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 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) 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.

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.

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 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.

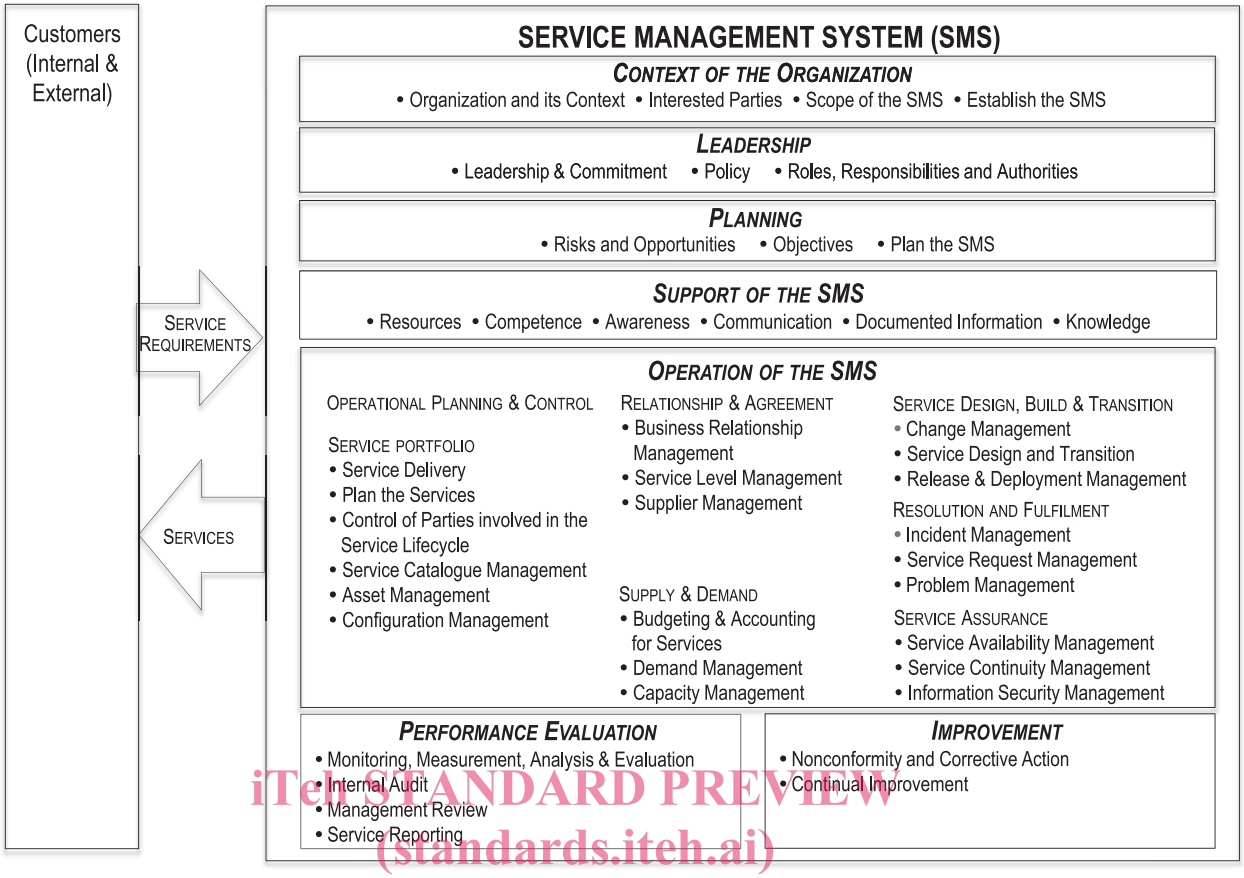

Figure 1 — Service management system

4.2 ISO/IEC Directives, Part 1, high level structure (HLS) for management system standards (MSS) common requirements

The ISO/IEC Directives, Part 1, HLS for MSS includes common terms and definitions, common requirements, and the clause structure (titles and sequence) required for MSS. Table 1 illustrates the HLS without any modifications for the subject matter. 'XXX' is replaced by the relevant subject for each standard.

Table 1 — The high level structure (HLS) for management system standards (MSS)

Clause	Title
4	**Context of the organization**
4.1	Understanding the organization and its context
4.2	Understanding the needs and expectations of interested parties
4.3	Determining the scope of the XXX management system
4.4	XXX management system
5	**Leadership**
5.1	Leadership and commitment
5.2	Policy
5.3	Organizational roles, responsibilities and authorities
6	**Planning**
6.1	Actions to address risks and opportunities
6.2	XXX objectives and planning to achieve them

Table 1 *(continued)*

Clause	Title
7	**Support**
7.1	Resources
7.2	Competence
7.3	Awareness
7.4	Communication
7.5	Documented information
8	**Operation**
8.1	Operational planning and control
9	**Performance evaluation**
9.1	Monitoring, measurement, analysis and evaluation
9.2	Internal audit
9.3	Management review
10	**Improvement**
10.1	Nonconformity and corrective action
10.2	Continual improvement

4.3 Service management specific requirements

Each MSS adds subject-specific terms and requirements to the HLS. This is done by adding to existing requirements within the HLS or by adding new sub-clauses. If justified, some of the HLS for MSS terms and requirements can be modified but this is only done by exception to try to retain the common terms and requirements to enable integration of the various MSS.

ISO/IEC 20000-1 lists the HLS for MSS terms and definitions as well as additional terms and definitions that are specific to service management. All modifications of HLS for MSS terms are explained in a note to the term.

An example of the modification of a HLS for MSS term is for corrective action where the text has been modified as indicated in Note 1 to entry:

> *'action to eliminate the cause or reduce the likelihood of recurrence of a detected nonconformity or other undesirable situation'*
>
> *Note 1 to entry: The original Annex SL definition has been changed by adding text to the original "action to eliminate the cause of a nonconformity and to prevent recurrence".*

An example of a modification of HLS for MSS requirements is in ISO/IEC 20000-1:2018, 4.2. The HLS for MSS text is: *'The organization shall determine: a) the interested parties that are relevant to the SMS;'*. This has been modified in ISO/IEC 20000-1 to add 'and the services':

> *'The organization shall determine: a) the interested parties that are relevant to the SMS and the services;'*

This modification to add 'and the services' has been made in many places because ISO/IEC 20000-1 is focused on the use of the SMS to ensure successful delivery of services.

Examples of the addition of subclauses can be seen in Table 2. ISO/IEC 20000-1 changed two clause titles: Clause 7 Support and Clause 8 Operation. These were changed to 'Support of the SMS' and 'Operation of the SMS' because the words support and operation have a specific meaning in service management. The HLS titles could have been interpreted as meaning support and operation of the services. In ISO/IEC 20000-1, the SMS is operated to deliver the services.

Table 2 shows the HLS with the added subclauses and title changes specific to service management in ISO/IEC 20000-1 shown in italics.

Table 2 — The high level structure modified for ISO/IEC 20000-1

Clause	Title
4	**Context of the organization**
4.1	Understanding the organization and its context
4.2	Understanding the needs and expectations of interested parties
4.3	Determining the scope of the *service* management system
4.4	*Service* management system
5	**Leadership**
5.1	Leadership and commitment
5.2	Policy
5.3	Organizational roles, responsibilities and authorities
6	**Planning**
6.1	Actions to address risks and opportunities
6.2	*Service* management objectives and planning to achieve them
6.3	*Plan the service management system*
7	**Support *of the service management system***
7.1	Resources
7.2	Competence
7.3	Awareness
7.4	Communication
7.5	Documented information
7.5.4	*Service management system documented information*
7.6	*Knowledge*
8	**Operation *of the service management system***
8.1	Operational planning and control
8.2	***Service portfolio***
8.2.1	*Service delivery*
8.2.2	*Plan the services*
8.2.3	*Control of parties involved in the service lifecycle*
8.2.4	*Service catalogue management*
8.2.5	*Asset management*
8.2.6	*Configuration management*
8.3	***Relationship and agreement***
8.3.1	*General*
8.3.2	*Business relationship management*
8.3.3	*Service level management*
8.3.4	*Supplier management*
8.4	***Supply and demand***
8.4.1	*Budgeting and accounting for services*
8.4.2	*Demand management*
8.4.3	*Capacity management*
8.5	***Service design, build and transition***
8.5.1	*Change management*

Table 2 *(continued)*

Clause	Title
8.5.2	*Service design and transition*
8.5.3	*Release and deployment management*
8.6	***Resolution and fulfilment***
8.6.1	*Incident management*
8.6.2	*Service request management*
8.6.3	*Problem management*
8.7	***Service assurance***
8.7.1	*Service availability management*
8.7.2	*Service continuity management*
8.7.3	*Information security management*
9	**Performance evaluation**
9.1	Monitoring, measurement, analysis and evaluation
9.2	Internal audit
9.3	Management review
9.4	*Service reporting*
10	**Improvement**
10.1	Nonconformity and corrective action
10.2	Continual improvement

4.4 Considerations for the integration of management system standards (MSS)

The adoption of the HLS with the common terms and requirements enables an organization to align or integrate multiple MSS within an integrated management system. For example, an SMS based on ISO/IEC 20000-1 can be integrated with a QMS based on ISO 9001 and/or an ISMS based on ISO/IEC 27001. When an MSS conforms to the HLS, this makes the integration easier. All new MSS and updates for existing MSS now have to conform to the HLS and there are only a few MSS which do not yet conform.

The HLS provides common requirements and terms. However, it is essential to remember that each standard has a different focus and the requirements will be interpreted and used within that focus area.

An integrated management system can support common activities across an organization. For example, if the internal audit process in an organization is common for all MSS, then this only needs to be designed, documented and audited once for all MSS. This saves time and effort at all stages. If there are some minor variances for an activity, then this can be shown in the process description. For example, if the management review process in an organization has a common base but some variances for each MSS, then the common process can be designed and documented with the variances for each MSS clearly shown.

It is important to look carefully at each MSS that is being integrated. There are some minor variances in HLS clauses which can be easily missed, e.g. the addition of 'and the services' in many HLS for MSS requirements for ISO/IEC 20000-1.

It is not only the HLS clauses that can be common across MSS. There are also many areas of commonality across MSS with different subject matters. For example, both ISO/IEC 20000-1 and ISO 9001 address knowledge and both ISO/IEC 20000-1 and ISO/IEC 27001 address change management. These commonalities and differences are explained further in this document.

An integrated management system should still make clear which clauses from each standard are being covered. For example, if knowledge were to be a common process in an integrated management system for ISO/IEC 20000-1 and ISO 9001, it should be clear that this is for ISO/IEC 20000-1:2018, 7.6 and ISO 9001:2015, 7.1.6.

5 Integration of ISO/IEC 20000-1:2018 with ISO 9001:2015

5.1 Introduction to ISO 9001:2015

ISO 9001 specifies requirements for a QMS when an organization:

a) needs to demonstrate its ability to consistently provide products and services that meet customer and applicable statutory and regulatory requirements;

b) aims to enhance customer satisfaction through the effective application of the system, including processes for improvement of the system and the assurance of conformity to customer and applicable statutory and regulatory requirements.

All the requirements of ISO 9001 are generic and are intended to be applicable to any organization, regardless of its type or size, or the products and services it provides.

The implementation of a QMS requires the adoption of a process approach, risk-based thinking and the pursuit of continual improvement using the "Plan-Do-Check-Act" cycle at all levels of the organization.

ISO 9000 includes the fundamental concepts and the quality management principles on which a sound QMS is based, as well as the relevant terms and definitions for the ISO 9000 series of standards. ISO 9000 provides the background for the proper understanding and implementation of ISO 9001. The quality management principles are:

— customer focus;

— leadership;

— engagement of people;

— process approach;

— improvement;

— evidence-based decision making;

— relationship management.

5.2 Similarities and differences in requirements between ISO/IEC 20000-1:2018 and ISO 9001:2015

5.2.1 General

Both ISO/IEC 20000-1 and ISO 9001 are based on the HLS with common terms and common requirements for many areas which will support integration. An SMS according to ISO/IEC 20000-1 is focused on the management of services to ensure that they meet agreed service requirements and deliver value for the customers, users and the organization itself. ISO 9001 focuses on meeting customer requirements and enhancing customer satisfaction through the use of a QMS. ISO/IEC 20000-1 includes clauses for a service lifecycle with many requirements not present in ISO 9001 providing assurance of the high-quality delivery of services throughout the service lifecycle following accepted service management best practice.

5.2.2 Service design and transition

Requirements for design and transition planning are similar in ISO 9001:2015, 8.3 *Design and development of products and services* (which itself does not refer to transition planning) and in ISO/IEC 20000-1:2018, 8.5 *Service design, build and transition*.

ISO/IEC 20000-1 and ISO 9001 differences are:

— ISO/IEC 20000-1, 8.5 *Service design, build and transition,* is used to create new services, change services, transfer services and remove services. ISO 9001:2015, 8.3 *Design and development of products and services,* is used to create new products or services as well as design changes;

— ISO/IEC 20000-1 refers to requirements, service acceptance criteria and intended outcomes; ISO 9001 refers to inputs and outputs of design and development;

— ISO/IEC 20000-1 refers to change management, configuration management, impact assessment and testing; in ISO 9001 the control of design and development refers to review, verification and validation activities.

A single design and development process may be defined to fulfil the extensive requirements of ISO/IEC 20000-1:2018, 8.5 and ISO 9001:2015, 8.3. However, careful consideration is needed to see if it is possible to have a combined process that is relevant to both products and services since there are considerable differences as well as commonalities between the requirements of each standard.

5.2.3 External suppliers

Management of external suppliers is similar in ISO/IEC 20000-1 and ISO 9001: both take a "risk-based thinking" approach or use impact evaluation to determine controls and apply criteria for the evaluation and monitoring of performance. The relevant clauses are in ISO/IEC 20000-1:2018, 8.2.3 *Control of parties involved in the service lifecycle,* and 8.3.4, *Supplier management,* and in ISO 9001:2015, 8.4 *Control of externally provided process, products and services*.

Communication of requirements to be met by external providers has different wording in ISO/IEC 20000-1 and ISO 9001, but the outcome is a documented agreement. ISO/IEC 20000-1 and ISO 9001 both require the determination and application of criteria for evaluation, selection, monitoring of performance and continual evaluation of external providers.

Differences between ISO/IEC 20000-1 and ISO 9001 are:

— In ISO/IEC 20000-1, it is necessary to have a documented contract with the external supplier containing the scope of the services, requirements to be met, service level targets, responsibilities and authorities. In ISO 9001, additional requirements should be communicated, namely, the approvals, competence of persons, control and monitoring of performance, and verification or validation activities intended to be performed at the supplier's premises.

— ISO/IEC 20000-1 requires the organization to assess alignment of service level targets or other contractual obligations for the external supplier against SLAs with customers and manage identified risks. For ISO 9001 the organization should take into consideration the potential impact of the externally provided processes, products, services and determine verification activities;

— ISO/IEC 20000-1:2018, 8.3.4 applies to external suppliers, internal suppliers, and customers acting as a supplier. ISO 9001:2015, 8.4 applies to external providers of processes, products and services. For ISO 9001 external providers could include associate companies (which include internal suppliers) or external suppliers.

5.3 Quality management specific requirements

ISO 9001 has the following specific requirements not related to ISO/IEC 20000-1:

a) 7.1.4 Environment for the operation of processes;

b) 7.1.5 Monitoring and measuring resources;

c) 8.5.2 Identification and traceability;

d) 8.5.3 Property belonging to customers or external providers;

e) 8.5.4 Preservation;

f) 8.5.5 Post-delivery activities;

g) 8.7 Control of nonconforming outputs.

5.4 Considerations for the integration of an SMS and a QMS

There are many questions asked about why an organization might want to use both ISO 9001 and ISO/IEC 20000-1 when ISO 9001 deals with services as well as products. ISO/IEC 20000-1 is applicable only to service management and services. There is a subtle difference in the focus of the two standards. A QMS according to ISO 9001 is focused on understanding and meeting the needs and expectations of customers and other relevant interested parties, for which it adopts a process-based approach.

The scope defines the boundaries of the management system, so it is possible to claim that the organization, or a part of it, meets the requirements of the MSS. The scope of a QMS can include all or a part of the organization's activities, products or services. The scope of an SMS can include all or part of an organization, and all or some of the services of the organization. It is common to see an organization with a QMS for the whole organization and an SMS for the part of the organization that delivers services.

In ISO 9001, some requirements may not be applicable and be excluded with an adequate justification. In ISO/IEC 20000-1 that is not possible: all requirements must be met and no exclusions may be made.

An organization can implement ISO 9001 with service management activities in the scope, but that does not mean the organization can demonstrate conformity with ISO/IEC 20000-1 since ISO 9001 is generic and does not require all of the service lifecycle processes that are specified in ISO/IEC 20000-1.

It will be possible to integrate some of the processes that are common across the SMS and QMS — see Annex B for a detailed mapping.

NOTE ISO/IEC 20000-3 provides guidance on scope definition for an SMS.

6 Integration of ISO/IEC 20000-1:2018 with ISO/IEC 27001:2013

6.1 Introduction to ISO/IEC 27001:2013

ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining and continually improving an ISMS within the context of the organization's information security risks. An ISMS preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that information security risks are adequately managed.

The establishment and implementation of an organization's ISMS is a strategic decision, influenced by the organization's needs and objectives, security requirements, the organizational processes and the size and structure of the organization. All these factors may change over time. The ISMS should be integrated into the organization's business processes. This means that information security should be considered in the design of business processes, information systems and controls.

ISO/IEC 27001 includes requirements for the assessment and treatment of information security risks implemented in a way that is tailored to the needs of the organization. It also specifies requirements for the implementation of a set of information security controls to control and mitigate these risks associated with information assets the organization is using. These controls are customized to the needs of the organization or parts of it.

ISO/IEC 27001 can be used by all organizations, regardless of type, size and nature.