilities

The following table gives examples for vulnerabilities in various security areas, including examples of threats that might exploit these vulnerabilities. The lists can provide help during the assessment of threats and vulnerabilities, to determine relevant incident scenarios. It is emphasized that in some cases other threats may exploit these vulnerabilities as well.

Types	Examples of vulnerabilities	Examples of threats
Hardware	Insufficient maintenance/faulty installation of storage media	Breach of information system maintainability
	Lack of periodic replacement schemes	Destruction of equipment or media
	Susceptibility to humidity, dust, soiling	Dust, corrosion, freezing
	Sensitivity to electromagnetic radiation	Electromagnetic radiation
	Lack of efficient configuration change control	Error in use
	Susceptibility to voltage variations	Loss of power supply
	Susceptibility to temperature variations	Meteorological phenomenon
	Unprotected storage	Theft of media or documents
	Lack of care at disposal	Theft of media or documents
	Uncontrolled copying	Theft of media or documents
Software	No or insufficient software testing	Abuse of rights
	Well-known flaws in the software	Abuse of rights
	No 'logout' when leaving the workstation	Abuse of rights
	Disposal or reuse of storage media without proper erasure	Abuse of rights
	Lack of audit trail	Abuse of rights
	Wrong allocation of access rights	Abuse of rights
	Widely-distributed software	Corruption of data
	Applying application programs to the wrong data in terms of time	Corruption of data
	Complicated user interface	Error in use
	Lack of documentation	Error in use
	Incorrect parameter set up	Error in use
	Incorrect dates	Error in use

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

	Lack of identification and authentication mechanisms like user authentication	Forging of rights
	Unprotected password tables	Forging of rights
	Poor password management	Forging of rights
	Unnecessary services enabled	Illegal processing of data
	Immature or new software	Software malfunction
	Unclear or incomplete specifications for developers	Software malfunction
	Lack of effective change control	Software malfunction
	Uncontrolled downloading and use of software	Tampering with software
	Lack of back-up copies	Tampering with software
	Lack of physical protection of the building, doors and windows	Theft of media or documents
	Failure to produce management reports	Unauthorised use of equipment
Network	Lack of proof of sending or receiving a message	Denial of actions
	Unprotected communication lines	Eavesdropping
	Unprotected sensitive traffic	Eavesdropping
	Poor joint cabling	Failure of telecommunication equipment
	Single point of failure	Failure of telecommunication equipment
	Lack of identification and authentication of sender and receiver	Forging of rights
	Insecure network architecture	Remote spying
	Transfer of passwords in clear	Remote spying
	Inadequate network management (resilience of routing)	Saturation of the information system
	Unprotected public network connections	Unauthorised use of equipment
Personnel	Absence of personnel	Breach of personnel availability
	Inadequate recruitment procedures	Destruction of equipment or media
	Insufficient security training	Error in use
	Incorrect use of software and hardware	Error in use
	Lack of security awareness	Error in use
	Lack of monitoring mechanisms	Illegal processing of data
	Unsupervised work by outside or cleaning staff	Theft of media or documents
	Lack of policies for the correct use of telecommunications media and messaging	Unauthorised use of equipment

© ISO/IEC 2008 All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Site	Inadequate or careless use of physical access control to buildings and rooms	Destruction of equipment or media
	Location in an area susceptible to flood	Flood
	Unstable power grid	Loss of power supply
	Lack of physical protection of the building, doors and windows	Theft of equipment
Organization	Lack of formal procedure for user registration and de-registration	Abuse of rights
	Lack of formal process for access right review (supervision)	Abuse of rights
	Lack or insufficient provisions (concerning security) in contracts with customers and/or third parties	Abuse of rights
	Lack of procedure of monitoring of information processing facilities	Abuse of rights
	Lack of regular audits (supervision)	Abuse of rights
	Lack of procedures of risk identification and assessment	Abuse of rights
	Lack of fault reports recorded in administrator and operator logs	Abuse of rights
	Inadequate service maintenance response	Breach of information system maintainability
	Lack or insufficient Service Level Agreement	Breach of information system maintainability
	Lack of change control procedure	Breach of information system maintainability
	Lack of formal procedure for ISMS documentation control	Corruption of data
	Lack of formal procedure for ISMS record supervision	Corruption of data
	Lack of formal process for authorization of public available information	Data from untrustworthy sources
	Lack of proper allocation of information security responsibilities	Denial of actions
	Lack of continuity plans	Equipment failure
	Lack of e-mail usage policy	Error in use
	Lack of procedures for introducing software into operational systems	Error in use
	Lack of records in administrator and operator logs	Error in use
	Lack of procedures for classified information handling	Error in use
	Lack of information security responsibilities in job descriptions	Error in use

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

	Lack or insufficient provisions (concerning information security) in contracts with employees	Illegal processing of data
	Lack of defined disciplinary process in case of information security incident	Theft of equipment
	Lack of formal policy on mobile computer usage	Theft of equipment
	Lack of control of off-premise assets	Theft of equipment
	Lack or insufficient 'clear desk and clear screen' policy	Theft of media or documents
	Lack of information processing facilities authorization	Theft of media or documents
	Lack of established monitoring mechanisms for security breaches	Theft of media or documents
	Lack of regular management reviews	Unauthorised use of equipment
	Lack of procedures for reporting security weaknesses	Unauthorised use of equipment
	Lack of procedures of provisions compliance with intellectual rights	Use of counterfeit or copied software

D.2 Methods for assessment of technical vulnerabilities

Proactive methods such as information system testing can be used to identify vulnerabilities depending on the criticality of the Information and Communications Technology (ICT) system and available resources (e.g. allocated funds, available technology, persons with the expertise to conduct the test). Test methods include:

- Automated vulnerability scanning tool
- Security testing and evaluation
- Penetration testing
- Code review

The automated vulnerability scanning tool is used to scan a group of hosts or a network for known vulnerable services (e.g. system allows anonymous File Transfer Protocol (FTP), sendmail relaying). It should be noted, however, that some of the potential vulnerabilities identified by the automated scanning tool may not represent real vulnerabilities in the context of the system environment. For example, some of these scanning tools rate potential vulnerabilities without considering the site's environment and requirements. Some of the vulnerabilities flagged by the automated scanning software may actually not be vulnerable for a particular site but may be configured that way because their environment requires it. Thus, this test method may produce false positives.

Security testing and evaluation (STE) is another technique that can be used in identifying ICT system vulnerabilities during the risk assessment process. It includes the development and execution of a test plan (e.g. test script, test procedures, and expected test results). The purpose of system security testing is to test the effectiveness of the security controls of an ICT system as they have been applied in an operational environment. The objective is to ensure that the applied controls meet the approved security specification for the software and hardware and implement the organization's security policy or meet industry standards.

© ISO/IEC 2008 All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Penetration testing can be used to complement the review of security controls and ensure that different facets of the ICT system are secured. Penetration testing, when used in the risk assessment process, can be used to assess an ICT system's ability to withstand intentional attempts to circumvent system security. Its objective is to test the ICT system from the viewpoint of a threat source and to identify potential failures in the ICT system protection schemes.

Code review is the most thorough (but also most expensive) way of vulnerability assessment.

The results of these types of security testing will help identify a system's vulnerabilities.

It is important to note that penetration tools and techniques can give false results unless the vulnerability is successfully exploited. To exploit particular vulnerabilities one needs to know the exact system/ application/ patches setup on tested system. If those data are not known at the time of testing, it might not be possible to successfully exploit particular vulnerability (for example, gaining remote reverse shell); however, it is still possible to crash or restart a tested process or system. In such a case, the tested object should be considered vulnerable as well.

Methods may include the following activities:

- Interview people and users
- Questionnaires
- Physical inspection
- Document analysis

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex E
(informative)

Information security risk assessment approaches

E.1 High-level information security risk assessment

The high-level assessment allows definition of the priorities and chronology in the actions. For various reasons, such as budget, it may not be possible to implement all controls simultaneously and only the most critical risks can be addressed through the risk treatment process. As well, it can be premature to begin detailed risk management if implementation is only envisaged after one or two years. To reach this objective, the high-level assessment may begin with a high-level assessment of consequences instead of starting with a systematic analysis of threats, vulnerabilities, assets and consequences.

