INTERNATIONAL STANDARD

ISO/IEC 27005

Fourth edition
2022-10

Information security, cybersecurity and privacy protection — Guidance on managing information security risks

Sécurité de l'information, cybersécurité et protection de la vie privée — Préconisations pour la gestion des risques liés à la sécurité de l'information

Reference number
ISO/IEC 27005:2022(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
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.

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 or www.iec.ch/members_experts/refdocs).

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) or the IEC list of patent declarations received (see https://patents.iec.ch).

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

For an explanation of 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 www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This fourth edition cancels and replaces the third edition (ISO/IEC 27005:2018), which has been technically revised.

The main changes are as follows:

- all guidance text has been aligned with ISO/IEC 27001:2022, and ISO 31000:2018;
- the terminology has been aligned with the terminology in ISO 31000:2018;
- the structure of the clauses has been adjusted to the layout of ISO/IEC 27001:2022;
- risk scenario concepts have been introduced;
- the event-based approach is contrasted with the asset-based approach to risk identification;
- the content of the annexes has been revised and restructured into a single annex.

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 and www.iec.ch/national-committees.

Introduction

This document provides guidance on:

- implementation of the information security risk requirements specified in ISO/IEC 27001;
- essential references within the standards developed by ISO/IEC JTC 1/SC 27 to support information security risk management activities;
- actions that address risks related to information security (see ISO/IEC 27001:2022, 6.1 and Clause 8);
- implementation of risk management guidance in ISO 31000 in the context of information security.

This document contains detailed guidance on risk management and supplements the guidance in ISO/IEC 27003.

This document is intended to be used by:

- organizations that intend to establish and implement an information security management system (ISMS) in accordance with ISO/IEC 27001;
- persons that perform or are involved in information security risk management (e.g. ISMS professionals, risk owners and other interested parties);
- organizations that intend to improve their information security risk management process.

Information security, cybersecurity and privacy protection — Guidance on managing information security risks

1 Scope

This document provides guidance to assist organizations to:

— fulfil the requirements of ISO/IEC 27001 concerning actions to address information security risks;

— perform information security risk management activities, specifically information security risk assessment and treatment.

This document is applicable to all organizations, regardless of type, size or sector.

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*