INTERNATIONAL STANDARD

ISO/IEC 27005

Third edition
2018-07

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 27005:2018(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

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

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

This third edition cancels and replaces the second edition (ISO/IEC 27005:2011) which has been technically revised. The main changes from the previous edition are as follows:

— all direct references to the ISO/IEC 27001:2005 have been removed;

— clear information has been added that this document does not contain direct guidance on the implementation of the ISMS requirements specified in ISO/IEC 27001 (see Introduction);

— ISO/IEC 27001:2005 has been removed from Clause 2;

— ISO/IEC 27001 has been added to the Bibliography;

— Annex G and all references to it have been removed;

— editorial changes have been made accordingly.

Introduction

This document provides guidelines for information security risk management in an organization. However, this document 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 an information security management system (ISMS), context of risk management, or industry sector. A number of existing methodologies can be used under the framework described in this document to implement the requirements of an ISMS. This document is based on the asset, threat and vulnerability risk identification method that is no longer required by ISO/IEC 27001. There are some other approaches that can be used.

This document does not contain direct guidance on the implementation of the ISMS requirements given in ISO/IEC 27001.

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

Information technology — Security techniques — Information security risk management

1 Scope

This document provides guidelines for information security risk management.

This document 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 document.

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

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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*

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

4 Structure of this document

This document 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. 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.

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;

— 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.

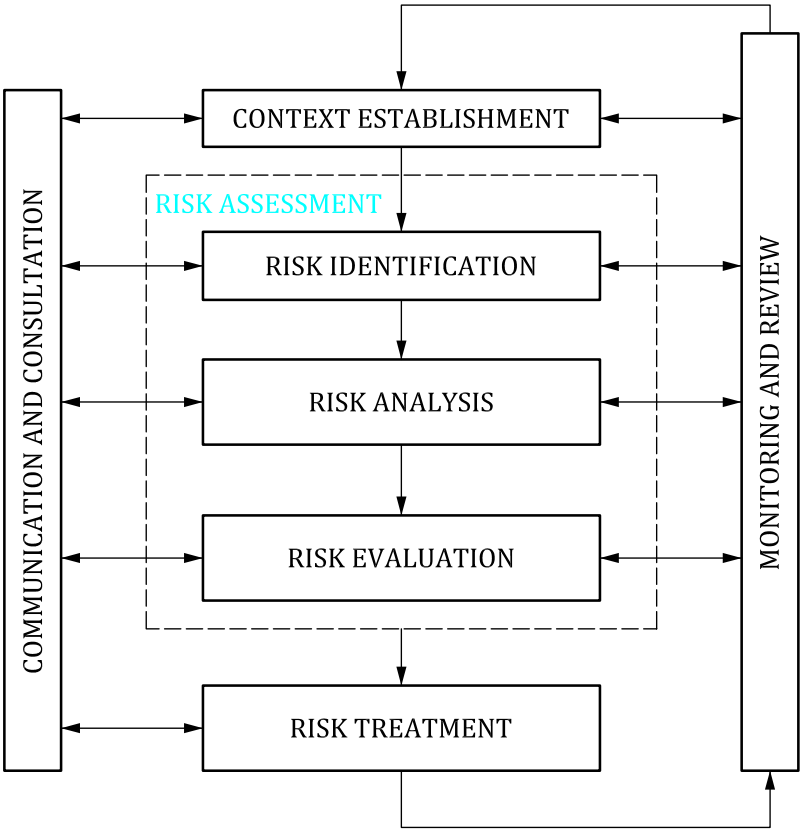

Figure 1 — The risk management process

Figure 2 shows how this document 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).

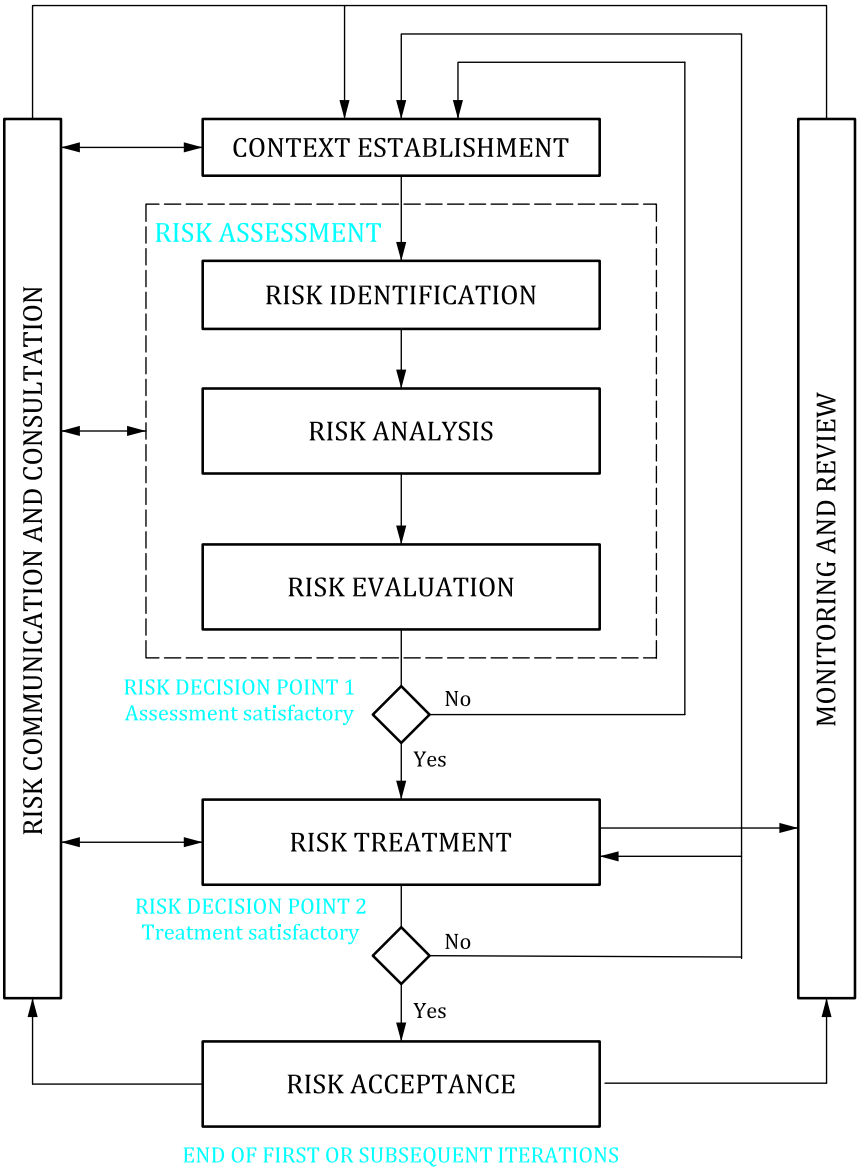

Figure 2 — Illustration of an information security risk management process

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 revised context (e.g. risk evaluation criteria, risk acceptance criteria or impact criteria) is 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 does 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, can 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 can 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 controls can be determined to implement the risk treatment options chosen.

The organization should establish, implement and maintain a procedure to identify the legal requirements applicable to:

— the selection of criteria for risk evaluation (7.2.2), risk impact (7.2.3) and risk acceptance (7.2.4);

— the definition of the scope and boundaries of information security risk management (7.3 and A.2);

— risk evaluation (8.4);

— risk treatment of (9.1) and the implementation of risk reduction plans (9.2 and Annex F);

— the monitoring, review and improvement of risk management (12.2);

— asset identification (B.1.3) and asset valuation (B.2.3); and

— risk estimation (see examples in E.2.1).

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: