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)

© ISO/IEC 2021



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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 ... **iv**

Introduction ... **v**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

4 Overview of ISO/IEC 27001 and ISO/IEC 20000-1 ... **1**
4.1 Understanding ISO/IEC 27001 and ISO/IEC 20000-1 ... 1
4.2 ISO/IEC 27001 concepts ... 2
4.3 ISO/IEC 20000-1 concepts ... 2
4.4 Similarities and differences ... 2

5 Approaches for integrated implementation ... **3**
5.1 General ... 3
5.2 Considerations of scope ... 3
5.3 Pre-implementation scenarios ... 4
5.3.1 General ... 4
5.3.2 Neither standard is currently used as the basis for a management system ... 4
5.3.3 The management system fulfils the requirements of one of the standards ... 5
5.3.4 Separate management systems exist which fulfil the requirements of each standard ... 6

6 Integrated implementation considerations ... **6**
6.1 General ... 6
6.2 Potential challenges ... 7
6.2.1 Requirements and controls ... 7
6.2.2 Assets and configuration items ... 7
6.2.3 Service design and transition ... 8
6.2.4 Risk assessment and management ... 9
6.2.5 Risk and other parties ... 10
6.2.6 Incident management ... 10
6.2.7 Problem management ... 11
6.2.8 Gathering of evidence ... 12
6.2.9 Major incident management ... 12
6.2.10 Classification and escalation of incidents ... 12
6.2.11 Change management ... 13
6.3 Potential gains ... 13
6.3.1 Service level management and reporting ... 13
6.3.2 Management commitment and continual improvement ... 13
6.3.3 Capacity management ... 14
6.3.4 Management of third parties and related risk ... 14
6.3.5 Continuity and availability management ... 15
6.3.6 Release and deployment management ... 15

Annex A (informative) **Correspondence between ISO/IEC 27001:2013, Clauses 1 to 10, and ISO/IEC 20000-1:2018, Clauses 1 to 10** ... **17**

Annex B (informative) **Correspondence between the controls in ISO/IEC 27001:2013, Annex A, and the requirements in ISO/IEC 20000-1:2018, Clauses 4 to 10** ... **19**

Annex C (informative) **Comparison of terms and definitions between ISO/IEC 27000:2018 and ISO/IEC 20000-1:2018** ... **22**

Bibliography ... **60**

© ISO/IEC 2021 – All rights reserved

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.

© ISO/IEC 2021 – All rights reserved

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.

© ISO/IEC 2021 – All rights reserved

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

© ISO/IEC 2021 – All rights reserved