Another reason to start with the high-level assessment is to synchronize with other plans related to change management (or business continuity). For example, it is not sound to completely secure a system or application if it is planned to outsource it in the near future, although it may still be worth doing the risk assessment in order to define the outsource contract.

Features of the high-level risk assessment iteration may include the following:

- The high-level risk assessment may address a more global view of the organization and its information systems, considering the technology aspects as independent from the business issues. By doing this, the context analysis concentrates more on the business and operational environment than technological elements.
- The high-level risk assessment may address a more limited list of threats, and vulnerabilities grouped in defined domains or, to expedite the process, it may focus on risk or attack scenarios instead of their elements.
- Risks presented in a high-level risk assessment are frequently more general risk domains than specific identified risks. As the scenarios or the threats are grouped in domains, the risk treatment proposes lists of controls in this domain. The risk treatment activities try then first to propose and select common controls that are valid across the whole system.
- However, the high-level risk assessment, because it seldom addresses technology details, is more appropriate to provide organizational and non-technical controls and management aspects of technical controls, or key and common technical safeguards such as back-ups and anti-virus.

The advantages of a high-level risk assessment are as follows:

- The incorporation of an initial simple approach is likely to gain acceptance of the risk assessment program.
- It should be possible to build a strategic picture of an organizational information security program, i.e. it will act as a good planning aid.
- Resources and money can be applied where they are most beneficial, and systems likely to be in the greatest need of protection will be addressed first.

As the initial risk analyses are at a high level, and potentially less accurate, the only potential disadvantage is that some business processes or systems may not be identified as requiring a second, detailed risk assessment. This can be avoided if there is adequate information on all aspects of the organization and its information and systems, including information gained from the evaluation of information security incidents.

The high-level risk assessment considers the business values of the information assets, and the risks from the organization's business point of view. At the first decision point (see Figure 1), several factors assist in determining whether the high-level assessment is adequate to treat risks; these factors may include the following:

- The business objectives to be achieved by using various information assets;

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

- The degree to which the organization's business depends on each information asset, i.e. whether functions that the organization considers critical to its survival or the effective conduct of business are dependent on each asset, or on the confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability of the information stored and processed on this asset;
- The level of investment in each information asset, in terms of developing, maintaining, or replacing the asset, and
- The information assets, for which the organization directly assigns value.

When these factors are assessed, the decision becomes easier. If the objectives of an asset are extremely important to an organization's conduct of business, or if the assets are at high risk, then a second iteration, the detailed risk assessment, should be conducted for the particular information asset (or part thereof).

A general rule to apply is: if the lack of information security can result in significant adverse consequences to an organization, its business processes or its assets, then a second iteration risk assessment, at more detailed level, is necessary to identify potential risks.

E.2 Detailed information security risk assessment

The detailed information security risk assessment process involves in-depth identification and valuation of assets, the assessment of threats to those assets, and assessment of vulnerabilities. The results from these activities are then used to assess the risks and then identify risk treatment.

The detailed step usually requires considerable time, effort and expertise, and may therefore be most suitable for information systems at high risk.

The final stage of the detailed information security risk assessment is to assess the overall risks, which is the focus of this annex.

Consequences may be assessed in several ways, including using quantitative, e.g. monetary, and qualitative measures (which can be based on the use of adjectives such as moderate or severe), or a combination of both. To assess the likelihood of threat occurrence, the time frame over which the asset will have value or needs to be protected should be established. The likelihood of a specific threat occurring is affected by the following:

- The attractiveness of the asset, or possible impact applicable when a deliberate human threat is being considered
- The ease of conversion exploiting a vulnerability of the asset into reward, applicable if a deliberate human threat is being considered
- The technical capabilities of the threat agent, applicable to deliberate human threats, and
- The susceptibility of the vulnerability to exploitation, applicable to both technical and non-technical vulnerabilities

Many methods make use of tables, and combine subjective and empirical measures. It is important that the organization uses a method with which the organization is comfortable, in which the organization has confidence, and that will produce repeatable results. A few examples of table-based techniques are given below.

