BS ISO/IEC 27005:2011

BSI Standards Publication

Information technology — Security techniques — Information security risk management

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

raising standards worldwide™

Full document details: BS ISO/IEC 27005:2011

National foreword

This British Standard is the UK implementation of ISO/IEC 27005:2011. It supersedes BS ISO/IEC 27005:2008 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT - Security techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© BSI 2011

ISBN 978 0 580 71714 7

ICS 35.040

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 June 2011.

Amendments issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27005:2011

INTERNATIONAL STANDARD

ISO/IEC 27005

Second edition
2011-06-01

Information technology — Security techniques — Information security risk management

Technologies de l'information — Techniques de sécurité — Gestion des risques liés à la sécurité de l'information

Reference number
ISO/IEC 27005:2011(E)

Documents
Document Sharing Hub

© ISO/IEC 2011

Full document details: BS ISO/IEC 27005:2011

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2011

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

© ISO/IEC 2011 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27005:2011

Contents

Page

Foreword v
Introduction vi
1 Scope 1
2 Normative references 1
3 Terms and definitions 1
4 Structure of this International Standard 5
5 Background 6
6 Overview of the information security risk management process 7
7 Context establishment 10
7.1 General considerations 10
7.2 Basic Criteria 10
7.2.1 Risk management approach 10
7.2.2 Risk evaluation criteria 10
7.2.3 Impact criteria 11
7.2.4 Risk acceptance criteria 11
7.3 Scope and boundaries 12
7.4 Organization for information security risk management 12
8 Information security risk assessment 13
8.1 General description of information security risk assessment 13
8.2 Risk identification 13
8.2.1 Introduction to risk identification 13
8.2.2 Identification of assets 14
8.2.3 Identification of threats 14
8.2.4 Identification of existing controls 15
8.2.5 Identification of vulnerabilities 15
8.2.6 Identification of consequences 16
8.3 Risk analysis 17
8.3.1 Risk analysis methodologies 17
8.3.2 Assessment of consequences 18
8.3.3 Assessment of incident likelihood 18
8.3.4 Level of risk determination 19
8.4 Risk evaluation 19
9 Information security risk treatment 20
9.1 General description of risk treatment 20

Documents
Document Sharing Hub

© ISO/IEC 2011 – All rights reserved

Full document details: BS ISO/IEC 27005:2011

9.2 Risk modification 22
9.3 Risk retention 23
9.4 Risk avoidance 23
9.5 Risk sharing 23
10 Information security risk acceptance 24
11 Information security risk communication and consultation 24
12 Information security risk monitoring and review 25
12.1 Monitoring and review of risk factors 25
12.2 Risk management monitoring, review and improvement 26
Annex A (informative) **Defining the scope and boundaries of the information security risk management process** 28
A.1 Study of the organization 28
A.2 List of the constraints affecting the organization 29
A.3 List of the legislative and regulatory references applicable to the organization 31
A.4 List of the constraints affecting the scope 31
Annex B (informative) **Identification and valuation of assets and impact assessment** 33
B.1 Examples of asset identification 33
B.1.1 The identification of primary assets 33
B.1.2 List and description of supporting assets 34
B.2 Asset valuation 38
B.3 Impact assessment 41
Annex C (informative) **Examples of typical threats** 42
Annex D (informative) **Vulnerabilities and methods for vulnerability assessment** 45
D.1 Examples of vulnerabilities 45
D.2 Methods for assessment of technical vulnerabilities 48
Annex E (informative) **Information security risk assessment approaches** 50
E.1 High-level information security risk assessment 50
E.2 Detailed information security risk assessment 51
E.2.1 Example 1 Matrix with predefined values 52
E.2.2 Example 2 Ranking of Threats by Measures of Risk 54
E.2.3 Example 3 Assessing a value for the likelihood and the possible consequences of risks 54
Annex F (informative) **Constraints for risk modification** 56
Annex G (informative) **Differences in definitions between ISO/IEC 27005:2008 and ISO/IEC 27005:2011** 58
Bibliography 68

© ISO/IEC 2011 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27005:2011

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 second edition cancels and replaces the first edition (ISO/IEC 27005:2008) which has been technically revised.

© ISO/IEC 2011 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27005:2011

Introduction

This International Standard provides guidelines for information security risk management in an organization, supporting in particular the requirements of an information security management (ISMS) according to ISO/IEC 27001. However, this International Standard does not provide any specific method 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 2011 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27005:2011

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 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following apply.

NOTE Differences in definitions between ISO/IEC 27005:2008 and this International Standard are shown in Annex G.

3.1
consequence
outcome of an **event** (3.3) affecting objectives

[ISO Guide 73:2009]

NOTE 1 An event can lead to a range of consequences.

NOTE 2 A consequence can be certain or uncertain and in the context of information security is usually negative.

NOTE 3 Consequences can be expressed qualitatively or quantitatively.

NOTE 4 Initial consequences can escalate through knock-on effects.

© ISO/IEC 2011 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27005:2011

3.2
control
measure that is modifying **risk** (3.9)

[ISO Guide 73:2009]

NOTE 1 Controls for information security include any process, policy, procedure, guideline, practice or organizational structure, which can be administrative, technical, management, or legal in nature which modify information security risk.

NOTE 2 Controls may not always exert the intended or assumed modifying effect.

NOTE 3 Control is also used as a synonym for safeguard or countermeasure.

3.3
event
occurrence or change of a particular set of circumstances

[ISO Guide 73:2009]

NOTE 1 An event can be one or more occurrences, and can have several causes.

NOTE 2 An event can consist of something not happening.

NOTE 3 An event can sometimes be referred to as an “incident” or “accident”.

3.4
external context
external environment in which the organization seeks to achieve its objectives

[ISO Guide 73:2009]

NOTE External context can include:

— the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;

— key drivers and trends having impact on the objectives of the organization; and

— relationships with, and perceptions and values of, external stakeholders.

3.5
internal context
internal environment in which the organization seeks to achieve its objectives

[ISO Guide 73:2009]

NOTE Internal context can include:

— governance, organizational structure, roles and accountabilities;

— policies, objectives, and the strategies that are in place to achieve them;

— the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);

— information systems, information flows and decision-making processes (both formal and informal);

— relationships with, and perceptions and values of, internal stakeholders;

— the organization's culture;

— standards, guidelines and models adopted by the organization; and

— form and extent of contractual relationships.

© ISO/IEC 2011 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27005:2011

3.6
level of risk
magnitude of a **risk** (3.9), expressed in terms of the combination of **consequences** (3.1) and their **likelihood** (3.7)

[ISO Guide 73:2009]

3.7
likelihood
chance of something happening

[ISO Guide 73:2009]

NOTE 1 In risk management terminology, the word "likelihood" is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).

NOTE 2 The English term "likelihood" does not have a direct equivalent in some languages; instead, the equivalent of the term "probability" is often used. However, in English, "probability" is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, "likelihood" is used with the intent that it should have the same broad interpretation as the term "probability" has in many languages other than English.

3.8
residual risk
risk (3.9) remaining after **risk treatment** (3.17)

[ISO Guide 73:2009]

NOTE 1 Residual risk can contain unidentified risk.

NOTE 2 Residual risk can also be known as "retained risk".

3.9
risk
effect of uncertainty on objectives

[ISO Guide 73:2009]

NOTE 1 An effect is a deviation from the expected — positive and/or negative.

NOTE 2 Objectives can have different aspects (such as financial, health and safety, information security, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).

NOTE 3 Risk is often characterized by reference to potential events (3.3) and consequences (3.1), or a combination of these.

NOTE 4 Information security risk is often expressed in terms of a combination of the consequences of an information security event and the associated likelihood (3.9) of occurrence.

NOTE 5 Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

NOTE 6 Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.

3.10
risk analysis
process to comprehend the nature of risk and to determine the **level of risk** (3.6)

[ISO Guide 73:2009]

© ISO/IEC 2011 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27005:2011

NOTE 1 Risk analysis provides the basis for risk evaluation and decisions about risk treatment.

NOTE 2 Risk analysis includes risk estimation.

