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.

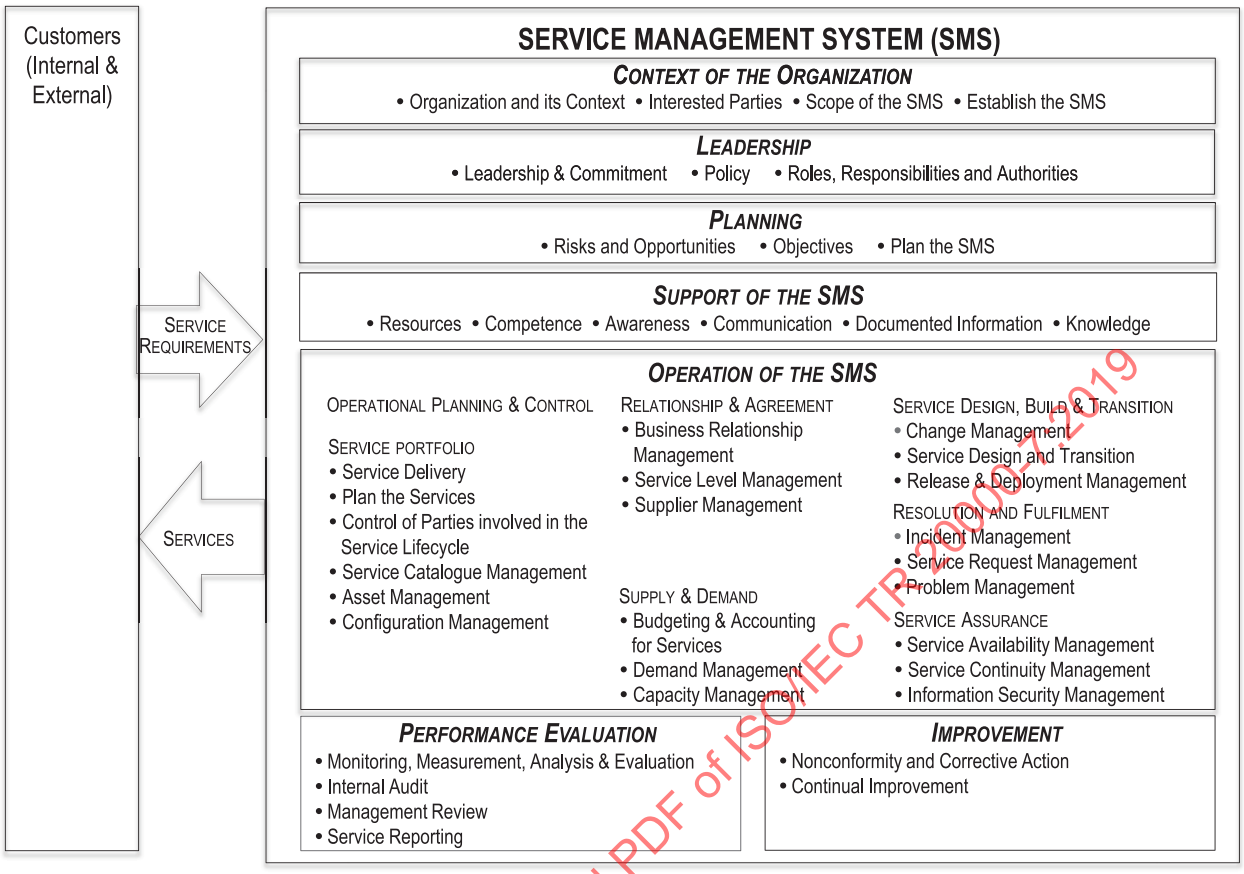

Figure 1 — Service management system

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.

ISO/IEC 27000 describes the overview and the vocabulary of an ISMS, with a description of the information security family of standards.

ISO/IEC 27013 focuses on the integrated implementation of an ISMS and an SMS as specified in ISO/IEC 20000-1, but does so from the perspective of ISO/IEC 27001. This document looks at the integration of an SMS and an ISMS from the perspective of ISO/IEC 20000-1. There is some commonality between ISO/IEC 27013 and this document.

6.2 Similarities and differences in requirements between ISO/IEC 20000-1:2018 and ISO/IEC 27001:2013

6.2.1 General

A significant part of the requirements of ISO/IEC 27001 is based on the HLS for MSS text. It therefore has many similarities with the requirements in ISO/IEC 20000-1 that are based on the HLS for MSS. Minor differences appear in some of these clauses. These differences are summarised and correlated in Annex C of this document. The most significant difference is in the area of risk management. Furthermore, several controls in ISO/IEC 27001:2013, Annex A have commonalities with requirements of ISO/IEC 20000-1.

6.2.2 Scope

The scope statement for ISO/IEC 27001 is focused on the organization, taking its activities and those performed by other parties into account. ISO/IEC 27006 also specifies that the statement of applicability with its version needs to be on the certificate of conformity. The scope statement of ISO/IEC 20000-1 does not include a statement of applicability and explicitly needs to state which services are in scope of the SMS.

NOTE ISO/IEC 27006 specifies requirements and provides guidance for bodies providing audit and certification of an information security management system (ISMS).

The scope of an ISMS can include all or a part of the organization's activities. The scope of an SMS can include all or part of an organization, and all or some of the services of the organization. For example, it is possible to see an organization with an ISMS for the whole organization and an SMS for the part of the organization that delivers services.

In ISO/IEC 20000-1 and ISO/IEC 27001, all requirements have to be met and no exclusions may be made in Clauses 4 to 10. However, ISO/IEC 27001 has controls listed in Annex A, some of which may be excluded with an adequate justification, based on the risk assessment.

6.2.3 Information security management

ISO/IEC 20000-1:2018, 8.7.3 covers some of the aspects of the requirements in ISO/IEC 27001 for information security management. These include the information security policy, information security risk and controls, and information security incidents.

The information security policy, as required by ISO/IEC 27001:2013, 5.2, is based on similar requirements as the service management policy in ISO/IEC 20000-1:2013, 5.2. In addition, control A.5 in ISO/IEC 27001 requires that a set of policies for information security should be defined, approved and communicated to internal employees and relevant external parties. This can map to the requirements of ISO/IEC 20000-1 for an information security policy. ISO/IEC 20000-1 states that the policy should be approved by management with appropriate authority. This can be top management for the ISMS if the policy already exists or top management for the SMS. There is a specific requirement in ISO/IEC 20000-1 that the policy should take into consideration the service requirements and obligations such as legal and regulatory requirements stated in the service management plan. If the ISMS has already produced an information security policy, then there may need to be some additions or amendments to ensure that it includes aspects related to the SMS and the services.

The requirements for information security controls in ISO/IEC 20000-1 are to assess and document information security risks (including those related to external organizations), determine, implement and operate controls to address these risks, and monitor and review these controls. These requirements can be mapped with some of the ISO/IEC 27001 risk assessment and risk treatment processes in subclauses 6.1.2 and 6.1.3. However, there is no requirement in ISO/IEC 20000-1 to use Annex A controls from ISO/IEC 27001 or to produce a statement of applicability. If an ISMS already exists, then the controls used need to be reviewed in order to ensure that they address the information security risks identified for the SMS and the services.

ISO/IEC 20000-1 specifies requirements to manage information security incidents that may or may not be handled in the same way as the general incident management process in subclause 8.6.1. Control A.16 in ISO/IEC 27001 has seven controls for information security incident management. The focus of these controls is on organizational and reporting aspects as well as incident assessment, incident response, evidence collection and learning from incidents. The last aspect includes elements of the problem management process of ISO/IEC 20000-1:2018, 8.6.3. The requirements from ISO/IEC 20000-1 and the controls from ISO/IEC 27001 may be combined into incident and problem management processes, taking the different perspectives of both standards into account.

6.2.4 Risk management

The definition of risk in ISO/IEC 27000 differs from that in ISO/IEC 20000-1 but they have the same intent and this difference has no impact on the integration of the two standards.

In ISO/IEC 20000-1, the default HLS for MSS requirements for risk assessment of the SMS and the services are present and subclause 6.1.2 contains some additional requirements. The risks and opportunities are assessed for their impact on the customers, risk acceptance criteria are defined and an approach to manage these risks is determined and documented.

Furthermore, the requirements for information security controls in ISO/IEC 20000-1:2018, 8.7.3.2 are to assess and document information security risks (including those related to external parties), determine, implement and operate controls to address these risks and monitor and review these controls.

In ISO/IEC 20000-1, risks are those that relate to the organization, the SMS, the services and suppliers. Risk is also required to be assessed and documented for service availability and service continuity in ISO/IEC 20000-1:2018, 8.7.1 and 8.7.2. Risk is also taken into consideration in ISO/IEC 20000-1:2018, 6.3, 8.2.2, 8.3.4.1, 8.5.1.3.

Risks and opportunities that need to be addressed in ISO/IEC 27001 are determined in subclause 6.1.1 to ensure the ISMS can achieve its intended outcomes, prevent undesired effects and achieve continual improvement, in relation to the organization and its interested parties. ISO/IEC 27001:2013, 6.1.2 has an emphasis on risks related to information security and provides the risk assessment requirements. ISO/IEC 27001:2013, 6.1.3 continues with requirements for risk treatment. Finally, ISO/IEC 27001:2013, 8.2 and 8.3 have requirements for the practical operation of the risk management process. Only in ISO/IEC 20000-1:2018, 8.7.3, are risks specifically related to information security identified. This difference in emphasis is important, even though the processes to manage risks can be set up in a generic way, such that they apply to all types of risk.

In ISO/IEC 27001:2013, Clause 6, the default requirements from the HLS for MSS to assess risks to and opportunities for the ISMS are listed. In addition to these, there are extensive requirements for a risk management process. This process should consist of two parts: risk assessment and risk treatment.

NOTE ISO 31000 provides guidance for risk management. ISO/IEC 27001's requirements for risk management are aligned to ISO 31000.

The risk assessment process in ISO/IEC 27001 consists of a number of activities, including:

a) establishing and maintaining information security risk criteria, including risk acceptance criteria and criteria for performing risk assessment;

b) identifying security risks, based on confidentiality, integrity and availability criteria, and identifying risk owners;

c) assessing risks based on potential impact and likelihood of occurrence;

d) evaluating risks by comparing them to the risk acceptance criteria and prioritizing them for treatment.

The risk treatment process in ISO/IEC 27001 consists of a number of activities, including:

— determining the treatment options for identified risks and the controls that are to be implemented for them;

— comparing these controls to the controls in ISO/IEC 27001:2013, Annex A and documenting these in a Statement of Applicability containing the selected controls and the justification why these were or were not selected, noting that other controls can also be used;

— defining a risk treatment plan, having this plan accepted by the risk owners and having any residual risks remaining after treatment accepted by these owners.

ISO/IEC 27001:2013, Clause 8 contains requirements to perform risk assessments at regular intervals and when significant changes take place. Furthermore, the risk treatment plan should be implemented.

6.2.5 ISO/IEC 27001:2013, Annex A Controls

6.2.5.1 General

ISO/IEC 27001:2013, Annex A lists 114 possible controls that an organization should compare to the controls determined by their information security risk assessment, to verify that no necessary controls have been omitted. Not all controls need to be implemented by all organizations. The controls determined are documented in the organization's Statement of Applicability along with a justification for their inclusion or exclusion. Other controls can also be used and, if this is the case, they should also be listed in the Statement of Applicability. The Statement of Applicability is a required document in ISO/IEC 27001, but not in ISO/IEC 20000-1.

In what follows, a comparison is made between some of the controls from ISO/IEC 27001:2013, Annex A and requirements from ISO/IEC 20000-1, assuming that the Annex A controls have been implemented. See Annex C for a full correlation between ISO/IEC 20000-1 and ISO/IEC 27001.

6.2.5.2 Asset management and configuration management

The word *asset* is not explicitly defined in ISO/IEC 27000. ISO/IEC 20000-1 defines an asset as anything that has potential or actual value to the organization (taken from ISO/IEC 19770-5). A note in the definition of *risk* in ISO/IEC 27000, however, focuses explicitly on vulnerabilities of *information* assets. The focus of ISO/IEC 27001 is on information security; therefore, it can be assumed that where that standard refers to assets, these are assets related to information. The use of the word asset in ISO/IEC 20000-1 is much broader, including both physical and non-physical assets, e.g. logical addressing and brands, which are not necessarily related to information.

NOTE Asset management in the context of ISO/IEC 20000-1 and ISO/IEC 27001 focuses on the management of assets. Asset management as meant by ISO 55001 has a broader focus, including managing assets, but also the strategic use of assets, the purpose of assets in the organization and other aspects.

In ISO/IEC 20000-1:2018, 8.2.5, the requirements for asset management are limited to ensuring that assets used to provide services are managed to meet service requirements and obligations such as legal and regulatory requirements. If an asset is also a configuration item (CI), its configuration information should be recorded and regularly verified, and the CIs should be controlled using the configuration management in ISO/IEC 20000-1:2018, 8.2.6.

Some of the controls related to assets in ISO/IEC 27001:2013, Annex A can be used to conform to some of the requirements in ISO/IEC 20000-1 for asset management and configuration management.

Control A.8 in ISO/IEC 27001 contains ten controls related to asset management. These controls include the identification of assets, assigning owners to them and defining protection measures for them. Furthermore, information is considered an asset that requires appropriate protection through classification and labelling. Media assets should be handled such that information stored on them cannot be disclosed to unauthorised parties.

Other controls related to assets in ISO/IEC 27001 are related to access rights (A.9.2.5), physical security (A.11.2) and the use of assets by suppliers (A.15.1). These controls may support asset management in ISO/IEC 20000-1 but there are no equivalent requirements.

6.2.5.3 Supplier management

ISO/IEC 20000-1 has extensive requirements for different types of suppliers in several clauses. Subclause 8.2.3 *Control of other parties involved in the service lifecycle* and subclause 8.3.4 *Supplier management*, cover the management and control of external suppliers, internal suppliers and customers acting as a supplier. ISO/IEC 20000-1:2018, 8.7.3 has a requirement that the information security policy should be communicated to internal and external suppliers and specifically requires controls related to information security risks related to external organizations.

ISO/IEC 20000-1 makes an explicit distinction between external suppliers, internal suppliers and customers acting as a supplier. ISO/IEC 27001 uses the word *supplier* in a generic sense, assuming it is a group external to the organization in the scope of the ISMS. If integrating the two standards, then the word 'supplier' in ISO/IEC 27001 can be the equivalent of the three types of supplier in ISO/IEC 20000-1.

Control A.15 in ISO/IEC 27001 considers the role of information security in supplier relationships. This includes protecting assets that are accessible to suppliers, and maintaining agreed levels of information security and service delivery by suppliers.

The controls in A.15 of ISO/IEC 27001 can help to meet some of the requirements around suppliers in ISO/IEC 20000-1, but are limited to making sure information security controls apply to suppliers and to monitoring and reviewing suppliers and changes to their service provision.

Control A.14.2.7 Outsourced development, has elements related to supplier management specifically where system development is outsourced. This may be part of an ISO/IEC 20000-1 scope and, if so, can be taken into account.

6.2.5.4 Change management and release and deployment management

The requirements in ISO/IEC 20000-1 for the change management process covers all of the controls in ISO/IEC 27001 for change management.

The requirements in ISO/IEC 20000-1 for change management focus on the services and configuration items although it can also be used for the SMS. Change management in control A.12.1.2 in ISO/IEC 27001 refers to the organization and its business processes, facilities and systems. There may well be overlap between these two scopes for change management, but care needs to be taken to what extent this overlap exists.

Control A.14.2 in ISO/IEC 27001 specifies controls for system development and support, including some controls for changes to these systems. The controls involve control of changes, review and testing after changes, restrictions to changing software packages, and system acceptance testing. These controls can provide some input to the change management and release and deployment management processes in ISO/IEC 20000-1 if applied to the services.

Control A.15.2.2 Managing changes to supplier services, is related to change management, where changes in suppliers need to be managed and a risk re-assessment may need to be performed, depending on the criticality of business information involved.

The requirements of ISO/IEC 20000-1 for these processes are, however, far more extensive than what is covered in the ISO/IEC 27001 controls.

6.2.5.5 Service design and transition

ISO/IEC 20000-1 has extensive requirements for service design and transition. A few controls in ISO/IEC 27001:2013, Annex A apply to this process, including:

a) A.12.1.4 specifying separation of development, testing and operational environments;

b) A.14.1.1 specifying information security analysis and requirements;

c) A.14.2.1 specifying secure development of systems and software;

d) A.14.2.5 specifying secure system engineering methodologies;

e) A.14.2.6 specifying the need for a secure development environment;

f) A.14.2.9 specifying system acceptance testing.

These controls are helpful in case they can be applied to the services, but can only fulfil the requirements for service design and transition in ISO/IEC 20000-1 to a small extent.

6.2.5.6 Service continuity management

ISO/IEC 20000-1 specifies requirements for service continuity that include planning, implementing, testing and reviewing of service continuity. This is a subset of the wider scope of business continuity in ISO 22301 for business continuity management systems.

Similarly, ISO/IEC 27001 controls in A.17 specify activities for business continuity management, with a focus on continuity of information security. These activities include planning, implementing, testing and reviewing information security continuity. This is also a subset of the wider business continuity requirements specified in ISO 22301.

The focus in ISO/IEC 20000-1 and ISO/IEC 27001 is different, but the principles and methodology are similar. Therefore, the two continuity approaches can be considered for integration.

6.3 Information security management specific requirements

Other requirements in ISO/IEC 27001 that do not have a direct match with requirements in ISO/IEC 20000-1 are in Annex A controls. If these controls are applied to a combined scope of an ISMS and an SMS, these include:

a) A.6 organization of information security, including internal organization, mobile devices and teleworking policies;

b) A.7 human resource security, prior to and during employment, as well as around termination and change;

c) A.8 asset management — A.8.1.1 has a relationship but the other controls do not;

d) A.9 access control, including physical and logical access to information systems — A.9.2.2 has a relationship but no other controls;

e) A.10 cryptography;

f) A.11 physical and environmental security for work areas and equipment;

g) A.12 aspects not mentioned before, including malware protection, backup and restore, event logging and monitoring, software and technical vulnerability management — A12.1.2, A.12.1.3 and A.12.1.4 have a relationship but no other controls;

h) A.13 communications security, including network security and information transfer;

i) A.18 compliance, including compliance with legal and contractual requirements, and information security reviews.

6.4 Considerations for the integration of an SMS and an ISMS

The main consideration for the integration of an SMS and an ISMS is the scope: does the ISMS scope include the services provided to the customers and do the assets considered in the ISMS match all assets that are part of the SMS? Depending on the answer to these questions, the integration of the SMS and the ISMS may be more or less complicated.

A second set of considerations is the number of ISO/IEC 27001:2013, Annex A controls adopted in the ISMS: not all controls may be applicable to the scope of the ISMS and therefore not all controls may have been implemented. The controls mentioned in 6.2.4 of this document can all be applied to the scope of an SMS and its services. However, in some organizations, these same controls may only have been applied to the assets of the organization and not to the services.

In summary, the scope applied to the SMS and ISMS and the applied controls determine how much opportunity for integration of the two management systems can be found.

An organization having a risk management process based on ISO/IEC 27001, can use this process to meet the requirements from ISO/IEC 20000-1, which have sufficient similarities in terms of risk impact, risk acceptance criteria, and risk management. The requirements from ISO/IEC 20000-1 alone, however, are not sufficient to meet the requirements from ISO/IEC 27001: a far more detailed risk management process needs to be put into place to meet the requirements of ISO/IEC 27001.

7 Integration of ISO/IEC 20000-1:2018, ISO 9001:2015 and ISO/IEC 27001:2013

7.1 Similarities and differences in requirements between ISO/IEC 20000-1:2018, ISO 9001:2015 and ISO/IEC 27001:2013

Clause 4 of this document has highlighted the common requirements from the ISO/IEC Directives, Part 1, HLS for MSS. Clause 5 focused on further commonalities and differences between ISO/IEC 20000-1 and ISO 9001. Clause 6 focused on further commonalities and differences between ISO/IEC 20000-1 and ISO/IEC 27001.

Table 3 brings all differences and commonalities from these three clauses together, indicating which clauses of ISO/IEC 20000-1 can benefit from input from ISO 9001 and ISO/IEC 27001 respectively. This is done at a high level only, to illustrate how the three standards can be combined. Details can be found in Clauses 4 to 6 and in Annexes B and C of this document.

Table 3 — High-level correlation between ISO/IEC 20000-1:2018, ISO 9001:2015 and ISO/IEC 27001:2013

ISO/IEC 20000-1:2018 clause	ISO 9001:2015 correlation	ISO/IEC 27001:2013 correlation	Comments
4.1 Understanding the organization and its context	Identical HLS requirements. ISO 9001 adds specific requirements.	Identical HLS requirements.	HLS requirements.
4.2 Understanding the needs and expectations of interested parties	Identical HLS requirements. ISO 9001 adds specific requirements.	Identical HLS requirements.	HLS requirements. ISO/IEC 20000-1 adds specific requirements to include services as well as the SMS.

Table 3 *(continued)*

ISO/IEC 20000-1:2018 clause	ISO 9001:2015 correlation	ISO/IEC 27001:2013 correlation	Comments
4.3 Determining the scope of the service management system	Identical HLS requirements, but scope may differ. ISO 9001 adds specific requirements.	Identical HLS requirements, but scope may differ. ISO/IEC 27001 adds specific requirements.	HLS requirements. ISO/IEC 20000-1 adds specific requirements.
4.4 Service management system	Identical HLS requirements. ISO 9001 adds specific requirements.	Identical HLS requirements ISO/IEC 27001 does not include the HLS wording about the processes and their interactions.	HLS requirements.
5.1 Leadership and commitment	Identical HLS requirements. ISO 9001 adds specific requirements.	Identical HLS requirements.	HLS requirements. ISO/IEC 20000-1 adds specific requirements. Some of the additions are to include services as well as the SMS.
5.2 Policy	Identical HLS requirements, but for different policies. ISO 9001 adds specific requirements.	Identical HLS requirements, but for different policies.	HLS requirements. ISO/IEC 20000-1 adds specific requirements to include services as well as the SMS.
5.3 Organizational roles, responsibilities and authorities	Identical HLS requirements. ISO 9001 adds specific requirements.	Identical HLS requirements.	HLS requirements. ISO/IEC 20000-1 adds specific requirements to include services as well as the SMS.
6.1 Actions to address risks and opportunities	Identical HLS requirements. ISO 9001 adds specific requirements.	Identical HLS requirements. The ISO/IEC 27001 additional risk management requirements significantly exceed the ISO/IEC 20000-1 risk management requirements.	HLS requirements. ISO/IEC 20000-1 adds specific requirements. Some of the additions are to include services as well as the SMS.
6.2 Service management objectives and planning to achieve them	Identical HLS requirements, but for different objectives. ISO 9001 adds specific requirements.	Identical HLS requirements, but for different objectives. ISO/IEC 27001 adds specific requirements.	HLS requirements.
6.3 Plan the service management system	No correlation.	No correlation.	Specific to ISO/IEC 20000-1.
7.1 Resources	Identical HLS requirements. ISO/IEC 9001 adds specific requirements. ISO 9001, 7.1.3 can relate to technical resources in ISO/IEC 20000-1.	Identical HLS requirements.	HLS requirements. ISO/IEC 20000-1 adds specific requirements. Some of the additions are to include services as well as the SMS.

Table 3 *(continued)*

ISO/IEC 20000-1:2018 clause	ISO 9001:2015 correlation	ISO/IEC 27001:2013 correlation	Comments
7.2 Competence	Identical HLS requirements.	Identical HLS requirements.	HLS requirements. ISO/IEC 20000-1 adds specific requirements. Some of the additions are to include services as well as the SMS.
7.3 Awareness	Identical HLS requirements.	Identical HLS requirements.	HLS requirements. ISO/IEC 20000-1 adds specific requirements.
7.4 Communication	Identical HLS requirements.	Identical HLS requirements. ISO/IEC 27001 adds specific requirements.	HLS requirements. ISO/IEC 20000-1 adds specific requirements.
7.5 Documented information	Identical HLS requirements. ISO 9001 adds specific requirements. ISO 9001, 4.4 can relate to ISO/IEC 20000-1, 7.5.4.	Identical HLS requirements.	HLS requirements. ISO/IEC 20000-1 adds specific requirements.
7.6 Knowledge	Similar requirements in ISO 9001, 7.1.6.	No correlation.	
8.1 Operational planning and control	Identical HLS requirements. ISO 9001 adds specific requirements.	Identical HLS requirements, but omits the HLS requirement to establish performance criteria.	HLS requirements. ISO/IEC 20000-1 adds specific requirements.
8.2.1 Service delivery	No correlation.	No correlation.	Specific to ISO/IEC 20000-1.
8.2.2 Plan the services	There are some similarities with the gathering of requirements in ISO/IEC 20000-1 from ISO 9001, clauses 8.2.2, 8.2.3, 8.2.4.	No correlation.	
8.2.3 Control of parties involved in the service lifecycle	Similarities in ISO 9001, 8.4.	Similarities in controls A.15.1 and A.14.2.7.	
8.2.4 Service catalogue management	No correlation.	No correlation.	Specific to ISO/IEC 20000-1.
8.2.5 Asset management	No correlation.	Similarities in control A.8.1.1.	
8.2.6 Configuration management	No correlation.	No correlation.	Specific to ISO/IEC 20000-1.
8.3.2 Business relationship management	Similarities in ISO 9001, 5.1.2, 8.2.1 and 9.1.2.	No correlation.	
8.3.3 Service level management	No correlation.	No correlation.	Specific to ISO/IEC 20000-1.
8.3.4 Supplier management	Similarities in ISO 9001, 8.4.	Similarities in control A.15.1.1 and A.15.2.	
8.4.1 Budgeting and accounting for services	No correlation.	No correlation.	Specific to ISO/IEC 20000-1.

Table 3 *(continued)*

ISO/IEC 20000-1:2018 clause	ISO 9001:2015 correlation	ISO/IEC 27001:2013 correlation	Comments
8.4.2 Demand management	No correlation.	No correlation.	Specific to ISO/IEC 20000-1.
8.4.3 Capacity management	No correlation.	Similarities in control A.12.1.3.	
8.5.1 Change management	Similarities in ISO 9001, 6.3, 8.3.6 and 8.5.6	Similarities in controls A.12.1.2, A.14.2.2, A.14.2.3, A.14.2.4 and A.15.2.2.	
8.5.2 Service design and transition	Similarities in ISO 9001, 8.3.	Similarities in controls A.12.1.4, A.14.1.1 and A.14.2.1/5/6/9.	
8.5.3 Release and deployment management	Similarities in ISO 9001, 8.6	Similarities in control A.14.2.	
8.6.1 Incident management	No correlation.	Similarities in control A.16.	
8.6.2 Service request management	No correlation.	Similarities in control A.9.2.2.	
8.6.3 Problem management	No correlation.	Similarities in control A.16.1.6.	
8.7.1 Service availability management	No correlation.	Similarities in control A.17.2.	
8.7.2 Service continuity management	No correlation.	Similarities in control A.17.	
8.7.3 Information security management	No correlation.	Requirements in ISO/IEC 20000-1 are aligned with the more extensive requirements in ISO/IEC 27001, particularly 5.2, 6.1.2, 6.1.3, 8.2, 8.3, A.5.1.1, A.15, A.16.1.	
9.1 Monitoring, measurement, analysis and evaluation	Identical HLS requirements. ISO 9001 adds specific requirements.	Identical HLS requirements. ISO/IEC 27001 adds specific requirements.	HLS requirements. ISO/IEC 20000-1 adds specific requirements. Some of the additions are to include services as well as the SMS.
9.2 Internal audit	Identical HLS requirements. ISO 9001 adds specific requirements.	Identical HLS requirements.	HLS requirements. ISO/IEC 20000-1 adds specific requirements.
9.3 Management review	Identical HLS requirements. ISO 9001 adds specific requirements.	Identical HLS requirements.	HLS requirements. ISO/IEC 20000-1 adds specific requirements. Some of the additions are to include services as well as the SMS.
9.4 Service reporting	No correlation.	No correlation.	Specific to ISO/IEC 20000-1.

Table 3 *(continued)*

ISO/IEC 20000-1:2018 clause	ISO 9001:2015 correlation	ISO/IEC 27001:2013 correlation	Comments
10.1 Nonconformity and corrective action	Identical HLS requirements. ISO 9001 adds specific requirements in 10.2 *Nonconformity and corrective action*.	Identical HLS requirements.	HLS requirements.
10.2 Continual improvement	Identical HLS requirements. ISO 9001 adds specific requirements in 10.1 *General* and 10.3 *Continual Improvement*.	Identical HLS requirements.	HLS requirements. ISO/IEC 20000-1 adds specific requirements. Some of the additions are to include services as well as the SMS.

7.2 Considerations for the integration of an SMS, a QMS and an ISMS

7.2.1 High level structure (HLS)

The purpose of the HLS for MSS is to facilitate integration among various MSS. From Table 3, it can be seen that the correlation is high between the HLS clauses, which makes fulfilment of the requirements between ISO/IEC 20000-1, ISO 9001 and ISO/IEC 27001 easier.

Two aspects should be kept in mind, though, that are related to the scope of the standards.

Some of the requirements apply specifically to a particular standard. For example, the requirements for 4.3 *Scope* and 5.2 *Policy* have some identical elements, but may refer to different things. The scope between the three standards may not be identical and the service, quality, and information security management policies are most likely to be different. Risk management appears common but it must be remembered that each standard has a different focus.

Each of the three standards has added their own small variations to the HLS for MSS text, which will have some impact on fulfilling the requirements jointly. For example, ISO/IEC 20000-1 has in many places added "and the services" to requirements for the SMS. ISO 9001 and ISO/IEC 27001 mostly apply their requirements to only the QMS and ISMS respectively. These additions lead to the organization needing to look carefully at apparently similar clauses.

NOTE In the ISO 33000 series of standards on process assessment, there are process reference models (PRMs) and process assessment models (PAMs) based on ISO/IEC 20000-1, ISO 9001, and ISO/IEC 27001. These PRMs and PAMs have common core processes for MSS which are based on the HLS.

7.2.2 Scope

The main consideration for integrating the three MSS is the exact scope of each. The boundary of the scope of the SMS may or may not be identical to the scope of the QMS or the ISMS for the same organization. The greater the overlap of scopes, the easier it is to develop an integrated management system. If the overlap is more limited, the organization should be very specific about which requirements have been fulfilled for which scope. For example, if the scope of the SMS includes three locations A, B and C, but the scope of the ISMS only applies to two locations A and B, then a high level of integration may be possible for locations A and B but no correlation is possible for location C.

Care should be taken to detail differences between the three scope statements, as this may have an impact on the level of integration that is possible. There are different requirements to describe the scope in the three standards in addition to the boundaries of the organization (all or part). ISO/IEC 20000-1 requires the scope statement to include the services in scope. ISO 9001 requires the types of products and services and justification for any requirements that are not applicable. ISO/IEC 27001 requires simply the organization and its boundaries to be defined. ISO/IEC 27006 requires that the certificate of

conformity references the version of the statement of applicability which lists the information security controls included and excluded.

7.2.3 Service design, build and transition

All three standards have requirements around service design. ISO 9001 has extensive requirements for product and service design in subclauses 8.2 to 8.5 and ISO/IEC 27001 has a set of controls in A.14.2 that focus on development. These two sets of requirements have a limited level of correlation with the requirements in ISO/IEC 20000-1:2018, 8.5.

It may be possible to combine the various service design, build and transition processes to cover requirements from all three standards but this should be considered carefully due to the differences in requirements and scope.

7.2.4 Change management and release and deployment management

All three standards have requirements around change management and release and deployment management. ISO 9001 has only a few requirements for change and release management and ISO/IEC 27001 has a considerable number of controls that can be used in this area. There is a considerable level of correlation between the requirements of the three standards. Therefore, a single integrated process covering the requirements from all three standards may be developed but this should be considered carefully due to the differences in requirements and scope.

7.2.5 Supplier management

Supplier management similarities and differences between ISO/IEC 20000-1, ISO 9001, and ISO/IEC 27001 have been explained in Clauses 5 and 6 of this document. ISO/IEC 27001 has controls in A.15 that can be applied to external suppliers. All three standards also have other requirements for external parties such as considering risks for the use of external parties and ensuring outsourced processes are controlled. The general aim of having control over suppliers is similar in all three standards. Again, an integrated supplier management process, taking the lead from the requirements of ISO/IEC 20000-1 and adding the specific aspects from ISO 9001 and ISO/IEC 27001, may be developed to meet the requirements of the three standards as long as this suits the various scopes. Care should be taken to also recognise the additional supplier management requirements in ISO/IEC 20000-1 for internal suppliers and customers acting as a supplier, which can also apply to the other two standards.

Annex A
(informative)

Correlation of terms and definitions between ISO/IEC 20000-1:2018, ISO 9000:2015, and ISO/IEC 27000:2018

Table A.1 — Correlation of ISO/IEC 20000-1:2018 terms to ISO 9000:2015 and ISO/IEC 27000:2018 terms

ISO/IEC 20000-1:2018		ISO 9000:2015		ISO/IEC 27000:2018	
Entry	**Definition**	**Entry**	**Difference**	**Entry**	**Difference**
3.1.1	**audit** systematic, independent and documented process (3.1.18) for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled Note 1 to entry: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines). Note 2 to entry: An internal audit is conducted by the organization (3.1.14) itself, or by an external party on its behalf. Note 3 to entry: "Audit evidence" and "audit criteria" are defined in ISO 19011.	3.13.1	**audit** Identical definition. See also 3.8.3 **objective evidence**; 3.13.2 **combined audit**; 3.13.3 **joint audit**; 3.13.4 **audit programme**; 3.13.5 **audit scope**; 3.13.6 **audit plan**; 3.13.7 **audit criteria**; 3.13.8 **audit evidence**; 3.13.9 **audit findings**;3.13.10 **audit conclusion**; 3.13.11 **audit client**; 3.13.12 **auditee**; 3.13.13 **guide**; 3.13.14 **audit team**; 3.13.15 **auditor**; 3.13.16 **technical expert**; 3.13.17 **observer**.	3.3	**audit** Identical definition. See also 3.4 **audit scope**.
3.1.2	**competence** ability to apply knowledge and skills to achieve intended results	3.10.4	**competence** Identical definition. See also 3.4.4 **competence acquisition**.	3.9	**competence** Identical definition.
3.1.3	**conformity** fulfilment of a requirement (3.1.19) Note 1 to entry: Conformity relates to requirements in this document as well as the organization's SMS requirements. Note 2 to entry: The original Annex SL definition has been modified by adding note 1.	3.6.11	**conformity** Identical definition.	3.11	**conformity** Identical definition.
3.1.4	**continual improvement** recurring activity to enhance performance (3.1.16)	3.3.2	**continual improvement** Identical definition. See also 3.3.1 **improvement.**	3.13	**continual improvement** Identical definition.
The entries from ISO 9000 and ISO/IEC 27000 are shown without their notes or other commentary. Notes to entries may differ between the three standards. Readers should refer to the respective standards for the full entries. For ISO/IEC 20000-1, terms numbered 3.1.x are common terms from the HLS for MSS and terms numbered 3.2.x are terms specific to service management.					

Table A.1 *(continued)*

ISO/IEC 20000-1:2018		ISO 9000:2015		ISO/IEC 27000:2018	
Entry	**Definition**	**Entry**	**Difference**	**Entry**	**Difference**
3.1.5	**corrective action** action to eliminate the cause or reduce the likelihood of recurrence of a detected nonconformity (3.1.12) or other undesirable situation Note 1 to entry: The original Annex SL definition has been changed. from "action to eliminate the cause of a nonconformity and to prevent recurrence".	3.12.2	**corrective action** action to eliminate the cause of a nonconformity and to prevent recurrence See also 3.12.1 **preventive action**; 3.12.3 **correction**.	3.17	**corrective action** action to eliminate the cause of a nonconformity and to prevent recurrence Also see 3.16 **correction**.
3.1.6	**documented information** information required to be controlled and maintained by an organization (3.1.14) and the medium on which it is contained EXAMPLE Policies (3.1.17), plans, process descriptions, procedures (3.2.11), service level agreements (3.2.20), contracts. Note 1 to entry: Documented information can be in any format and media and from any source. Note 2 to entry: Documented information can refer to: — the management system (3.1.9), including related processes (3.1.18); — information created in order for the organization to operate (documentation); — evidence of results achieved (records (3.2.12)). Note 3 to entry: The original Annex SL definition has been modified by adding examples.	3.8.6	**documented information** Identical definition without the example. Also see 3.8.5 **document**.	3.19	**documented information** Identical definition without the example.
3.1.7	**effectiveness** extent to which planned activities are realized and planned results achieved	3.7.11	**effectiveness** Identical definition.	3.20	**effectiveness** Identical definition.
The entries from ISO 9000 and ISO/IEC 27000 are shown without their notes or other commentary. Notes to entries may differ between the three standards. Readers should refer to the respective standards for the full entries. For ISO/IEC 20000-1, terms numbered 3.1.x are common terms from the HLS for MSS and terms numbered 3.2.x are terms specific to service management.					

Table A.1 *(continued)*

ISO/IEC 20000-1:2018		ISO 9000:2015		ISO/IEC 27000:2018	
Entry	**Definition**	**Entry**	**Difference**	**Entry**	**Difference**
3.1.8	**interested party** person or organization (3.1.14) that can affect, be affected by, or perceive itself to be affected by a decision or activity related to the SMS (3.2.23) or the services (3.2.15) Note 1 to entry: An interested party can be internal or external to the organization. Note 2 to entry: Interested parties can include parts of the organization outside the scope of the SMS, customers (3.2.3), users (3.2.28), community, external suppliers (3.2.4), regulators, public sector bodies, nongovernment organizations, investors or employees. Note 3 to entry: Where interested parties are specified in the requirements (3.1.19) of this document, the interested parties can differ depending on the context of the requirement. Note 4 to entry: The original Annex SL definition has been modified by adding "related to the SMS or the services" and by adding notes 1, 2 and 3.	3.2.3	**interested party** stakeholder person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity	3.37	**interested party** (preferred term) stakeholder (admitted term) person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity
The entries from ISO 9000 and ISO/IEC 27000 are shown without their notes or other commentary. Notes to entries may differ between the three standards. Readers should refer to the respective standards for the full entries. For ISO/IEC 20000-1, terms numbered 3.1.x are common terms from the HLS for MSS and terms numbered 3.2.x are terms specific to service management.					

Table A.1 *(continued)*

ISO/IEC 20000-1:2018		ISO 9000:2015		ISO/IEC 27000:2018	
Entry	**Definition**	**Entry**	**Difference**	**Entry**	**Difference**
3.1.9	**management system** set of interrelated or interacting elements of an organization (3.1.14) to establish policies (3.1.17) and objectives (3.1.13) and processes (3.1.18) to achieve those objectives Note 1 to entry: A management system can address a single discipline or several disciplines. Note 2 to entry: The management system elements include the organization's structure, roles and responsibilities, planning, operation, policies, objectives, plans, processes and procedures (3.2.11). Note 3 to entry: The scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations. Note 4 to entry: The original Annex SL definition has been modified by clarifying that the system is a management system and listing further elements in note 2.	3.5.3	**management system** Identical definition. See also 3.3.3 **management;** 3.5.1 **system**.	3.41	**management system** Identical definition.
3.1.10	**measurement** process (3.1.18) to determine a value	3.11.4	**measurement** Identical definition	3.43	**measurement** Identical definition. See also 3.42 **measure**.
3.1.11	**monitoring** determining the status of a system, a process (3.1.18) or an activity Note 1 to entry: To determine the status there may be a need to check, supervise or critically observe.	3.11.3	**monitoring** Identical definition.	3.46	**monitoring** Identical definition.
The entries from ISO 9000 and ISO/IEC 27000 are shown without their notes or other commentary. Notes to entries may differ between the three standards. Readers should refer to the respective standards for the full entries. For ISO/IEC 20000-1, terms numbered 3.1.x are common terms from the HLS for MSS and terms numbered 3.2.x are terms specific to service management.					

Table A.1 *(continued)*

ISO/IEC 20000-1:2018		ISO 9000:2015		ISO/IEC 27000:2018	
Entry	**Definition**	**Entry**	**Difference**	**Entry**	**Difference**
3.1.12	**nonconformity** non-fulfilment of a requirement (3.1.19) Note 1 to entry: Nonconformity relates to requirements in this document as well as the organization's SMS requirements.	3.6.9	**nonconformity** Identical definition.	3.47	**nonconformity** Identical definition.
3.1.13	**objective** result to be achieved Note 1 to entry: An objective can be strategic, tactical, or operational. Note 2 to entry: Objectives can relate to different disciplines (such as financial, health and safety, service management (3.2.22) and environmental goals) and can apply at different levels (such as strategic, organization-wide, service (3.2.15) project, product and process (3.1.18)). Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as a service management objective or by the use of other words with similar meaning (e.g. aim, goal, or target). Note 4 to entry: In the context of an SMS (3.2.23), service management objectives are set by the organization, consistent with the service management policy (3.1.17), to achieve specific results. Note 5 to entry: The original Annex SL definition has been modified by adding service management and service to note 2.	3.7.1	**objective** Identical definition. See also 3.7.2 **quality objective**.	3.49	**objective** Identical definition.
The entries from ISO 9000 and ISO/IEC 27000 are shown without their notes or other commentary. Notes to entries may differ between the three standards. Readers should refer to the respective standards for the full entries. For ISO/IEC 20000-1, terms numbered 3.1.x are common terms from the HLS for MSS and terms numbered 3.2.x are terms specific to service management.					

Table A.1 *(continued)*

ISO/IEC 20000-1:2018		ISO 9000:2015		ISO/IEC 27000:2018	
Entry	**Definition**	**Entry**	**Difference**	**Entry**	**Difference**
3.1.14	**organization** person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives (3.1.13) Note 1 to entry: The concept of organization includes, but is not limited to sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private. Note 2 to entry: An organization or part of an organization that manages and delivers a service (3.2.15) or services to internal or external customers (3.2.3) can be known as a service provider (3.2.24). Note 3 to entry: If the scope of the SMS (3.2.23) covers only part of an organization, then organization, when used in this standard, refers to the part of the organization that is within the scope of the SMS. Any use of the term organization with a different intent is distinguished clearly. Note 4 to entry: The original Annex SL definition has been modified by adding notes 2 and 3.	3.2.1	**organization** Identical definition. See also 3.2.2 **context of the organization**.	3.50	**organization** Identical definition. See also 3.22 **external context** and 3.38 **internal context**.
3.1.15	**outsource (verb)** make an arrangement where an external organization (3.1.14) performs part of an organization's function or process (3.1.18) Note 1 to entry: An external organization is outside the scope of the SMS (3.2.23), although the outsourced function or process, is within the scope.	3.4.6	**outsource (verb)** Identical definition.	3.51	**outsource (verb)** Identical definition.
The entries from ISO 9000 and ISO/IEC 27000 are shown without their notes or other commentary. Notes to entries may differ between the three standards. Readers should refer to the respective standards for the full entries. For ISO/IEC 20000-1, terms numbered 3.1.x are common terms from the HLS for MSS and terms numbered 3.2.x are terms specific to service management.					

Table A.1 *(continued)*

ISO/IEC 20000-1:2018		ISO 9000:2015		ISO/IEC 27000:2018	
Entry	**Definition**	**Entry**	**Difference**	**Entry**	**Difference**
3.1.16	**performance** measurable result Note 1 to entry: Performance can relate either to quantitative or qualitative findings. Note 2 to entry: Performance can relate to the management of activities, processes (3.1.18), products, services (3.2.15), systems or organizations (3.1.14). Note 3 to entry: The original Annex SL definition has been modified by adding services to note 2.	3.7.8	**performance** Identical definition. See also 3.9.1 **feedback**; 3.9.2 **customer satisfaction**; 3.9.3 **complaint.**	3.52	**performance** Identical definition.
3.1.17	**policy** intentions and direction of an organization (3.1.14) as formally expressed by its top management (3.1.21)	3.5.8	**policy** Identical definition. See also 3.5.9 **quality policy**.	3.53	**policy** Identical definition.
The entries from ISO 9000 and ISO/IEC 27000 are shown without their notes or other commentary. Notes to entries may differ between the three standards. Readers should refer to the respective standards for the full entries. For ISO/IEC 20000-1, terms numbered 3.1.x are common terms from the HLS for MSS and terms numbered 3.2.x are terms specific to service management.					

Table A.1 *(continued)*

ISO/IEC 20000-1:2018		ISO 9000:2015		ISO/IEC 27000:2018	
Entry	**Definition**	**Entry**	**Difference**	**Entry**	**Difference**
3.1.18	**process** set of interrelated or interacting activities that use inputs to deliver an intended result Note 1 to entry: Whether the "intended result" of a process is called output, product or service (3.2.15) depends on the context of the reference. Note 2 to entry: Inputs to a process are generally the outputs of other processes and outputs of a process are generally the inputs to other processes. Note 3 to entry: Two or more interrelated and interacting processes in series can also be referred to as a process. Note 4 to entry: Processes in an organization (3.1.14) are generally planned and carried out under controlled conditions to add value. Note 5 to entry: The original Annex SL definition has been changed from "set of interrelated or interacting activities which transforms inputs into outputs". The original Annex SL definition has also been modified by adding notes 1 - 4. The revised definition and notes 1 - 4 are sourced from ISO 9000:2015.	3.4.1	**process** Identical definition. See also 3.7.5 **output**.	3.54	**process** set of interrelated or interacting activities which transforms inputs into outputs
The entries from ISO 9000 and ISO/IEC 27000 are shown without their notes or other commentary. Notes to entries may differ between the three standards. Readers should refer to the respective standards for the full entries. For ISO/IEC 20000-1, terms numbered 3.1.x are common terms from the HLS for MSS and terms numbered 3.2.x are terms specific to service management.					

Table A.1 *(continued)*

ISO/IEC 20000-1:2018		ISO 9000:2015		ISO/IEC 27000:2018	
Entry	**Definition**	**Entry**	**Difference**	**Entry**	**Difference**
3.1.19	**requirement** need or expectation that is stated, generally implied or obligatory Note 1 to entry: "Generally implied" means that it is custom or common practice for the organization (3.1.14) and interested parties (3.1.8) that the need or expectation under consideration is implied. Note 2 to entry: A specified requirement is one that is stated, for example, in documented information (3.1.6). Note 3 to entry: In the context of an SMS (3.2.23), service requirements (3.2.26) are documented and agreed rather than generally implied. There can also be other requirements such as legal and regulatory requirements. Note 4 to entry: The original Annex SL definition has been modified by adding note 3.	3.6.4	**requirement** Identical definition.	3.56	**requirement** Identical definition.
The entries from ISO 9000 and ISO/IEC 27000 are shown without their notes or other commentary. Notes to entries may differ between the three standards. Readers should refer to the respective standards for the full entries. For ISO/IEC 20000-1, terms numbered 3.1.x are common terms from the HLS for MSS and terms numbered 3.2.x are terms specific to service management.					

Table A.1 *(continued)*

ISO/IEC 20000-1:2018		ISO 9000:2015		ISO/IEC 27000:2018	
Entry	**Definition**	**Entry**	**Difference**	**Entry**	**Difference**
3.1.20	**risk** effect of uncertainty Note 1 to entry: An effect is a deviation from the expected — positive or negative. Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to understanding or knowledge of, an event, its consequence, or likelihood. Note 3 to entry: Risk is often characterized by reference to potential events (as defined in ISO Guide 73:2009, 3.5.1.3) and consequences (as defined in ISO Guide 73:2009, 3.6.1.3), or a combination of these. Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood (as defined in ISO Guide 73:2009, 3.6.1.1) of occurrence.	3.7.9	**risk** Identical definition.	3.61	**risk** effect of uncertainty *on objectives* See also 3.12 **consequence**; 3.14 **control**; 3.39 **level of risk**; 3.40 **likelihood**; 3.57 **residual risk**; 3.62 **risk acceptance**; 3.63 **risk analysis**; 3.64 **risk assessment**; 3.65 **risk communication and consultation**; 3.66 **risk criteria**; 3.67 **risk evaluation**; 3.68 **risk identification**; 3.69 **risk management**; 3.70 **risk management process**; 3.71 **risk owner**; 3.72 **risk treatment;** 3.74 **threat;** 3.77 **vulnerability**.
3.1.21	**top management** person or group of people who directs and controls an organization (3.1.14) at the highest level Note 1 to entry: Top management has the power to delegate authority and provide resources within the organization. Note 2 to entry: If the scope of the management system (3.1.9) covers only part of an organization then top management refers to those who direct and control that part of the organization.	3.1.1	**top management** Identical definition.	3.75	**top management** Identical definition.
The entries from ISO 9000 and ISO/IEC 27000 are shown without their notes or other commentary. Notes to entries may differ between the three standards. Readers should refer to the respective standards for the full entries. For ISO/IEC 20000-1, terms numbered 3.1.x are common terms from the HLS for MSS and terms numbered 3.2.x are terms specific to service management.					

Table A.1 *(continued)*

ISO/IEC 20000-1:2018		ISO 9000:2015		ISO/IEC 27000:2018	
Entry	**Definition**	**Entry**	**Difference**	**Entry**	**Difference**
3.2.1	**asset** item, thing, or entity that has potential or actual value to an organization (3.1.14) Note 1 to entry: Value can be tangible or intangible, financial or non-financial, and includes consideration of risks (3.1.20) and liabilities. It can be positive or negative at different stages of the asset life. Note 2 to entry: Physical assets usually refer to equipment, inventory and properties owned by the organization. Physical assets are the opposite of intangible assets, which are non-physical assets such as leases, brands, digital assets, use rights, licences, intellectual property rights, reputation or agreements. Note 3 to entry: A grouping of assets referred to as an asset system could also be considered as an asset. Note 4 to entry: An asset can also be a configuration item (3.2.2). Some configuration items are not assets. [SOURCE: ISO/IEC 19770-5:2015, 3.2, modified — Note 4 to entry contains new content.]		Not defined		Not defined
3.2.2	**configuration item** CI element that needs to be controlled in order to deliver a service (3.2.15) or services	3.10.6	**configuration** interrelated functional and physical characteristics of a product or service defined in product configuration information		Not defined
The entries from ISO 9000 and ISO/IEC 27000 are shown without their notes or other commentary. Notes to entries may differ between the three standards. Readers should refer to the respective standards for the full entries. For ISO/IEC 20000-1, terms numbered 3.1.x are common terms from the HLS for MSS and terms numbered 3.2.x are terms specific to service management.					

Table A.1 *(continued)*

ISO/IEC 20000-1:2018		ISO 9000:2015		ISO/IEC 27000:2018	
Entry	**Definition**	**Entry**	**Difference**	**Entry**	**Difference**
		3.3.13	**configuration object** object within a configuration that satisfies an end-use function. See also 3.1.5 **configuration authority**; 3.3.9 **configuration management**; 3.6.8 **product configuration information**; 3.8.14 **configuration status accounting**; 3.10.7 **configuration baseline**.		
3.2.3	**customer** organization (3.1.14) or part of an organization that receives a service (3.2.15) or services EXAMPLE Consumer, client, beneficiary, sponsor or purchaser. Note 1 to entry: A customer can be internal or external to the organization delivering the service or services. Note 2 to entry: A customer can also be a user (3.2.28). A customer can also act as a supplier.	3.2.4	**customer** person or organization that could or does receive a product or a service that is intended for or required by this person or organization EXAMPLE Consumer, client, end-user, retailer, receiver of product or service from an internal process, beneficiary and purchaser.		Not defined
3.2.4	**external supplier** another party that is external to the organization that enters into a contract to contribute to the planning, design, transition (3.2.27), delivery or improvement of a service (3.2.15), service component (3.2.18) or process (3.1.18) Note 1 to entry: External suppliers include designated lead suppliers but not their sub-contracted suppliers. Note 2 to entry: If the organization in the scope of the SMS is part of a larger organization, the other party is external to the larger organization.	3.2.6 3.2.5	**external provider** external supplier provider that is not part of the organization **provider** supplier organization that provides a product or a service See also 3.4.7 **contract**.		Not defined
The entries from ISO 9000 and ISO/IEC 27000 are shown without their notes or other commentary. Notes to entries may differ between the three standards. Readers should refer to the respective standards for the full entries. For ISO/IEC 20000-1, terms numbered 3.1.x are common terms from the HLS for MSS and terms numbered 3.2.x are terms specific to service management.					

Table A.1 *(continued)*

ISO/IEC 20000-1:2018		ISO 9000:2015		ISO/IEC 27000:2018	
Entry	**Definition**	**Entry**	**Difference**	**Entry**	**Difference**
3.2.5	**incident** unplanned interruption to a service (3.2.15), a reduction in the quality of a service or an event that has not yet impacted the service to the customer (3.2.3) or users (3.2.28)		Not defined		Not defined See 3.31 **information security incident**.
3.2.6	**information security** preservation of confidentiality, integrity and availability of information Note 1 to entry: In addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved. [SOURCE: ISO/IEC 27000:2018]		Not defined	3.28	**information security** Identical definition. See also 3.6 **authenticity;** 3.7 **availability;** 3.10 **confidentiality**; 3.36 **integrity**; 3.48 **non-repudiation;** 3.55 **reliability**.
3.2.7	**information security incident** single or a series of unwanted or unexpected information security (3.2.6) events that have a significant probability of compromising business operations and threatening information security [SOURCE: ISO/IEC 27000:2018]		Not defined	3.31	**information security incident** Identical definition. See also 3.21 **event**; 3.30 **information security event**; 3.32 **information security incident management**.
3.2.8	**internal supplier** part of a larger organization (3.1.14) that is outside the scope of the SMS (3.2.23) that enters into a documented agreement to contribute to the planning, design, transition (3.2.27), delivery or improvement of a service (3.2.15), service component (3.2.18) or process (3.1.18) Note 1 to entry: The internal supplier and the organization in the scope of the SMS are both part of the same larger organization. EXAMPLE Procurement, infrastructure, finance, human resources, facilities.	3.2.5	**provider** supplier organization that provides a product or a service EXAMPLE Producer, distributor, retailer or vendor of a product or a service.		Not defined
The entries from ISO 9000 and ISO/IEC 27000 are shown without their notes or other commentary. Notes to entries may differ between the three standards. Readers should refer to the respective standards for the full entries. For ISO/IEC 20000-1, terms numbered 3.1.x are common terms from the HLS for MSS and terms numbered 3.2.x are terms specific to service management.					

Table A.1 *(continued)*

ISO/IEC 20000-1:2018		ISO 9000:2015		ISO/IEC 27000:2018	
Entry	**Definition**	**Entry**	**Difference**	**Entry**	**Difference**
3.2.9	**known error** problem (3.2.10) that has an identified root cause or a method of reducing or eliminating its impact on a service (3.2.15)		Not defined		Not defined
3.2.10	**problem** cause of one or more actual or potential incidents (3.2.5)		Not defined		Not defined
3.2.11	**procedure** specified way to carry out an activity or a process (3.1.18) Note 1 to entry: Procedures can be documented or not. [SOURCE: ISO 9000:2015, 3.4.5]	3.4.5	Identical definition.		Not defined
3.2.12	**record** document stating results achieved or providing evidence of activities performed EXAMPLE Audit (3.1.1) reports, incident (3.2.5) details, list of training delegates, minutes of meetings. Note 1 to entry: Records can be used, for example, to formalize traceability and to provide evidence of verification, preventive action and corrective action (3.1.5). Note 2 to entry: Generally, records need not be under revision control. [SOURCE: ISO 9000:2015]	3.8.10	Identical definition.		Not defined
3.2.13	**release (noun)** collection of one or more new or changed services (3.2.15) or service components (3.2.18) deployed into the live environment as a result of one or more changes	3.12.7	**Release** permission to proceed to the next stage of a process or the next process		Not defined
The entries from ISO 9000 and ISO/IEC 27000 are shown without their notes or other commentary. Notes to entries may differ between the three standards. Readers should refer to the respective standards for the full entries. For ISO/IEC 20000-1, terms numbered 3.1.x are common terms from the HLS for MSS and terms numbered 3.2.x are terms specific to service management.					

Table A.1 *(continued)*

ISO/IEC 20000-1:2018		ISO 9000:2015		ISO/IEC 27000:2018	
Entry	**Definition**	**Entry**	**Difference**	**Entry**	**Difference**
3.2.14	**request for change** proposal for a change to be made to a service (3.2.15), service component (3.2.18) or the SMS (3.2.23) Note 1 to entry: A change to a service includes the provision of a new service, transfer of a service or the removal of a service that is no longer required.	3.3.10	**Change control** <configuration management> activities for control of the output after formal approval of its product configuration information See also 3.6.8 **product configuration information**		Not defined
3.2.15	**service** means of delivering value for the customer (3.2.3) by facilitating outcomes the customer wants to achieve Note 1 to entry: Service is generally intangible. Note 2 to entry: The term service as used in this document means the service or services in the scope of the SMS (3.2.23). Any use of the term service with a different intent is distinguished clearly.	3.7.7	**service** output of an organization with at least one activity necessarily performed between the organization and the customer Also see 3.7.6 **product**; 3.9.4 **customer service**.		Not defined
3.2.16	**service availability** ability of a service (3.2.15) or service component (3.2.18) to perform its required function at an agreed time or over an agreed period of time Note 1 to entry: Service availability can be expressed as a ratio or percentage of the time that the service or service component is actually available for use compared to the agreed time.		Not defined	3.7	**availability** property of being accessible and usable on demand by an authorized entity
3.2.17	**service catalogue** documented information about services that an organization provides to its customers		Not defined		Not defined
The entries from ISO 9000 and ISO/IEC 27000 are shown without their notes or other commentary. Notes to entries may differ between the three standards. Readers should refer to the respective standards for the full entries. For ISO/IEC 20000-1, terms numbered 3.1.x are common terms from the HLS for MSS and terms numbered 3.2.x are terms specific to service management.					

Table A.1 *(continued)*

ISO/IEC 20000-1:2018		ISO 9000:2015		ISO/IEC 27000:2018	
Entry	**Definition**	**Entry**	**Difference**	**Entry**	**Difference**
3.2.18	**service component** part of a service (3.2.15) that when combined with other elements will deliver a complete service Note 1 to entry: A service component can include configuration items (3.2.2), assets (3.2.1) or other elements. EXAMPLE Infrastructure, applications, documentation, licences, information, resources or supporting services.		Not defined		Not defined
3.2.19	**service continuity** capability to deliver a service (3.2.15) without interruption, or with consistent availability as agreed Note 1 to entry: Service continuity management can be a subset of business continuity management. ISO 22301 provides requirements (3.1.19) for business continuity management.		Not defined	3.29	**information security continuity** processes and procedures for ensuring continued information security operations
3.2.20	**service level agreement** SLA documented agreement between the organization (3.1.14) and the customer (3.2.3) that identifies services (3.2.15) and their agreed performance Note 1 to entry: A service level agreement can also be established between the organization and an external supplier (3.2.4), an internal supplier (3.2.8) or a customer acting as a supplier. Note 2 to entry: A service level agreement can be included in a contract or another type of documented agreement.		Not defined		Not defined
3.2.21	**service level target** specific measurable characteristic of a service (3.2.15) that an organization (3.1.14) commits to		Not defined		Not defined

The entries from ISO 9000 and ISO/IEC 27000 are shown without their notes or other commentary. Notes to entries may differ between the three standards. Readers should refer to the respective standards for the full entries.

For ISO/IEC 20000-1, terms numbered 3.1.x are common terms from the HLS for MSS and terms numbered 3.2.x are terms specific to service management.

Table A.1 *(continued)*

ISO/IEC 20000-1:2018		ISO 9000:2015		ISO/IEC 27000:2018	
Entry	**Definition**	**Entry**	**Difference**	**Entry**	**Difference**
3.2.22	**service management** set of capabilities and processes (3.1.18) to direct and control the organization's (3.1.14) activities and resources for the planning, design, transition (3.2.27), delivery and improvement of services (3.2.15) to deliver value (3.2.29) Note 1 to entry: This document provides a set of requirements which is split into clauses and sub-clauses. Each organization can choose how to combine the requirements into processes. The sub-clauses can be used to define the processes of the organization's SMS.	3.3.4	**quality management** management with regard to quality		Not defined
3.2.23	**service management system** management system (3.1.9) to direct and control the service management (3.2.22) activities of the organization (3.1.14) Note 1 to entry: An SMS includes service management policies (3.1.17), objectives (3.1.13), plans, processes (3.1.18), documented information and resources required for the planning, design, transition (3.2.27), delivery and improvement of services to meet the requirements (3.1.19) specified in this document.	3.5.4	**quality management system** part of a management system with regard to quality		Not defined
3.2.24	**service provider** organization (3.1.14) that manages and delivers a service (3.2.15) or services to customers (3.2.3)		Not defined		Not defined
3.2.25	**service request** request for information, advice, access to a service (3.2.15) or a pre-approved change		Not defined		Not defined
The entries from ISO 9000 and ISO/IEC 27000 are shown without their notes or other commentary. Notes to entries may differ between the three standards. Readers should refer to the respective standards for the full entries. For ISO/IEC 20000-1, terms numbered 3.1.x are common terms from the HLS for MSS and terms numbered 3.2.x are terms specific to service management.					

Table A.1 *(continued)*

ISO/IEC 20000-1:2018		ISO 9000:2015		ISO/IEC 27000:2018	
Entry	**Definition**	**Entry**	**Difference**	**Entry**	**Difference**
3.2.26	**service requirement** needs of customers (3.2.3), users (3.2.28) and the organization (3.1.14) related to the services (3.2.15) and the SMS (3.2.23) that are stated or obligatory Note 1 to entry: In the context of an SMS (3.2.23), service requirements are documented and agreed rather than generally implied. There can also be other requirements such as legal and regulatory requirements.	3.6.5	**quality requirement** requirement related to quality See also 3.6.2 **quality**; 3.6.6 **statutory request**; 3.6.7 **regulatory requirement**.		Not defined
3.2.27	**transition** activities involved in moving a new or changed service (3.2.15) to or from the live environment		Not defined		Not defined
3.2.28	**user** individual or group that interacts with or benefits from a service (3.2.15) or services Note 1 to entry: Examples of users include a person or community of people. A customer (3.2.3) can also be a user.		Not defined		Not defined
3.2.29	**value** importance, benefit or usefulness Note 1 to entry: The creation of value from services (3.2.15) includes realizing benefits at an optimal resource level while managing risk (3.35). An asset (3.2.1) and a service (3.2.15) are examples that can be assigned a value. EXAMPLE Monetary value, achieving service outcomes, achieving service management (3.2.22) objectives (3.1.13), customer retention or removal of constraints.		Not defined		Not defined
The entries from ISO 9000 and ISO/IEC 27000 are shown without their notes or other commentary. Notes to entries may differ between the three standards. Readers should refer to the respective standards for the full entries. For ISO/IEC 20000-1, terms numbered 3.1.x are common terms from the HLS for MSS and terms numbered 3.2.x are terms specific to service management.					

Annex B
(informative)

Correlation of ISO/IEC 20000-1:2018 to ISO 9001:2015

Table B.1 — Correlation of ISO/IEC 20000-1:2018 to ISO 9001:2015

ISO/IEC 20000-1:2018		ISO 9001:2015		Correlation notes
	Introduction		**Introduction**	Specific to each standard
1	**Scope**	**1**	**Scope**	Specific to each standard
2	**Normative references**	**2**	**Normative references**	Specific to each standard
3	**Terms and definitions**	**3**	**Terms and definitions**	Specific to each standard
4	**Context of the organization**	**4**	**Context of the organization**	
4.1	Understanding the organization and its context	4.1	Understanding the organization and its context	Similar requirements based on the HLS. ISO 20000-1 includes determining the external and internal issues that affect its ability to achieve the intended outcome(s) of its SMS whereas ISO 9001 includes determining the external and internal issues that are relevant to the organization's strategic direction and that affect its ability to achieve the intended results of the QMS. ISO 9001 adds a requirement to monitor and review information about issues.
4.2	Understanding the needs and expectations of interested parties	4.2	Understanding the needs and expectations of interested parties	Identical HLS requirements. ISO/IEC 20000-1 includes determining the interested parties that are relevant to the SMS and the services. ISO 9001 includes determining the interested parties that are relevant to the QMS due to their effect or potential effect on the organization's ability to consistently provide products and services that meet customer and applicable statutory and regulatory requirements. ISO 9001 also adds a requirement to monitor and review the needs and expectations of interested parties which is covered in Clause 9 in ISO/IEC 20000-1.

Table B.1 *(continued)*

ISO/IEC 20000-1:2018		ISO 9001:2015		Correlation notes
4.3	Determining the scope of the service management system	4.3	Determining the scope of the quality management system	Identical HLS requirements. The scope in ISO 9001 includes the products and services of the organization. ISO/IEC 20000-1 specifies that the definition of the scope of the SMS shall include the services in scope and the name of the organization managing and delivering the services. ISO/IEC 20000-1 includes a note that ISO/IEC 20000-3 provides guidance on scope definition and a note on the SMS scope definition for services. For ISO 9001 an organization can state requirements that are not applicable to the scope of the QMS if these do not affect the organization's ability or responsibility to ensure the conformity of its products or services and the enhancement of customer satisfaction. In ISO/IEC 20000-1, Clause 1.2 *Application* states that exclusions of any of the requirements in Clause 4 to 10 are not acceptable.
4.4	Service management system	4.4	Quality management system and its processes	Identical HLS requirements. ISO 9001 adds requirements for process design and documentation in the QMS and maintenance of this documented information.
5	**Leadership**	**5**	**Leadership**	
5.1	Leadership and commitment	5.1	Leadership and commitment	Identical HLS requirements. ISO/IEC 20000-1 adds requirements for leadership to ensure the service management
		5.1.1	General	
		5.1.2	Customer focus	
5.2	**Policy**	**5.2**	**Policy**	
5.2.1	Establishing the service management policy	5.2.1	Establishing the quality policy	Identical HLS requirements. ISO/IEC 20000-1 adds specific requirements to ensure continual improvement also applies to the services.
5.2.2	Communicating the service management policy	5.2.2	Communicating the quality policy	Identical HLS requirements ISO 9001 adds that the policy is not only communicated but also understood and applied.

Table B.1 *(continued)*

ISO/IEC 20000-1:2018		ISO 9001:2015		Correlation notes
5.3	Organizational roles, responsibilities and authorities	5.3	Organizational roles, responsibilities and authorities	Identical HLS requirements. ISO 9001 adds requirements for top management to ensure processes deliver their outputs, customer focus is maintained and QMS integrity is maintained. ISO/IEC 20000-1 adds specific requirements to ensure authorities and responsibilities also apply to the services.
6	**Planning**	**6**	**Planning**	
6.1	Actions to address risks and opportunities	6.1	Actions to address risks and opportunities	Identical HLS requirements. ISO 9001 adds a requirement to 6.1 to determine risks that need to be addressed to enhance desirable effects. ISO/IEC 20000-1 adds clause 6.1.2 on determining and documenting risks, the impact of risks, risk acceptance criteria and risk management approach.
6.2	**Service management objectives and planning to achieve them**	**6.2**	**Quality objectives and planning to achieve them**	
6.2.1	Establish objectives	6.2.1		Identical HLS requirements ISO 9001 adds that the quality objectives be relevant to conformity of products and services and to enhancement of customer satisfaction. ISO/IEC 20000-1 has removed 'if practicable' from the need for objectives to be measurable in 6.2.1.
6.2.2	Plan to achieve objectives	6.2.2		Identical HLS requirements
6.3	Plan the service management system			Specific to ISO/IEC 20000-1

Table B.1 *(continued)*

ISO/IEC 20000-1:2018		ISO 9001:2015		Correlation notes
7	**Support**	**7**	**Support**	
7.1	Resources	7.1	Resources	Similar requirements to ISO/IEC 20000-1, 7.1. ISO 9001 adds a requirement in 7.1.1 to consider capabilities, constraints and external resources. ISO/IEC 20000-1 refers to human, technical, financial and information resources, applying these to the SMS and the services to meet service requirements and achieve service management objectives. ISO 9001 adds clauses for people, infrastructure, environment for operation of the services, monitoring and measuring resources, and organizational knowledge. ISO 9001, 7.1.3 Infrastructure has requirements related to what ISO/IEC 20000-1 refers to as technical resources.
7.2	Competence	7.2	Competence	Identical HLS requirements. ISO/IEC 20000-1 adds specific requirements to ensure competence is relevant to both the SMS and the services.
7.3	Awareness	7.3	Awareness	Identical HLS requirements. ISO/IEC 20000-1 adds service management objectives and the services relevant to their work as objects of awareness.
7.4	Communication	7.4	Communication	Identical HLS requirements. ISO/IEC 20000-1 adds requirements to determine communication for the SMS and also the services.
7.5	**Documented Information**	**7.5**	**Documented Information**	
7.5.1	General	7.5.1	General	Identical HLS requirements
7.5.2	Creating and updating documented information	7.5.2	Creating and updating	Identical HLS requirements
7.5.3	Control of documented information	7.5.3	Control of documented information	Identical HLS requirements ISO 9001 adds a requirement for documented information retained as evidence of conformity to be protected from unintended alterations

Table B.1 *(continued)*

ISO/IEC 20000-1:2018		ISO 9001:2015		Correlation notes
7.5.4	Service management system documented information	4.4	Quality management system and its processes	Similar to ISO 9001, 4.4, which requires that documented information is maintained to support the operation of the processes.
7.6	Knowledge	7.1.6	Organizational knowledge	Similar to ISO 9001, 7.1.6 which has more requirements for knowledge than ISO/IEC 20000-1, including acquiring additional knowledge and determining sources of knowledge.
8	**Operation**	**8**	**Operation**	
8.1	Operational planning and control	8.1	Operational planning and control	Identical HLS requirements. ISO 9001 adds determining the requirements for the products and services, criteria for the acceptance of products and services, determining the resources needed to achieve conformity to the product and service requirements, using documented information to demonstrate the conformity of products and services to their requirements and the output being suitable for the organization's operations. ISO/IEC 20000-1 emphasises performance criteria and also specifies planned changes are for the SMS.
8.2	**Service portfolio**			
8.2.1	Service delivery			Specific to ISO/IEC 20000-1
8.2.2	Plan the services	8.2.2 8.2.3 8.2.4	Determining the requirements for products and services Review of the requirements for products and services Changes to requirements for products and services	There are some similarities with the gathering of requirements in ISO/IEC 20000-1 from ISO 9001, 8.2.2, 8.2.3, and 8.2.4.
8.2.3	Control of parties involved in the service lifecycle	8.4	Control of externally provided processes, products and services	Similarities in ISO 9001, 8.4.
8.2.4	Service catalogue management			Specific to ISO/IEC 20000-1
8.2.5	Asset management			Specific to ISO/IEC 20000-1
8.2.6	Configuration management			Specific to ISO/IEC 20000-1
8.3	**Relationship and agreement**			
8.3.1	General			Specific to ISO/IEC 20000-1

Table B.1 *(continued)*

ISO/IEC 20000-1:2018		ISO 9001:2015		Correlation notes
8.3.2	Business relationship management	5.1.2 8.2.1 9.1.2	Customer focus Customer communication Customer satisfaction	ISO 9001, 5.1.2 is about customer focus which is covered in this clause. ISO 9001, 8.2.1 has some requirements related to complaints similar to this clause. ISO 9001, 9.1.2 has some requirements similar to this clause.
8.3.3	Service level management			Specific to ISO/IEC 20000-1
8.3.4	Supplier management			
8.3.4.1	Management of external suppliers	8.4	Control of externally provided processes, products and services	There are some similarities with ISO 9001, 8.4 and ISO/IEC 20000-1, 8.2.3 *Control of parties involved in the service lifecycle* as well as 8.3.4 *Supplier management*– see discussion on external suppliers in section 5.
8.3.4.2	Management of internal suppliers and customers acting as a supplier			Specific to ISO/IEC 20000-1
8.4	**Supply and demand**			
8.4.1	Budgeting and accounting for services			Specific to ISO/IEC 20000-1.
8.4.2	Demand management			Specific to ISO/IEC 20000-1.
8.4.3	Capacity management			Specific to ISO/IEC 20000-1.
8.5	**Service design, build and transition**			
8.5.1	Change management	6.3	Planning of changes	There are some similarities with ISO 9001, 6.3.
		8.3.6	Design and development changes	ISO 9001, 8.3.6 requires that changes during, or after, the design and development needs to be determined, reviewed, authorized and with action to prevent adverse impacts.
		8.5.6	Control of changes	ISO 9001, 8.5.6 requires changes for production or service provision needs to be reviewed and authorized. ISO/IEC 20000-1, 8.5.1 Change Management has an extensive set of requirements, change management policy, change management initiation and activities.
8.5.2	Service design and transition	8.3	Design and development of products and services	There are some similarities between requirements in ISO 9001, 8.3 and ISO/IEC 20000-1, 8.5.2 – see discussion on service design, build and transition in Section 5.
8.5.3	Release and deployment management	8.6	Release of products and services	There are some similarities with ISO 9001, 8.6.
8.6	**Resolution and fulfilment**			
8.6.1	Incident management			Specific to ISO/IEC 20000-1.
8.6.2	Service request management			Specific to ISO/IEC 20000-1.