E.2.1 Example 1 Matrix with predefined values

In risk assessment methods of this type, actual or proposed physical assets are valued in terms of replacement or reconstruction costs (i.e. quantitative measurements). These costs are then converted onto the same qualitative scale as that used for information (see below). Actual or proposed software assets are valued in the same way as physical assets, with purchase or reconstruction costs identified and then converted to the same qualitative scale as that used for information. Additionally, if any application software is found to have its own intrinsic requirements for confidentiality or integrity (for example if source code is itself commercially sensitive), it is valued in the same way as for information.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The values for information are obtained by interviewing selected business management (the “data owners”) who can speak authoritatively about the data, to determine the value and sensitivity of the data actually in use, or to be stored, processed or accessed. The interviews facilitate assessment of the value and sensitivity of the information in terms of the worst case scenarios that could be reasonably expected to happen from adverse business consequences due to unauthorized disclosure, unauthorized modification, non-availability for varying time periods, and destruction.

The valuation is accomplished using information valuation guidelines, which cover such issues as:

- Personal safety
- Personal information
- Legal and regulatory obligations
- Law enforcement
- Commercial and economic interests
- Financial loss/disruption of activities
- Public order
- Business policy and operations
- Loss of goodwill
- Contract or agreement with a customer

The guidelines facilitate identification of the values on a numeric scale, such as the 0 to 4 scale shown in the example matrix below, thus enabling the recognition of quantitative values where possible and logical, and qualitative values where quantitative values are not possible, e.g. for endangerment of human life.

The next major activity is the completion of pairs of questionnaires for each threat type, for each grouping of assets that a threat type relates to, to enable the assessment of the levels of threats (likelihood of occurrence) and levels of vulnerabilities (ease of exploitation by the threats to cause adverse consequences). Each question answer attracts a score. These scores are accumulated through a knowledge base and compared with ranges. This identifies threat levels on say a high to low scale and vulnerability levels similarly, as shown in the example matrix below, differentiating between the types of consequences as relevant. Information to complete the questionnaires should be gathered from interviews with appropriate technical, personnel and accommodation people, and physical location inspections, and reviews of documentation.

The asset values, and the threat and vulnerability levels, relevant to each type of consequence, are matched in a matrix such as that shown below, to identify for each combination the relevant measure of risk on a scale of 0 to 8. The values are placed in the matrix in a structured manner. An example is given below:

Table E.1 a)

	Likelihood of occurrence – Threat	Low			Medium			High		
	Ease of Exploitation	L	M	H	L	M	H	L	M	H
Asset Value	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

For each asset, the relevant vulnerabilities and their corresponding threats are considered. If there is a vulnerability without a corresponding threat, or a threat without corresponding vulnerability, there is presently no risk (but care should be taken in case this situation changes). Now the appropriate row in the matrix is identified by the asset value, and the appropriate column is identified by the likelihood of the threat occurring and the ease of exploitation. For example, if the asset has the value **3**, the threat is "**high**" and the vulnerability "**low**", the measure of risk is **5**. Assume an asset has a value of 2, e.g. for modification, the threat level is "low" and the ease of exploitation is "high", then the measure of risk is 4. The size of the matrix, in terms of the number of threat likelihood categories, ease of exploitation categories and the number of asset valuation categories, can be adjusted to the needs of the organization. Additional columns and rows will necessitate additional risk measures. The value of this approach is in ranking the risks to be addressed.

A similar Matrix as shown in Table E.1 b) results from the consideration of the likelihood of an incident scenario, mapped against the estimated business impact. The likelihood of an incident scenario is given by a threat exploiting a vulnerability with a certain likelihood. The Table maps this likelihood against the business impact related to the incident scenario. The resulting risk is measured on a scale of 0 to 8 that can be evaluated against risk acceptance criteria. This risk scale could also be mapped to a simple overall risk rating, for example as:

- Low risk: 0-2
- Medium Risk: 3-5
- High Risk:6-8

Table E.1 b)

	Likelihood of incident scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

E.2.2 Example 2 Ranking of Threats by Measures of Risk

A matrix or table such as that shown in Table E.2 can be used to relate the factors of consequences (asset value) and likelihood of threat occurrence (taking account of vulnerability aspects). The first step is to evaluate the consequences (asset value) on a predefined scale, e.g. 1 through 5, of each threatened asset (column "b" in the table). The second step is to evaluate the likelihood of threat occurrence on a predefined scale, e.g. 1 through 5, of each threat (column "c" in the table). The third step is to calculate the measure of risk by multiplying (b $\times$ c). Finally the threats can be ranked in order of their associated measure of risk. Note that in this example, 1 is taken as the lowest consequence and the lowest likelihood of occurrence.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table E.2

Threat descriptor (a)	Consequence (asset) value (b)	Likelihood of threat occurrence (c)	Measure of risk (d)	Threat ranking (e)
Threat A	5	2	10	2
Threat B	2	4	8	3
Threat C	3	5	15	1
Threat D	1	3	3	5
Threat E	4	1	4	4
Threat F	2	4	8	3

As shown above, this is a procedure which permits different threats with differing consequences and likelihood of occurrence to be compared and ranked in order of priority, as shown here. In some instances it will be necessary to associate monetary values with the empirical scales used here.

E.2.3 Example 3 Assessing a value for the likelihood and the possible consequences of risks

In this example, the emphasis is placed on the consequences of information security incidents (i.e. incident scenarios) and on determining which systems should be given priority. This is done by assessing two values for each asset and risk, which in combination will determine the score for each asset. When all the asset scores for the system are summed, a measure of risk to that system is determined.

First, a value is assigned to each asset. This value relates to the potential adverse consequences that can arise if the asset is threatened. For each applicable threat to the asset, this asset value is assigned to the asset.

Next a likelihood value is assessed. This is assessed from a combination of the likelihood of the threat occurring and the ease of exploitation of the vulnerability, see Table E.3 expressing the likelihood of an incident scenario.

Table E.3

Likelihood of Threat	Low			Medium			High		
Levels of Vulnerability	L	M	H	L	M	H	L	M	H
Likelihood Value of an incident scenario	0	1	2	1	2	3	2	3	4

Next, an asset/threat score is assigned by finding the intersection of asset value and likelihood value in Table E.4. The asset/threat scores are totalled to produce an asset total score. This figure can be used to differentiate between the assets forming part of a system.

© ISO/IEC 2008 All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table E.4

Asset Value	0	1	2	3	4
Likelihood Value					
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

The final step is to total all the asset total scores for the assets of the system, producing a system score. This can be used to differentiate between systems and to determine which system's protection should be given priority.

In the following examples all values are randomly chosen.

Suppose System S has three assets A1, A2 and A3. Also suppose there are two threats T1 and T2 applicable to system S. Let the value of A1 be 3, similarly let the asset value of A2 be 2 and the asset value of A3 be 4.

If for A1 and T1 the threat likelihood is low and the ease of exploitation of the vulnerability is medium, then the likelihood value is 1 (see Table E.3).

The asset/threat score A1/T1 can be derived from Table E.4 as the intersection of asset value 3 and likelihood value 1, i.e. 4. Similarly, for A1/T2 let the threat likelihood is medium and the ease of exploitation of vulnerability is high, giving an A1/T2 score of 6.

Now the total asset score A1T can be calculated, i.e. 10. The total asset score is calculated for each asset and applicable threat. The total system score is calculated by adding A1T + A2T + A3T to give ST.

Now different systems can be compared to establish priorities and different assets within one system as well.

Above example shows in terms of information systems, however similar approach can be applied to business processes.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex F
(informative)

Constraints for risk reduction

While considering constraints for risk reduction the following constraints should be taken into account:

Time constraints:

Many types of time constraints can exist. For example, controls should be implemented within a time period acceptable for the organization's managers. Another type of time constraint is whether a control can be implemented within the lifetime of the information or system. A third type of time constraint may be the period of time the organization's managers decides is an acceptable period to be exposed to a particular risk.