3.11
risk assessment
overall process of **risk identification** (3.15), **risk analysis** (3.10) and **risk evaluation** (3.14)

[ISO Guide 73:2009]

3.12
risk communication and consultation
continual and iterative processes that an organization conducts to provide, share or obtain information, and to engage in dialogue with **stakeholders** (3.18) regarding the management of **risk** (3.9)

[ISO Guide 73:2009]

NOTE 1 The information can relate to the existence, nature, form, likelihood, significance, evaluation, acceptability and treatment of risk.

NOTE 2 Consultation is a two-way process of informed communication between an organization and its stakeholders on an issue prior to making a decision or determining a direction on that issue. Consultation is:

— a process which impacts on a decision through influence rather than power; and

— an input to decision making, not joint decision making.

3.13
risk criteria
terms of reference against which the significance of a **risk** (3.9) is evaluated

[ISO Guide 73:2009]

NOTE 1 Risk criteria are based on organizational objectives, and external and internal context.

NOTE 2 Risk criteria can be derived from standards, laws, policies and other requirements.

3.14
risk evaluation
process of comparing the results of **risk analysis** (3.10) with **risk criteria** (3.13) to determine whether the risk and/or its magnitude is acceptable or tolerable

[ISO Guide 73:2009]

NOTE Risk evaluation assists in the decision about risk treatment.

3.15
risk identification
process of finding, recognizing and describing risks

[ISO Guide 73:2009]

NOTE 1 Risk identification involves the identification of risk sources, events, their causes and their potential consequences.

NOTE 2 Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholders' needs.

© ISO/IEC 2011 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27005:2011

3.16
risk management
coordinated activities to direct and control an organization with regard to risk

[ISO Guide 73:2009]

NOTE This International Standard uses the term 'process' to describe risk management overall. The elements within the risk management process are termed 'activities'

3.17
risk treatment
process to modify risk

[ISO Guide 73:2009]

NOTE 1 Risk treatment can involve:

— avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
— taking or increasing risk in order to pursue an opportunity;
— removing the risk source;
— changing the likelihood;
— changing the consequences;
— sharing the risk with another party or parties (including contracts and risk financing); and
— retaining the risk by informed choice.

NOTE 2 Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction".

NOTE 3 Risk treatment can create new risks or modify existing risks.

3.18
stakeholder
person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

[ISO Guide 73:2009]

NOTE A decision maker can be a stakeholder.

4 Structure of this International Standard

This International 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,

© ISO/IEC 2011 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27005:2011

- 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. Annex C gives examples of typical threats and Annex D discusses vulnerabilities and methods for vulnerability assessment. Examples of information security risk assessment approaches are presented in Annex E.

Constraints for risk modification are presented in Annex F.

Differences in definitions between ISO/IEC 27005:2008 and ISO/IEC 27005:2011 are shown in Annex G.

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

Information security risk management should contribute to the following:

- Risks being identified
- Risks being assessed in terms of their consequences to the business and the likelihood of their occurrence
- The likelihood and consequences of these risks being communicated and understood
- Priority order for risk treatment being established
- Priority for actions to reduce risks occurring
- Stakeholders being involved when risk management decisions are made and kept informed of the risk management status
- Effectiveness of risk treatment monitoring

© ISO/IEC 2011 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27005:2011

- 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

A high level view of the risk management process is specified in ISO 31000 and shown in Figure 1.

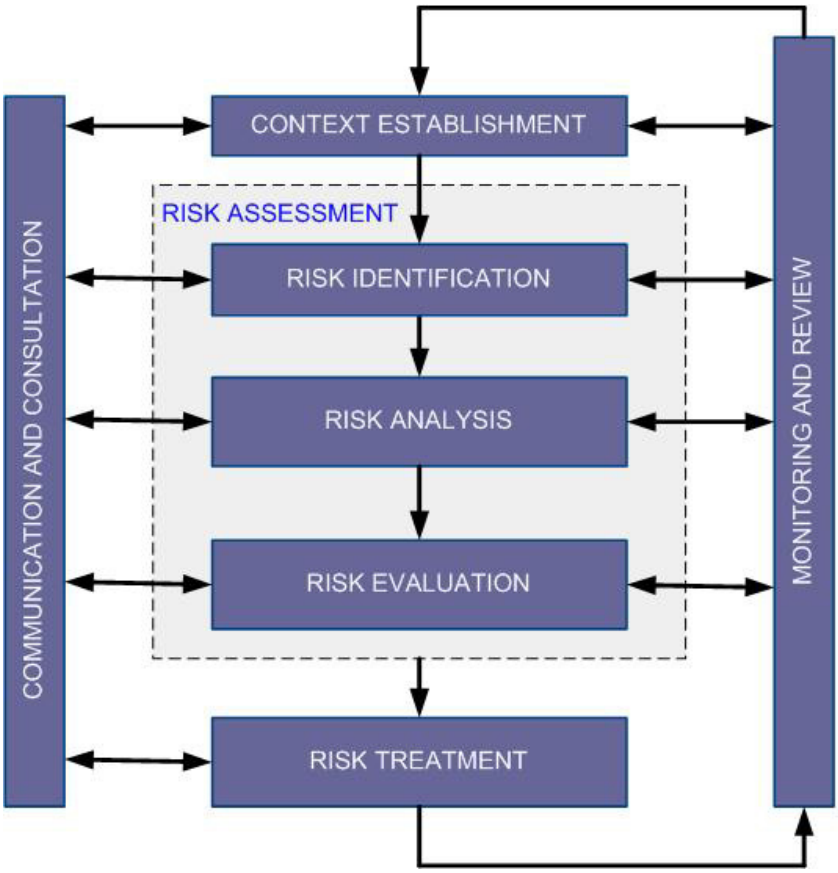

Figure 1 — The risk management process

© ISO/IEC 2011 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27005:2011

Figure 2 shows how this International Standard applies this 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 and consultation (Clause 11), and risk monitoring and review (Clause 12).

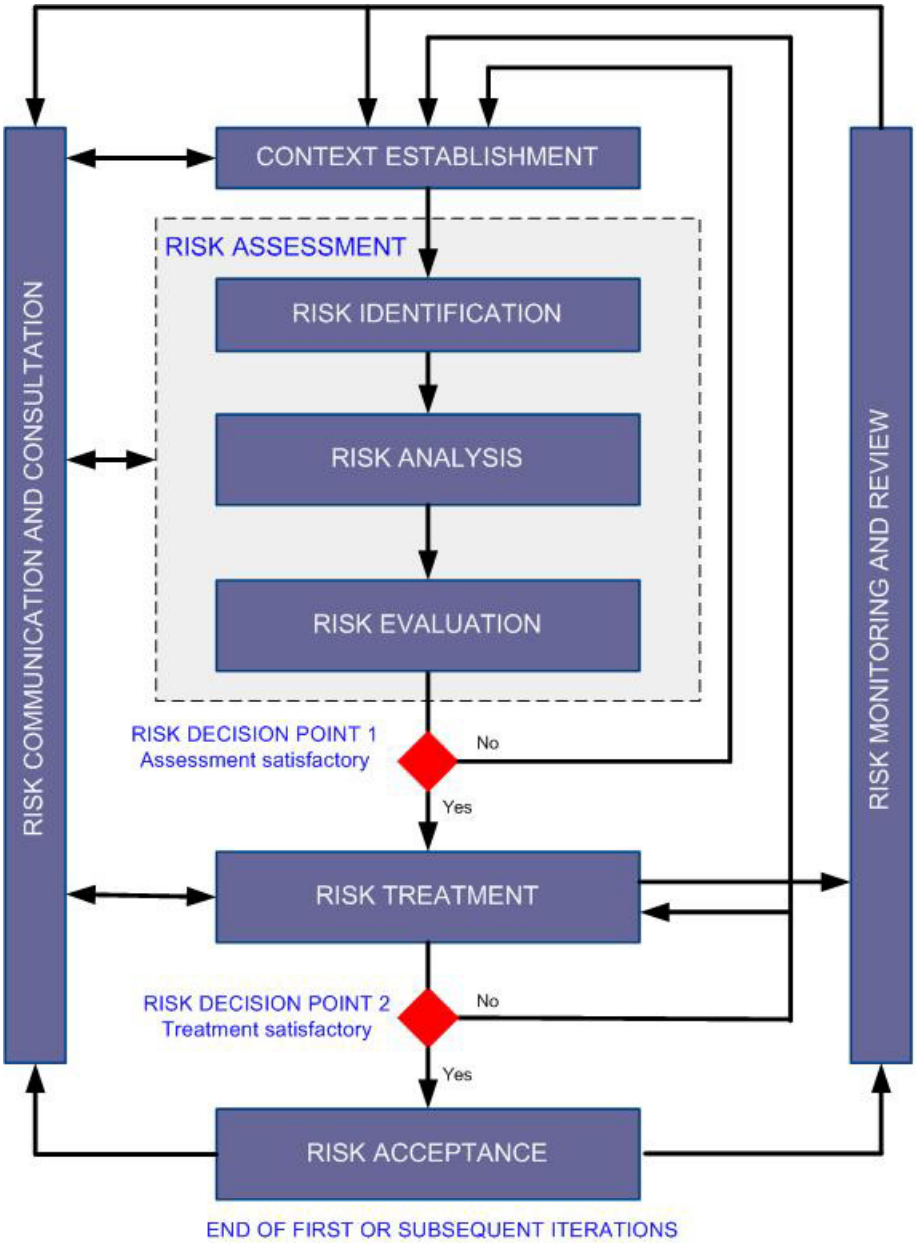

Figure 2 — Illustration of an information security risk management process

As Figure 2 illustrates, the information security risk management process can be iterative for risk assessment and/or risk treatment activities. An iterative approach to conducting risk assessment can increase depth and detail of the assessment at each iteration. The iterative approach provides a good balance between minimizing the time and effort spent in identifying controls, while still ensuring that high risks are appropriately assessed.

The context is established first. Then a risk assessment is conducted. If this provides sufficient information to effectively determine the actions required to modify the risks to an acceptable level then the task is complete and the risk treatment follows. If the information is insufficient, another iteration of the risk assessment with

© ISO/IEC 2011 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27005:2011

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 2, Risk Decision Point 1).

The effectiveness of the risk treatment depends on the results of the risk assessment.

Note that risk treatment involves a cyclical process of:

- assessing a risk treatment;
- deciding whether residual risk levels are acceptable;
- generating a new risk treatment if risk levels are not acceptable; and
- assessing the effectiveness of that treatment

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 2, 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 need to 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 2011 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27005:2011

7 Context establishment

7.1 General considerations

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

Action: The external and internal 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 27001:2005 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 27001:2005.

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

7.2 Basic Criteria

7.2.1 Risk management approach

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 27001:2005 (Clause 5.2.1) concerning the provision of resources for the implementation and operation of an ISMS.

7.2.2 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

© ISO/IEC 2011 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27005:2011

- 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.

7.2.3 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 27001:2005 [Clause 4.2.1 d) 4] concerning the impact criteria identification for losses of confidentiality, integrity and availability.

7.2.4 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 27001:2005 Clause 4.2.1 c) 2).

More information can be found in Annex A.

© ISO/IEC 2011 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27005:2011

7.3 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 27001:2005 Clause 4.2.1 a)] to address those risks that might arise through these boundaries.

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

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

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

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

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

NOTE The scope and boundaries of the information security risk management is related to the scope and boundaries of the ISMS required in ISO/IEC 27001:2005 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 27001:2005 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 27001:2005.

© ISO/IEC 2011 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27005:2011

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 27001:2005.

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.

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 Identification (clause 8.2)
- Risk analysis (clause 8.3)
- Risk evaluation (clause 8.4)

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 identification

8.2.1 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 should collect input data for the risk analysis activity.

Risk identification should include risks whether or not their source is under the control of the organization, even though the risk source or cause may not be evident.

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

© ISO/IEC 2011 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27005:2011

8.2.2 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 27001:2005, 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.

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 8.3.2 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.

8.2.3 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 27001:2005, 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 8.3.3) 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 should also be considered when addressing threats.

© ISO/IEC 2011 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27005:2011

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.

8.2.4 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 audits

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

8.2.5 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 27001:2005, Clause 4.2.1 d) 3)).

© ISO/IEC 2011 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27005:2011

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

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.

8.2.6 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 27001:2005 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 27002:2005, 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 27001:2005 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

© ISO/IEC 2011 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27005:2011