INTERNATIONAL STANDARD

**ISO/IEC 27013**

Third edition
2021-11

# Information security, cybersecurity and privacy protection — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

*Sécurité de l'information, cybersécurité et protection de la vie privée — Recommandations pour la mise en œuvre intégrée de l'ISO/IEC 27001 et de l'ISO/IEC 20000-1*

Reference number
ISO/IEC 27013:2021(E)

## COPYRIGHT PROTECTED DOCUMENT



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 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 third edition cancels and replaces the second edition (ISO/IEC 27013:2015), which has been technically revised. The main change compared with the previous edition is the alignment with ISO/IEC 20000-1:2018.

A list of all parts in the ISO/IEC 27000 series can be found on the ISO and IEC websites.

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

The relationship between information security management and service management is so close that many organizations already recognize the benefits of adopting the two International Standards for these domains: ISO/IEC 27001 for information security management and ISO/IEC 20000-1 for service management. It is common for an organization to improve the way it operates to achieve conformity with the requirements specified in one International Standard and then make further improvements to achieve conformity with the requirements of another.

There are a number of advantages for an organization in ensuring its management system takes into account both the service lifecycle and the protection of the organization's information. These benefits can be experienced whether one International Standard is implemented before the other, or ISO/IEC 27001 and ISO/IEC 20000-1 are implemented simultaneously. Management and organizational processes, in particular, can derive benefit from the mutually reinforcing concepts and similarities between these International Standards and their common objectives.

Key benefits of an integrated implementation of information security management and service management include the following:

a) credibility to internal and external customers, and other interested parties of the organization, of effective and secure services;

b) lower cost of implementing, maintaining and auditing an integrated management system, where effective and efficient management of both services and information security are part of an organization's strategy;

c) reduction in implementation time due to the integrated development of processes supporting both service management and information security management;

d) better communication, increased reliability and improved operational efficiency through elimination of unnecessary duplication;

e) a greater understanding by service management and information security personnel of each other's viewpoints;

f) an organization certified for ISO/IEC 27001 can more easily fulfil the requirements for information security specified in ISO/IEC 20000-1:2018, 8.7.3, as ISO/IEC 27001 and ISO/IEC 20000-1 are complementary in requirements.

This document is based on ISO/IEC 27001:2013 and ISO/IEC 20000-1:2018.

This document is intended for use by persons who intend to integrate ISO/IEC 27001 and ISO/IEC 20000-1, and who are familiar with both, either or neither of those International Standards.

This document does not reproduce content of ISO/IEC 27001 or ISO/IEC 20000-1. Equally, it does not describe all parts of each International Standard comprehensively. Only those parts where subject matter overlaps or differs are described in detail. It is assumed that users of this document have access to ISO/IEC 20000-1 and ISO/IEC 27001.

NOTE Specific legislations can exist, which can impact the planning of an organization's management system.

# Information security, cybersecurity and privacy protection — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

## 1 Scope

This document gives guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 for organizations intending to:

a) implement ISO/IEC 27001 when ISO/IEC 20000-1 is already implemented, or vice versa;

b) implement both ISO/IEC 27001 and ISO/IEC 20000-1 together; or

c) integrate existing management systems based on ISO/IEC 27001 and ISO/IEC 20000-1.

This document focuses exclusively on the integrated implementation of an information security management system (ISMS) as specified in ISO/IEC 27001 and a service management system (SMS) as specified in ISO/IEC 20000-1.

## 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 20000-1:2018, *Information technology — Service management — Part 1: Service management system requirements*

ISO/IEC 27000:2018, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2013, *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 27000:2018 and ISO/IEC 20000-1:2018 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 Overview of ISO/IEC 27001 and ISO/IEC 20000-1

### 4.1 Understanding ISO/IEC 27001 and ISO/IEC 20000-1

An organization should have a good understanding of the characteristics, similarities and differences of ISO/IEC 27001 and ISO/IEC 20000-1 before planning an integrated management system for information security management and service management. This maximizes the time and resources available

for implementation. Subclauses 4.2 to 4.4 provide an introduction to the main concepts underlying ISO/IEC 27001 and ISO/IEC 20000-1 but should not be used as a substitute for a detailed review.

## 4.2 ISO/IEC 27001 concepts

ISO/IEC 27001 provides a model for establishing, implementing, maintaining and continually improving an information security management system (ISMS) to protect information. Information can take any form, be stored in any way and be used for any purpose by, or within, the organization.

To achieve conformity with the requirements specified in ISO/IEC 27001, an organization should implement an ISMS based on a risk assessment process. As part of a risk treatment process, the organization should select, implement, monitor and review a variety of measures to manage identified risks. These measures are known as information security controls. The organization should determine acceptable levels of risk, taking into account the requirements of interested parties relevant to information security. Examples of requirements are business requirements, legal and regulatory requirements or contractual obligations.

ISO/IEC 27001 can be used by any type and size of organization. Excluding any of the requirements specified in ISO/IEC 27001:2013, Clauses 4 to 10, is not acceptable when an organization claims conformity to ISO/IEC 27001.

## 4.3 ISO/IEC 20000-1 concepts

ISO/IEC 20000-1 specifies requirements for establishing, implementing, maintaining and continually improving a service management system (SMS). An SMS supports the management of the service lifecycle, including the planning, design, transition, delivery and improvement of services, which meet agreed requirements and deliver value for customers, users and the organization delivering the services.

Some of the requirements specified in ISO/IEC 20000-1 are grouped into clauses indicating processes, such as incident management, change management and supplier management. Some requirements for information security management are specified in ISO/IEC 20000-1:2018, 8.7.3. All requirements specified in ISO/IEC 20000-1 are generic and are intended to be applicable to all organizations, regardless of the organization's type or size, or the nature of the services delivered. ISO/IEC 20000-1 is intended for management of services using technology and digital information. Exclusion of any of the requirements in ISO/IEC 20000-1:2018, Clauses 4 to 10, is not acceptable when the organization claims conformity to ISO/IEC 20000-1, irrespective of the nature of the organization.

## 4.4 Similarities and differences

Service management and information security management are sometimes treated as if they are neither connected nor interdependent. The context for such separation is that service management can easily be related to efficiency, service quality, customer satisfaction and profitability, while information security management is often not understood to be fundamental to effective service delivery. As a result, service management is frequently implemented first. There are some shared concepts between these two disciplines, as well as concepts that are unique to each.

Information security management and service management clearly address very similar requirements and activities, even though the SMS and the ISMS each highlight different details. When working with ISO/IEC 27001 and ISO/IEC 20000-1, it should be understood that their characteristics differ in more than one aspect. It is possible that the scopes of an ISMS and an SMS can differ (see 5.2). They also have different intended outcomes. ISO/IEC 20000-1 is designed to ensure that the organization provides effective services, while ISO/IEC 27001 is designed to enable the organization to manage information security risk and recover from or prevent information security incidents.

See Annex A for details of the correspondence between ISO/IEC 27001:2013, Clauses 1 to 10, and ISO/IEC 20000-1:2018, Clauses 1 to 10. See Annex B for a comparison of topics between the controls in ISO/IEC 27001:2013, Annex A, and the requirements in ISO/IEC 20000-1:2018. See Annex C for a comparison of terms and definitions between ISO/IEC 27000 and ISO/IEC 20000-1.