Financial constraints:

Controls should not be more expensive to implement or to maintain than the value of risks they are designed to protect, except where compliance is mandatory (e.g. with legislation). Every effort should be made not to exceed assigned budgets and achieve financial advantage through the use of controls. However, in some cases it may not be possible to achieve the desired security and level of risk acceptance due to budget constraints. This therefore becomes an organization's managers' decision for resolution of this situation.

Great care should be taken if the budget reduces the number or quality of controls to be implemented since this can lead to the implicit retention of greater risk than planned. The established budget for controls should only be used as a limiting factor with considerable care.

Technical constraints:

Technical problems, like the compatibility of programmes or hardware, can easily be avoided if they are taken into account during the selection of controls. In addition, the retrospective implementation of controls to an existing process or system is often hindered by technical constraints. These difficulties may move the balance of controls towards the procedural and physical aspects of security. It may be necessary to revise the information security programme in order to achieve security objectives. This can occur when controls do not meet the expected results in reducing risks without lessening productivity.

Operational constraints

Operational constraints such as the need to operate 24x7 yet still perform back-ups can result in complex and costly implementation of controls unless they are built into the design right from the start.

Cultural constraints:

Cultural constraints to the selection of controls may be specific to a country, a sector, an organization or even a department within an organization. Not all controls can be applied in all countries. For example, it may be possible to implement bag searches in parts of Europe but not in parts of the Middle East. Cultural aspects cannot be ignored because many controls rely on the active support of the staff. If the staff does not understand the need for the control or do not find it culturally acceptable, the control will become ineffective over time.

Ethical constraints:

Ethical constraints can have major implications on controls as ethics change based on social norms. This can prevent implementing controls such as email scanning in some countries. Privacy of information can also change dependent on the ethics of the region or government. These may be of more concern in some industry sectors than others, for example, government and healthcare.

© ISO/IEC 2008 All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Environmental constraints:

Environmental factors may influence the selection of controls, such as space availability, extreme climate conditions, surrounding natural and urban geography. For example earthquake proofing may be required in some countries but unnecessary in others.

Legal constraints:

Legal factors such as personal data protection or criminal code provisions for information processing could affect the selection of controls. Legislative and regulatory compliance can mandate certain types of control including data protection and financial audit; they can also prevent the use of some controls, e.g. encryption. Other laws and regulations such as labour relations legislation, fire department, health and safety, and economic sector regulations, etc., could affect control selection as well.

Ease of use:

A poor human-technology interface will result in human error and may render the control useless. Controls should be selected to provide optimal ease of use while achieving an acceptable level of residual risk to the business. Controls that are difficult to use will impact their effectiveness, as users may try to circumvent or ignore them as much as possible. Complex access controls within an organization could encourage users to find alternate, unauthorized methods of access.

Personnel constraints:

The availability and salary cost of specialized skill sets to implement controls, and the ability to move staff between locations in adverse operating conditions, should be considered. Expertise may not be readily available to implement planned controls or the expertise may be overly costly for the organization. Other aspects such as the tendency of some staff to discriminate other staff members who are not security screened can have major implications for security policies and practices. As well, the need to hire the right people for the work, and finding the right people, may result in hiring before security screening is completed. The requirement for security screening to be completed before hiring is the normal, and safest, practice.

Constraints of integrating new and existing controls:

Integration of new controls in the existing infrastructure and the interdependencies between controls are often overlooked. New controls may not easily be implemented if there is incongruity or incompatibility with existing controls. For example, a plan to use biometric tokens for physical access control may cause conflict with an existing PIN-pad based system for access control. The cost of changing controls from existing controls to the planned controls should include elements to be added to the overall costs of risk treatment. It may not be possible to implement a selected control due to interference with current controls.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Bibliography

[1] ISO/IEC Guide 73:2002, *Risk management — Vocabulary — Guidelines for use in standards*

[2] ISO/IEC 16085:2006, *Systems and software engineering — Life cycle processes — Risk management*

[3] AS/NZS 4360:2004, *Risk Management*

[4] NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*

[5] NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology*

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

ICS 35.040

Price based on 55 pages

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale