TECHNICAL REPORT

ISO/IEC TR 20000-7

First edition
2019-07

Information technology — Service management —

Part 7:

Guidance on the integration and correlation of ISO/IEC 20000-1:2018 to ISO 9001:2015 and ISO/IEC 27001:2013

Reference number
ISO/IEC TR 20000-7:2019(E)

© ISO/IEC 2019



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2019

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
Fax: +41 22 749 09 47
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 ... **2**

4 Integration of ISO/IEC 20000-1:2018 with other management system standards (MSS) ... **2**
4.1 Introduction to ISO/IEC 20000-1:2018 ... 2
4.2 ISO/IEC Directives, Part 1, high level structure (HLS) for management system standards (MSS) common requirements ... 3
4.3 Service management specific requirements ... 4
4.4 Considerations for the integration of management system standards (MSS) ... 6

5 Integration of ISO/IEC 20000-1:2018 with ISO 9001:2015 ... **7**
5.1 Introduction to ISO 9001:2015 ... 7
5.2 Similarities and differences in requirements between ISO/IEC 20000-1:2018 and ISO 9001:2015 ... 7
5.2.1 General ... 7
5.2.2 Service design and transition ... 7
5.2.3 External suppliers ... 8
5.3 Quality management specific requirements ... 8
5.4 Considerations for the integration of an SMS and a QMS ... 9

6 Integration of ISO/IEC 20000-1:2018 with ISO/IEC 27001:2013 ... **9**
6.1 Introduction to ISO/IEC 27001:2013 ... 9
6.2 Similarities and differences in requirements between ISO/IEC 20000-1:2018 and ISO/IEC 27001:2013 ... 10
6.2.1 General ... 10
6.2.2 Scope ... 10
6.2.3 Information security management ... 10
6.2.4 Risk management ... 11
6.2.5 ISO/IEC 27001:2013, Annex A Controls ... 12
6.3 Information security management specific requirements ... 14
6.4 Considerations for the integration of an SMS and an ISMS ... 15

7 Integration of ISO/IEC 20000-1:2018, ISO 9001:2015 and ISO/IEC 27001:2013 ... **15**
7.1 Similarities and differences in requirements between ISO/IEC 20000-1:2018, ISO 9001:2015 and ISO/IEC 27001:2013 ... 15
7.2 Considerations for the integration of an SMS, a QMS and an ISMS ... 19
7.2.1 High level structure (HLS) ... 19
7.2.2 Scope ... 19
7.2.3 Service design, build and transition ... 20
7.2.4 Change management and release and deployment management ... 20
7.2.5 Supplier management ... 20

Annex A (informative) **Correlation of terms and definitions between ISO/IEC 20000-1:2018, ISO 9000:2015, and ISO/IEC 27000:2018** ... **21**

Annex B (informative) **Correlation of ISO/IEC 20000-1:2018 to ISO 9001:2015** ... **40**

Annex C (informative) **Correlation of ISO/IEC 20000-1:2018 to ISO/IEC 27001:2013** ... **49**

Bibliography ... **57**

© ISO/IEC 2019 – All rights reserved

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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 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 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.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 40, *IT Service Management and IT Governance*.

A list of all parts in the ISO/IEC 20000 series can be found on the ISO website.

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.

© ISO/IEC 2019 – All rights reserved

Introduction

This document provides guidance on the integration of ISO/IEC 20000-1:2018, ISO 9001:2015 and ISO/IEC 27001:2013. All three standards use the clause structure, common terms and common requirements from the high level structure (HLS) of management system standards (MSS) specified in the ISO/IEC Directives, Part 1. The adoption of the HLS enables an organization to align or integrate multiple management system standards. For example, a service management system (SMS) can be integrated with a quality management system based on ISO 9001 or an information security management system based on ISO/IEC 27001. The relationship between these three standards is very close; therefore, many organizations may already recognise the benefits of adopting two or all three of them.

Benefits of an integrated implementation of management systems can be:

a) less effort and lower cost for the organization to implement the integrated management system and less ongoing effort required to keep it updated;

b) increased credibility to external parties of the organization having a single integrated management system;

c) more effective internal processes and improved communication in the organization by streamlining the interaction between the service, quality, and information security management aspects of their management system.

Apart from the common terms, requirements and the HLS, there are other commonalities in these three standards that provide an opportunity for integration. On the other hand, there are also differences that need to be kept in mind when integrating these management systems.

It is assumed that users of this document have access to and a basic understanding of the ISO/IEC 20000-1, ISO 9001, and ISO/IEC 27001 standards. The content of these standards is not repeated nor fully explained in this document.

NOTE The high level structure (HLS) of management system standards (MSS) specified in the ISO/IEC Directives, Part 1, Annex L, is referred to in this document as either "HLS" or "HLS of MSS". The high level structure was formerly contained in the ISO/IEC Directives, Part 1, Annex SL. In this document, the term "Annex SL" is used only when making a direct citation to a standard that was published when the Annex SL was still in place, e.g. ISO 9001:2015, ISO/IEC 20000-1:2018, ISO/IEC 27001:2013.

© ISO/IEC 2019 – All rights reserved

Information technology — Service management —

Part 7: Guidance on the integration and correlation of ISO/IEC 20000-1:2018 to ISO 9001:2015 and ISO/IEC 27001:2013

1 Scope

This document provides guidance on the integrated implementation of a service management system (SMS) as specified in ISO/IEC 20000-1 with a quality management system (QMS) as specified in ISO 9001 and an information security management system (ISMS) as specified in ISO/IEC 27001. It is aimed at those organizations that are intending to either:

a) implement ISO 9001 when ISO/IEC 20000-1 is already implemented, or vice versa;

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

c) implement both ISO 9001 and ISO/IEC 20000-1 together, or implement both ISO/IEC 27001 and ISO/IEC 20000-1 together;

d) implement ISO/IEC 20000-1, ISO 9001 and ISO/IEC 27001 together; or

e) integrate existing management systems based on ISO/IEC 20000-1, ISO 9001 and ISO/IEC 27001.

In practice, an SMS, QMS or ISMS can also be integrated with other management system standards (MSS), such as ISO 22301 or ISO 55001.

Clause 4 provides an introduction to ISO/IEC 20000-1, the HLS of MSS specified in ISO/IEC Directives Part 1 and considerations for the integration of an MSS.

Clause 5 provides an introduction to ISO 9001, commonalities and differences with ISO/IEC 20000-1 and considerations for the integration of an SMS with a QMS.

Clause 6 provides an introduction to ISO/IEC 27001, commonalities and differences with ISO/IEC 20000-1 and considerations for the integration of an SMS with an ISMS.

Clause 7 looks at considerations for the integration of an SMS, a QMS, and an ISMS.

This document also provides correlation information for the terms and definitions of ISO/IEC 20000-1 with ISO 9001 and ISO/IEC 27001 in Annex A. Correlation of the clauses of ISO/IEC 20000-1 with ISO 9001 is shown in Annex B. Correlation of the clauses of ISO/IEC 20000-1 with ISO/IEC 27001 is shown in Annex C.

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 9000:2015, *Quality management systems — Fundamentals and vocabulary*

ISO/IEC 20000-1:2018, *Information technology — Service management — Part 1: Service management system requirements*

© ISO/IEC 2019 – All rights reserved

ISO/IEC 27000:2018, *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 9000:2015, ISO/IEC 20000-1:2018, and ISO/IEC 27000:2018 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 Integration of ISO/IEC 20000-1:2018 with other management system standards (MSS)

4.1 Introduction to ISO/IEC 20000-1:2018

ISO/IEC 20000-1 specifies requirements for establishing, implementing, maintaining and continually improving an 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. The organization in the scope of the SMS can be a whole or part of a larger organization. The organization in the scope of the SMS can also be known as the service provider.

ISO/IEC 20000-1 is intentionally independent of specific guidance. The organization can use a combination of generally accepted frameworks and its own experience. Appropriate tools for service management can be used to support the SMS.

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. For example, the services can be information technology, business process outsourcing, or facilities management.

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.

The organization cannot demonstrate conformity to the requirements specified in ISO/IEC 20000-1 if other parties are used to provide or operate *all* services, service components or processes within the scope of the SMS.

ISO/IEC 20000-10 includes the concepts for an SMS, the vocabulary used for the ISO/IEC 20000 series, a description of each part of the series and related standards. The vocabulary is split into subclause 3.1 for the HLS terms, subclause 3.2 for service management specific terms used in ISO/IEC 20000-1 and subclause 3.3 for terms used in the rest of the series. Subclauses 3.1 and 3.2 are the same as in ISO/IEC 20000-1.

Figure 1 illustrates an SMS showing the clause content of ISO/IEC 20000-1.

© ISO/IEC 2019 – All rights reserved