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)

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;