Technical Report

ISO/IEC TR 20000-17

First edition
2024-10

Information technology — Service management —

Part 17: Scenarios for the practical application of service management systems based on ISO/IEC 20000-1:2018

Technologies de l'information — Gestion des services —

Partie 17: Scénarios pour l'application pratique des systèmes de gestion des services sur la base de l'ISO/IEC 20000-1:2018

Reference number
ISO/IEC TR 20000-17:2024(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

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

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

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

This document provides scenarios, explanations and examples for the practical application of service management systems (SMS) based on ISO/IEC 20000-1:2018.

These scenarios have arisen from comments resulting from the practical usage of ISO/IEC 20000-1:2018 over the years since its publication. These comments provided evidence of apparent misconceptions and a lack of knowledge about how ISO/IEC 20000-1:2018 and an SMS can be applied.

This document aims to support users of ISO/IEC 20000-1:2018 in its application to establish and improve an SMS using examples of practical situations. The list of scenario-based examples in this document is not exhaustive and other scenarios are possible.

Information technology — Service management —

Part 17: Scenarios for the practical application of service management systems based on ISO/IEC 20000-1:2018

1 Scope

This document provides scenarios, explanations and examples for the practical application of service management systems (SMS) based on ISO/IEC 20000-1:2018. These scenarios provide examples of situations in which an SMS can be used and how the requirements of ISO/IEC 20000-1:2018 can be applied.

This document can be used with ISO/IEC 20000-1 as well as with ISO/IEC 20000-2, ISO/IEC 20000-3, ISO/IEC TS 20000-5 and other parts of the ISO/IEC 20000 series.

This document is aimed at:

a) organizations that are intending to implement an SMS based on the requirements of ISO/IEC 20000-1;

b) organizations that have already implemented an SMS based on the requirements of ISO/IEC 20000-1;

c) consultants, trainers and other experts supporting these organizations.

This document does not add to, change or replace any of the requirements in ISO/IEC 20000-1. This document is not intended to be used for a conformity assessment.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

ISO/IEC 20000-10, *Information technology — Service management — Part 10: Concepts and vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 20000-1 and ISO/IEC 20000-10 apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

4 Overview of 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 in the field of information technology (IT), business process outsourcing or facilities management. While ISO/IEC 20000-1 can be used "regardless of the organization's type or size, or the nature of the services delivered", ISO/IEC 20000-1 has its roots in IT. It is intended for service management of services using technology and digital information. The examples given in this document illustrate a variety of uses of ISO/IEC 20000-1.

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, such as suppliers, are used to provide or operate all services, all service components or all processes within the scope of the SMS.

Figure 1 illustrates an SMS showing the clause content of ISO/IEC 20000-1. Numbers in parentheses in Figure 1 indicate ISO/IEC 20000-1 clause numbers.

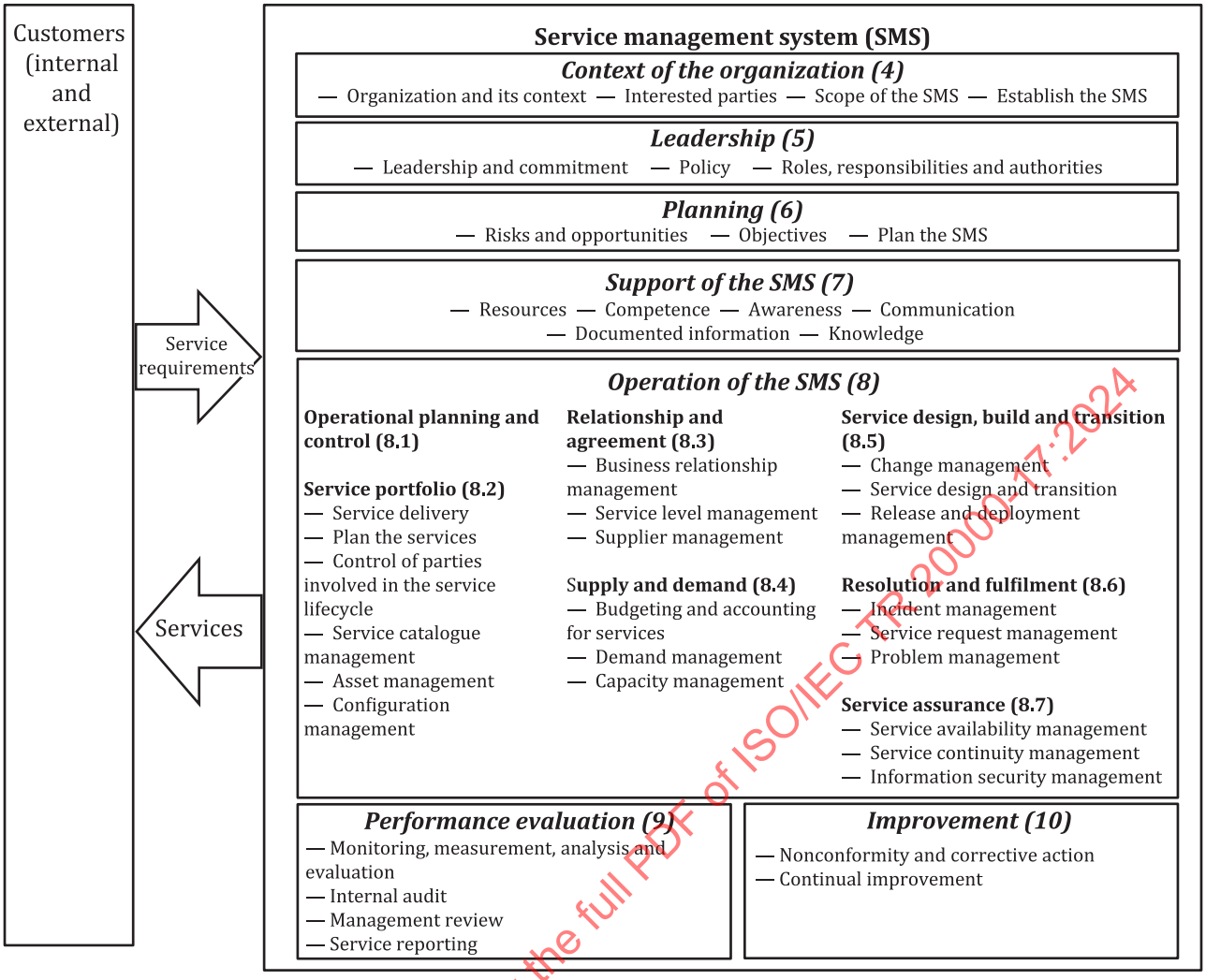

Figure 1 — Service management system

5 Scenario-based examples

5.1 Introduction to the scenarios

The scenarios, explanation and examples listed in this document are many and varied. Some are complex and some are simple. Some relate to a single clause and others relate to multiple clauses in ISO/IEC 20000-1.

Each scenario has a title in the form of a question and an introduction. It is followed by explanation and examples of how this scenario can be applied within an SMS. The relevant clause numbers of ISO/IEC 20000-1 at their lowest level are also shown. All clause numbers include their subclauses. See Annex A for a list of the ISO/IEC 20000-1 clause numbers and titles.

5.2 What types of services can be used with ISO/IEC 20000-1?

Requirements for services contained in ISO/IEC 20000-1 are independent of service size, type, location or characteristics and therefore can be applied to all services defined in an organization's SMS. Services provided by organizations that are managed in an SMS can have a variety of configurations. They can be simple services or bundled services, depending on the needs of the customers. In addition, many services and their components are a combination of internally provided and externally provided services. See Table 1.

Table 1 — Using ISO/IEC 20000-1 for different types of services

Topic	ISO/IEC 20000-1:2018 clause number
Can ISO/IEC 20000-1 be used with micro, aggregated, centralized, decentralized or distributed services? The requirements in ISO/IEC 20000-1 for managing services through an effective SMS apply to all types of services regardless of their configuration, size or complexity, or whether they are provided by internal or external service providers. A service can be provided, supported and consumed from any location. Whether a service is micro, aggregated, centralized, decentralized or distributed, it is critical for each service component to be defined and documented for planning, implementing, maintaining, improvement and retirement purposes. Examples of micro, aggregated, centralized, decentralized and distributed services are: — micro: the "buy" button when purchasing a product online; — aggregated: an online banking service where all accounts for one user can be accessed from one page; — centralized: a centralized IT network where all users connect to a single central server; — decentralized: customers receive energy supplies from multiple sources; — distributed: mobile phone networks which use multiple base stations to provide connectivity. Although all clauses are relevant to operating, supporting, measuring and improving the services defined in the SMS, of significance is configuration management and its requirements to define services as configuration items (CIs). Each service is comprised of multiple CIs which can include other internally or externally provided services, technical components, service support groups, service consumer groups, facilities and documentation. Once services have been defined in the SMS, their configurations and CI relationships can be defined as well. This ensures that if there is an addition, modification or removal of any service within the SMS, all requirements in ISO/IEC 20000-1 can more easily be addressed and met. In summary, ISO/IEC 20000-1 is applicable to all services defined in an SMS regardless of: — size: micro to large; — composition: single or aggregated (comprised of multiple CIs or components); — service provision source: centralized, decentralized or distributed services provided internally or externally; — service consumption source: internal or external customers/users.	Clauses 4 – 10
Can ISO/IEC 20000-1 be used with bundled services? An example of a bundled service configuration is an online banking application provided by a banking organization. This service includes multiple service and technology components and is used by the bank's customers. Examples of bundled services include:	Clauses 4 – 10

Table 1 *(continued)*

Topic	ISO/IEC 20000-1:2018 clause number
— online banking application: the service component that processes online banking transactions; — support group: an internally-provided technical micro service; — network services: the group that supports and enables enterprise network and internet connectivity; — internet service provider: an externally provided service to connect the organization to the internet and which provides consumer access to the online banking application; — web hosting service: an externally-provided service that hosts the website of the banking organization; — internal service desk: provides first line support services to the staff of the bank; — customer service desk: provides technical support services to the customers using the online banking application. Each service listed can be considered micro to large depending upon the size of the organization and can be centralized or decentralized depending upon the requirements of the organization. In some cases, components of a bundled service can also be known as underpinning services or can be bundled services themselves. As a bundled service, each service and component is subject to the requirements of ISO/IEC 20000-1. Due to the defined relationships between the services and components within a bundle, any introduction, modification or removal of a service in the bundle can affect other parts. These actions, for example, can be the result of a modification to the context of the organization, a leadership decision or a change to an externally provided service. Management of change is essential for bundled services, to ensure that the impact of any introduction, modification or removal of service or component in the bundle is assessed, and that changes are appropriately approved and controlled in line with the requirements of ISO/IEC 20000-1. A robust integrated service management toolset can support all service management activities including the management of service definitions and CI relationships within a service. This includes bundled services like the example above. Each service is defined as a CI with its relationship to other CIs. Service management tools can provide a visual service mapping allowing a view of the CI connectivity within a service bundle and any relationships to other services in the SMS. Of equal importance is the storage of, or link to, service-related documentation.	

Table 1 *(continued)*

Topic	ISO/IEC 20000-1:2018 clause number
Can ISO/IEC 20000-1 be used with cloud-based services? There are cloud-based services that provide requirements management, version control, reporting, task management, build, test and release management capabilities. The cloud-based services can cover the complete application lifecycle. When deciding to use a cloud-based service, consider the requirements including the following points dependent on the context. a) Supplier management: are regular supplier reviews carried out to ensure functional requirements, service levels and performance requirements are met and concerns are discussed? b) Service availability management: how reliable is the service? Can the customer's service levels be achieved? c) Capacity management: is there enough to meet the customer's demands, accounting for peaks in the service or development lifecycle? d) Service continuity management: what is the supplier's data back-up and restore process? Does it meet the customer's requirements? How often is this tested? e) Configuration management: how will the service manage new baselines? f) Change management: what process is used, what is the approval mechanism? g) Incident and problem management: what is the process for raising an incident or problem? h) Information security management: is the information secure in the cloud service?	8.2.6 8.3.4 8.4.3 8.5.1 8.6.1, 8.6.3 8.7.1, 8.7.2, 8.7.3

5.3 Can an SMS be sustainable?

Guided by the UN 2030 agenda for sustainable development and its sustainability development goals (SDGs), organizations around the globe are adopting initiatives in areas that are crucial for the planet across environmental, social and economic pillars. ISO/IEC 20000-1 specifies an SMS for managing services across the lifecycle, by providing visibility, control and continual improvement. An SMS, as an element of the management of services, can include support across all of the three sustainability pillars. See Table 2.

Table 2 — Sustainability within an SMS

Topic	ISO/IEC 20000-1:2018 clause number
Building sustainability into the SMS ISO/IEC 20000-1 specifies requirements for managing services across lifecycle stages of planning, support, operation, performance evaluation and improvement of services to fulfil service requirements and deliver value. Top management ensures that the organization's sustainability vision and plan are applied to the SMS through appropriate inclusions in the service management policy, service management objectives and service management plan. Organizations can utilize the SMS to identify sustainability goals and legal or regulatory requirements applicable to service management, such as data centre greenhouse gas emissions disclosure. Any customer requirements for sustainability are taken into account for the SMS. These can be discussed at customer reviews. A sourcing strategy can be used to set out the requirements when selecting and managing suppliers, taking into account alignment to the organization's goals or customer requirements for sustainability. Planning the SMS and designing services includes identification and management of risks and opportunities around social and environmental elements (e.g. health risks, carbon footprint). These also consider the impact on economic aspects. Improvements can arise from optimized IT asset utilization, responsible procurement, sustainable supplier management, and improving IT facilities operations management in terms of electricity, water and HVAC (heating, ventilation, air conditioning) consumption and other actions that are relevant for the organization. See ISO/IEC TS 20000-16:—[a] for information on sustainability with service management.	4.1, 4.2 5.1, 5.2 6.1, 6.2, 6.3 8.2.3 8.3.2
Environmental aspects An SMS can enable a sustainable supply chain through procurement practices with evaluation and selection of appropriate suppliers and supplier performance monitoring, for example, supplier policies for waste management, carbon neutrality, estimated lifetime cost of energy consumption of new equipment. Asset management ensures that assets used to deliver the services are managed according to legal and regulatory requirements and contractual obligations which can include sustainability requirements, for example, selection of assets with minimum eco-footprint, asset tracking, re-use and effective disposal. ISO/IEC 20000-1 requires demand management and capacity management to forecast and manage capacity requirements as well as to monitor and optimize service performance. An organization can design its services to use components that have minimum environmental impact and optimized utilization enabling sustainability, for example, to reduce energy consumption per service and reduce resource requirements (e.g. CPU, memory, storage per service).	8.1 8.2.5 8.3.4 8.4.2, 8.4.3 8.5.2

Table 2 *(continued)*

Topic	ISO/IEC 20000-1:2018 clause number
Social aspects Effective delivery of an SMS strategy which includes sustainability requires allocation of human resources with the right awareness, skills and competency levels to implement the sustainability vision, plan and actions designed within the SMS. The cultures of the organization, sector and geography are also considered. Supplier evaluation criteria and sustainability-related contractual obligations influence supplier policies and actions (e.g. safe and secure working environment, fair wages).	7.1, 7.2, 7.3 8.2.3 8.3.4
Economic aspects ISO/IEC 20000-1 requires budgeting and accounting for services to enable effective financial control and decision-making for services. Financial accounting can include costs and cost savings from sustainability actions (e.g. asset reuse, circular economy). Sustainable procurement and consumption practices affect service costs. Budgeting and accounting includes monitoring and reporting on actual costs against budget (e.g. asset reuse, circular economy).	8.4.1
[a] Under preparation. Stage at the time of publication: ISO/IEC DTS 20000-16:2024.	

5.4 Can an SMS be used with different methods, frameworks and technologies?

The service management and technology environment is constantly changing. That does not mean that ISO/IEC 20000-1 needs to constantly change with each of these increments. The requirements in ISO/IEC 20000-1 are generic and can be used with all types of methods, frameworks and technology. These are unique to each organization and will impact how the SMS and the services are designed. See Table 3.

Table 3 — Operating an SMS with different methods, frameworks and technologies

Topic	ISO/IEC 20000-1:2018 clause number
The SMS and technology ISO/IEC 20000-1 has been written as a generic International Standard that can be applied regardless of the nature of services delivered or the type or size of the organization. Even though the title of the document specifies "information technology", it is about managing the services and the technology used to deliver the services, rather than about defining the technology used. ISO/IEC 20000-1 has been applied in a wide range of services, including pure IT services (e.g. internet services) and services using digital information (e.g. forestry management services). At the same time, hardly any services today do not make use of an IT component, even if just for payment or registration to the services.	1.2

Table 3 *(continued)*

Topic	ISO/IEC 20000-1:2018 clause number
The SMS and methodologies/frameworks/tools Increasingly, organizations adopt service delivery practices that aim for faster value creation for customers. Like technologies, the requirements in ISO/IEC 20000-1 are also independent of the methodology, products or tools used to implement and manage the SMS or provide the services. ISO/IEC 20000-1 specifies what the organization is required to do, not how it is done. Detailed guidance to manage an SMS and the services can be found in frameworks such as ITIL®[a] and process reference models such as CMMI®[b] for Services. There are many others that can be considered, such as FitSM®,[c] COBIT®[d] and VeriSM®.[e] Frameworks such as Lean, Agile or DevOps, or a combination of these, can be used to support the management of services. An organization can even choose to provision services using their own framework or no framework at all; the nature of the services with the size and maturity of the organization determines what is most appropriate. When multiple suppliers are used, the organization can choose to utilize service integration and management, SIAM™,[f] which provides a framework to manage multiple suppliers centrally using a service integrator function. For more information, see: — ISO/IEC TS 20000-11 for guidance on using ITIL with an SMS; — ISO/IEC TS 20000-14 for guidance on using SIAM with an SMS; — ISO/IEC 20000-3 for examples of the use of a service integrator with an SMS; — ISO/IEC TS 20000-15 for guidance on using Agile and DevOps with an SMS. The ISO/IEC 20000 Handbook: IT service management – A practical guide, also contains useful information on this topic.	1.2
The SMS and digital transformation Digital disruption has escalated and the speed of change is evident across industries resulting in new business models. The use of digital technologies in business services and the need to adapt the organization to them is referred to as digital transformation. Digital transformation can include the use of basic technologies such as process automation or advanced technologies (e.g. cloud computing, software-defined infrastructure, internet-of-things (IoT) and artificial intelligence (AI)). The common aspects of current digital transformation technologies suggest the following: — rapidly changing business models present benefits and challenges to the SMS, providing stability and reliability to assure business and service continuity, while simultaneously offering flexibility and agility to respond to changing business demands; — the SMS has to focus first on knowledge of the business and service objectives and second on enabling processes and tools; — in a significant change in customer expectations, success is all about the customer experience as judged by the customers themselves, indicating that an “outside-in” perspective is essential when designing and improving the SMS; — services are most effective when defined from the perspective of the end-to-end business processes and when they include all the components that enable delivery of the services beyond the technologies that enable it; — the organization addresses the risk that services will increasingly rely on complex and sophisticated technologies.	4 6 7.6 8.3.2, 8.3.3 8.7.2

Table 3 *(continued)*

Topic	ISO/IEC 20000-1:2018 clause number
See the ISO/IEC 20000 Handbook: IT service management – A practical guide, for useful information on this topic.	
Example: Process automation The incident management requirement in ISO/IEC 20000-1 is just one example of a process that can benefit from this type of automation. For some services, the process of opening, resolving and closing incidents can be automated, removing the need for human intervention. For example, a cloud-based service can have automation in place that collects events from the servers and storage to decide, based on specific rules, to switch over to backup processing and storage if the primary servers become unavailable. Automation can create an incident ticket for this event, switch over the systems to backup, test the availability of the services and, if successful, resolve and close the incident, noting the action taken to restore the services. With the agreed policies and processes in place, process automation can speed up incident resolution and as a result, enhance the customer experience. It is important to ensure that the organization is able to demonstrate evidence of meeting the requirements of ISO/IEC 20000-1 when process automation is put in place.	8.3.2 8.6.1
[a] ITIL® is a registered trade mark and product owned by AXELOS Limited. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO or IEC of the product named. Equivalent products may be used if they can be shown to lead to the same results. [b] CMMI® is a registered trademark of the CMMI Institute, LLC. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO or IEC of the product named. Equivalent products may be used if they can be shown to lead to the same results. [c] FitSM® is a registered trademark of ITEMO. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO or IEC of the product named. Equivalent products may be used if they can be shown to lead to the same results. [d] COBIT® is a registered trademark of ISACA. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO or IEC of the product named. Equivalent products may be used if they can be shown to lead to the same results. [e] VeriSM® is a registered trademark of IFDC. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO or IEC of the product named. Equivalent products may be used if they can be shown to lead to the same results. [f] SIAM™ is the trademark of a product supplied by EXIN. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO or IEC of the product named. Equivalent products may be used if they can be shown to lead to the same results. NOTE Within SIAM, the term "supplier" is referred to as "service provider".	

5.5 Who can be assigned as top management?

Top management is a term used in ISO/IEC 20000-1 and other management system standards. This can be a point of confusion about what exactly is meant and who can take up the role. See Table 4.

Table 4 — Top management within an SMS

Topic	ISO/IEC 20000-1:2018 clause number
Top management Top management is defined in ISO/IEC 20000-1:2018, 3.1.21, as "person or group of people who directs and controls an organization 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 covers only part of an organization, then top management refers to those who direct and control that part of the organization." Top management can be one person or a group of people with specific responsibilities. The key is in Note 1 to entry of the definition – that they have the power to delegate authority and provide resources. For a small organization or an organization where the provision of services is the whole organization, top management is the person or board at the top of the organization. For a large organization, as stated in Note 2 to entry of the definition, top management is the top of the relevant part of the organization in scope of the SMS (e.g. the top of the IT service department if that is the scope of the SMS). Where SIAM is involved, if the customer organization is the scope of the SMS, then top management is in the customer organization. If the SIAM supplier is the scope of the SMS, then top management is in the SIAM supplier. It is not possible to outsource the role of top management who always remain accountable for the SMS and delivery of services. Top management has specific responsibilities for leadership and management review. In addition, for major incidents, top management are kept informed. Refer to ISO/IEC 20000-2 and ISO/IEC TS 20000-5 for other useful information about the role of top management. Refer to ISO/IEC TS 20000-14 for guidance on using SIAM with an SMS.	5.1 5.2.1 5.3 8.6.1 9.3

5.6 What is the difference between the many types of requirements in ISO/IEC 20000-1?

There are many types of requirements in ISO/IEC 20000-1. These include general requirements (referred to hereafter as "shall statements"), service requirements and capacity requirements. To establish an SMS, it is important to understand the difference between the different type of requirements. See Table 5.

Table 5 — Different types of requirements in ISO/IEC 20000-1

Topic	ISO/IEC 20000-1:2018 clause number
"Shall statements" In ISO/IEC documents, the language used is significant. The following verbal forms are used to indicate specific provision types: a) "shall" indicates a requirement; b) "should" indicates a recommendation; c) "may" indicates a permission; d) "can" indicates a possibility or a capability.	Clauses 4 – 10

Table 5 *(continued)*

Topic	ISO/IEC 20000-1:2018 clause number
Information marked as “NOTE” is for guidance in understanding or clarifying the associated requirement. A "shall statement" indicates a requirement that needs to be met by an organization if it wants to demonstrate conformity to the document. For example, the simple statement "The organization shall retain documented information on the service management objectives" requires an organization to be able to provide evidence of the documentation about the service management objectives to demonstrate conformity to this requirement. ISO/IEC 20000-1:2018, 4.4. states "The organization shall establish, implement, maintain and continually improve an SMS, including the processes needed and their interactions, in accordance with the requirements of this document." Similarly in ISO/IEC 20000-1:2018, 5.3, top management assigns responsibility and authority for "ensuring that the SMS conforms to the requirements of this document." The phrase "requirements specified in this document" is also referred to in planning for the SMS and for documentation. Internal audit requirements in ISO/IEC 20000-1:2018, 9.1, state the need to check that the SMS conforms to "the requirements of this document." For control of parties involved in the service lifecycle, ISO/IEC 20000-1:2018, 8.2.3.1, states "The organization shall retain accountability for the requirements specified in this document and the delivery of the services regardless of which party is involved in performing activities to support the service lifecycle." In all these cases, the requirements are referring to the "shall statements" in the document. It is the "shall statements" which refer to the other types of requirements which are explained below. The other verbal forms (should, can, may) do not indicate requirements and organizations do not need to demonstrate conformity to these. However, conformity to them is likely to be useful. The definition of service management in ISO/IEC 20000-1:2018, 3.2.22 has a useful note referring to requirements: "This document provides a set of requirements that are split into clauses and subclauses. Each organization can choose how to combine the requirements into processes. The subclauses can be used to define the processes of the organization’s SMS."	
Requirements (overview) A requirement is defined in ISO/IEC 20000-1:2018, 3.1.19, as a "need or expectation that is stated, generally implied or obligatory." The first two notes which accompany this definition are important: "Note 1 to entry: “Generally implied” means that it is custom or common practice for the organization and interested parties 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."	4.2 4.3 5.2.1 6.1.1 6.2.1 8.1 8.3.4.1

Table 5 *(continued)*

Topic	ISO/IEC 20000-1:2018 clause number
There are many places in ISO/IEC 20000-1 which refer to requirements generically. For example, in ISO/IEC 20000-1:2018, 4.2, "The organization shall determine the relevant requirements of these interested parties" followed by a note stating that these requirements can be of various types such as service, legal, regulatory or contractual obligations. These requirements from ISO/IEC 20000-1:2018, 4.2, are then referred to again to ensure that the requirements are carried through when determining the scope of the SMS as well as the risks and opportunities. There is a requirement that the service management policy "includes a commitment to satisfy applicable requirements." Similarly, "applicable requirements" are to be taken into account when setting service management objectives. These "applicable requirements" are those identified in ISO/IEC 20000-1:2018, 4.2, as well as all other requirements within the document as relevant to the service management policy and objectives. Operational planning and control requirements are covered in "plan, implement and control the processes needed to meet requirements" and "establishing performance criteria for the processes based on requirements." These requirements are as above, i.e. gathered from looking at the context of the organization and all others within the document. Management of external suppliers refers to "requirements to be met by the external supplier." These are very specific requirements that will vary depending on the service or product that is being purchased from the external supplier (e.g. service targets, product specification, information security requirements).	
SMS requirements The SMS requirements are those built into the design and establishment of the SMS. The SMS is established to meet the requirements of ISO/IEC 20000-1. How this is done is different for each organization according to their own processes, policies and services. The SMS requirements are embodied in the plans, policies, processes and procedures that make up the SMS. There is a critical requirement for top management to ensure "the integration of the SMS requirements into the organization's business processes." This means that the SMS is not just an add-on to the normal business activities, but is integrated into them. The internal audit process is required to check for conformity to "the organization's own requirements for its SMS". Ensuring awareness of the SMS requirements including the benefits and implications of not meeting them is important.	4.2, 4.4 5.1 f), 5.1 h) 7.3 9.2.1 a) 1)
Service requirements Service requirements are defined in ISO/IEC 20000-1:2018, 3.2.26, as "needs of customers, users and the organization related to the services and the SMS that are stated or obligatory Note 1 to entry: In the context of an SMS, service requirements are documented and agreed rather than generally implied. There can also be other requirements such as legal and regulatory requirements." ISO/IEC 20000-1 frequently refers to service requirements. Examples are service level targets, hours of service, functionality and information security. The design of new or changed services includes requirements for "changes to human, technical, information and financial resources" and requirements for "appropriate education, training and experience." The capacity and performance, service availability and service continuity requirements are part of the service requirements.	4.2, 4.3 5.1 b) 6.1.2 a) 2), 6.3 7.1 , 7.5.4 f) 8.2 8.3 8.4.3 8.5 8.7

Table 5 *(continued)*

Topic	ISO/IEC 20000-1:2018 clause number
Obligations — contractual, policies, standards, legal and regulatory requirements Obligations are referred to in the service management plan. This refers to: a) policies (e.g. service management policy, organizational policies, technical architecture policies); b) standards (e.g. ISO/IEC 20000-1, other international or national standards, other regulatory body standards); c) contractual requirements e.g.: 1) the organization's contractual requirements to its customers such as service levels; 2) supplier's contractual requirements to the organization such as delivery times for products; 3) the organization's contractual requirements to its suppliers such as payment terms; d) legal and regulatory requirements. They can also be referred to as "obligations". These will vary according to many factors such as country and type of service (e.g. data protection laws, environmental regulations). Obligations are documented in the service management plan or referred to from there. They are then referred to again in requirements for asset management. The most common example here is about meeting contractual obligations with asset suppliers such as software licence terms. The information security policy takes into account the obligations in the service management plan. In the management of external suppliers, contractual obligations are in the contract which can be drawn up by the organization or the supplier. The organization assesses the alignment of these contractual obligations with the customer service level targets and manages identified risks. The organization monitors supplier performance including against these contractual obligations.	4.2 Note 1 6.3 c) 8.2.5 8.3.4.1 8.7.3.1
Capacity and performance requirements Capacity and performance requirements are only referred to in the capacity management clause of ISO/IEC 20000-1. Capacity requirements are for "human, technical, information and financial resources" to meet current and future demands for services (see 5.8 of this document for an explanation of resources). Capacity requirements take into consideration service requirements and performance requirements. Examples of performance requirements are speed of response to an incident or speed of online service requests. Capacity requirement examples are: — human resources: number of staff, capability of staff; — technical resources: network bandwidth, storage space, memory, number of laptops/desktops; — information resources: storage for the documented information, storage and processing capacity for the data within the systems; — financial resources: budget.	8.4.3

Table 5 *(continued)*

Topic	ISO/IEC 20000-1:2018 clause number
Service availability requirements Service availability requirements are determined in the service availability clause. They are also a consideration for capacity planning. Service availability is defined in ISO/IEC 20000-1:2018, 3.2.16, as "ability of a service or service component to perform its required function at an agreed time or over an agreed period of time." The requirements are derived from the risks for service availability and considering the business requirements, service requirements and service targets. Examples of service availability requirements are hours of service or percentage up time. Service availability requirements can be at a service or component level.	8.4.3 b) 8.7.1
Service continuity requirements Service continuity requirements are determined in the service continuity clause. They are also a consideration for capacity planning. Service continuity is defined in ISO/IEC 20000-1:2018, 3.2.19, as "capability to deliver a service without interruption, or with consistent availability as agreed." The requirements are derived from the risks for service continuity and considering the business requirements, service requirements and service targets. Examples of service continuity requirements are service level targets when in a continuity state and targets for recovery by service. There is an additional requirement for the service continuity plan to include service recovery requirements. These will typically cover which infrastructure and systems need to be brought back on-line first to enable services to recommence. The remaining recovery sequence is normally derived from business impact assessments to prioritize those systems which have the highest business impact if they are unavailable for a prolonged time.	8.4.3 b) 8.7.2
Business requirements Planning the services refers to prioritizing requests for change or proposals for new or changed services to align with “business needs.” Agreed requirements for service availability and service continuity both refer to taking into consideration “business requirements.” In both these cases, it is important to consider the customer of the service and their business needs (e.g. the service needs to be available 24/7 to satisfy customer demand, the continuity test cannot include powering down the whole system for half a day due to business demands).	8.2.2 8.7.1, 8.7.2
Planning and reporting requirements Internal audit refers to an audit programme including the “planning requirements.” An example of the planning requirements for internal auditing are given in the list of items to consider for planning the audit programme. “Additional planning requirements” can be dates of external audits, availability of internal auditors and any issues that arise with the SMS. “Reporting requirements” are referred to in service reporting. The reporting requirements are reports which are mandatory in the document, those that are required by customers or regulators and those that are required by the organization itself. Refer to ISO/IEC 20000-2:2019, Annex A, for a list of mandatory reports required in ISO/IEC 20000-1.	9.2.2 a) 9.4

5.7 How does risk management fit within an SMS?

Identification and actions to address risks are a key part of ISO/IEC 20000-1 and all other management system standards. Risk is covered in several places in the document so many questions about how risks can be managed in an SMS can arise. See Table 6.

Table 6 — Risk management within an SMS

Topic	ISO/IEC 20000-1:2018 clause number
Risk-based thinking Risk-based thinking enables an organization to determine the factors that could cause its management system and processes to deviate from the planned results, to put in place preventive controls to minimize negative effects and to make maximum use of opportunities as they arise. Risk-based thinking is embedded in ISO/IEC 20000-1. It allows management to prioritize customer requirements and define their effect on service provision. It ensures that the risks are fully understood before making a decision. In applying risk-based thinking, both short-term and long-term benefits can be considered. It is possible to sacrifice a short-term benefit to achieve a long-term gain. The risks identified by an assessment of the organization are addressed during SMS planning to give assurance that the SMS can achieve its intended results. Risk assessment is the overall process of identification, analysis, evaluation and treatment of risks. Categorizing risks and maintaining their historical data makes assessment and treatment of similar risks in the future much easier. Refer to ISO 31000 for guidance on risk assessment.	6.1
Risks and opportunities Risks are identified by conducting a risk assessment to assure that the SMS can achieve its objectives and the service requirements can be met. The impact and probability of the risks related to the management and operation of the SMS and the services are determined. An approach to address the identified risks is developed to include any actions required to treat risks. Risks are reviewed at regular intervals to ensure effective management. Risk acceptance criteria indicate a threshold. Risks below the threshold can be accepted by the appropriate level of management and risks above the threshold need to be treated. Every organization will have a different risk appetite, which is the level of risk that is acceptable to the organization in order to achieve its goals. In some organizations, top management can authorize the acceptance of a high risk item. It is possible for different divisions within a single organization to have different risk appetites. Although the main requirements for risk are in ISO/IEC 20000-1:2018, 6.1, there are also many other mentions of risk in the document. Risks are assessed for the SMS, services, service availability, service continuity and information security. There are additional considerations for risks when making decisions about approval or rejection of change requests, supplier contract alignment with customer service level agreements and planning the SMS. Risks are also considered when reviewing potential opportunities for improvement where risk reduction can be a good reason for approval, and risk reduction can be a target to measure success of the improvement. Opportunities are also identified. These are positive risks – which allow an organization to gain benefits. Examples are where an organization can gain a competitive advantage by being certified to ISO/IEC 20000-1 or where the time and effort spent on service continuity planning and testing can support the needs of the business for business continuity.	6.1 6.3 10.2

Table 6 *(continued)*

Topic	ISO/IEC 20000-1:2018 clause number
Documenting risks A risk register can be used to document, manage and progress the mitigation of risks. There are different ways to document a risk varying from complex risk tools to spreadsheet format. Some organizations have different risk registers for different types of risk. For example: — information security risks are separate from all other risks; — business continuity risks are stated in the business continuity plan; — corporate risks are kept separately and other documented risks are only added to the corporate risk register if they are very high risks. To provide clarity of the source of risks and updates to the mitigation and resolution of each risk, the following information can be considered for a risk register: — unique identifier (e.g. risk no. 123); — date identified; — risk description; — trigger (e.g. loss of power to the office); — impact description; — target date for mitigation; — risk category (e.g. commercial, information security, operational); — risk sub-category (e.g. external party); — risk owner (accountable for monitoring, escalation and reporting progress); — impact (e.g. low/medium/high); — likelihood (e.g. unlikely, likely, very likely); — calculated risk (e.g. impact × likelihood); — residual risk; — initial mitigation; — status (e.g. new, open, closed).	6.1.2, 6.1.3
Management review Documented risks are reported on a regular basis (e.g. monthly). Those risks deemed critical/high are escalated to top management when they arise. Any risks that have materialized are reported to top management and mitigating actions are agreed as a matter of urgency. The risk report is in an agreed format that the organization can understand and provides the required level of information for decisions to be made and action to be taken. A review is conducted to confirm the effectiveness of mitigating actions taken and to identify any further improvements. The SMS management review covers a review of the risk log and the effectiveness of actions to mitigate the risks.	9.3

Table 6 *(continued)*

Topic	ISO/IEC 20000-1:2018 clause number
Suppliers The risks of the involvement of third parties are identified and actions planned to address any risks (e.g. the risk of suppliers not providing goods/services when requested can possibly be mitigated by having alternative suppliers available). When procuring and managing suppliers, it is important to assess the risk of supplier viability in continuing to operate in the marketplace. Agreements are in place to ensure that the supplier understands their obligations to fulfil the organization's requirements. This is particularly important for resolving incidents within an agreed service level. Risks are identified when agreeing the supplier contract to review the alignment of the supplier service levels with the customer service levels (e.g. if the customer service level is to resolve an incident within 8 hours and the supplier who will be involved in some incidents has a 12-hour service level, then this is a risk).	6.1.2 8.3.4.1
Example: Transition to a SIAM environment with an SMS An example of the management of risk in an SMS is where an organization undertakes the transition to a SIAM model in a manner that meets its needs and risk appetite. SIAM is a service management methodology that includes services integrated across multiple suppliers (known as service providers in SIAM). Moving to a SIAM model is a significant change for an organization which requires careful assessment and planning of the implementation requirements for time, budget and effort. A SIAM implementation can include the following risks: — issues or constraints that were not identified in discovery and strategy stages; — intermediate states that have not been identified in the plan and build stage; — project dependencies that were not previously identified or are not met during the implementation stage; — delays in implementation; — organizational change resistance. Refer to ISO/IEC TS 20000-14 for guidance on using SIAM with an SMS.	6.1
Plan the services and change management The change management process needs to focus on the risks of making the change. During the steps of the change management process, particularly assessment and approval, risks are considered and mitigated. Risks can include: — human resources (e.g. are there sufficient resources to effectively plan, build and test the change?); — skills (e.g. do the staff have the capability to perform all the activities?); — testing the change (e.g. is there a suitable test environment and test data?); — time (e.g. is the timescale realistic to meet the target implementation date?); — other services (e.g. will this change have an adverse impact on other services?). Whatever the case, all risks are considered and either mitigated or accepted by the business. The alternative scenario can also be considered: what is the risk if the change is not approved? Sometimes the answer to this question is much more telling that assessing the change itself.	8.2.2 8.5.1.3

Table 6 *(continued)*

Topic	ISO/IEC 20000-1:2018 clause number
Service continuity **— Business impact analysis (BIA)** Prior to drafting service continuity plans, a risk analysis is required against those areas within scope. This is commonly known as a business impact analysis. In addition to identifying key service requirements, it will also identify risks impacting the continuity of the business. These risks are documented and mitigated where possible. Examples of risks to service continuity are fire, flood, cyber-attack, power outage. Refer to ISO 22301 for further information and guidance for business continuity. **— Plans** Service continuity plans can include risks to recovery that have been identified during the BIA but not fully mitigated. **— Test reports** A service continuity exercise, where a scenario is tested against service continuity plan(s), is likely to identify risks associated with the recovery of the service(s) being affected. The exercise report will document these risks and they can be managed to closure via the organization's risk or continual improvement process. On completion, the exercise can be repeated until deemed successful. It is important to note that in each of the areas above, the danger of not acting on identified service continuity risks increases the likelihood of protracted outages during a service continuity event.	8.7.2
Information security Information security risks impacting the SMS need to be identified and mitigated by the use of controls. Information security covers three pillars: confidentiality, integrity and availability. The risk assessment needs to consider all of these three pillars. Plans to test information security risk scenarios are to be scheduled in conjunction with the service continuity process. ISO/IEC 27001 and ISO/IEC 27005 contain requirements and guidance about information security risks.	8.7.3.2

Table 6 *(continued)*

Topic	ISO/IEC 20000-1:2018 clause number
Demand management, capacity management, service availability management, service continuity management These processes are interrelated but remain distinct: — service availability concerns the design and management of the service to meet availability needs in a normal environment; — service continuity concerns ensuring availability under non-typical circumstances; — capacity concerns the resources needed to support service delivery either in a normal or a disrupted environment; — without capacity, service availability and, by default, service continuity, service delivery cannot be guaranteed. When service availability requirements and targets are defined, risks are assessed and documented. Users identify potential causes of unavailability (e.g. failed component, too many users, software bug), and plan how availability can be managed to meet the requirements and targets. Then, they consider the unthinkable, plan for it and include it in the service continuity plans. When considering capacity, it is important to allow enough capacity to support what has been agreed. This is where understanding demand is necessary (e.g. are there seasonal variations or times where capacity-related outages cannot be tolerated?). Capacity is something that can be fully utilized and therefore plans to replace or expand capacity are to be included in the risk assessment (e.g. will current suppliers have the necessary resources to support the organization's needs? Is it necessary to engage additional suppliers?). Lastly, service continuity is in place to deliver the agreed services at an agreed level if a disaster has occurred. There are multiple scenarios for developing service continuity plans (including do nothing) and this is an important discussion to be held between the customer and top management. Service continuity planning and having the necessary resources and facilities to deliver services in times of dysfunction is not without cost (e.g. personnel, technology, office space). Too often, service continuity is the process that is dropped from the operational budget when funds become tight – what is the risk there? In reality, service continuity only has value if it is available when needed. Otherwise, it is an investment that does not provide any return and that can be very difficult to sell to management.	8.4.2, 8.4.3 8.7.1, 8.7.2

5.8 What are the four types of resources in ISO/IEC 20000-1?

ISO/IEC 20000-1 always refers to resources as four types: human, technical, information and financial. However, there is no definition of resources or these types of resources. See Table 7.

Table 7 — The four types of resources in ISO/IEC 20000-1

Topic	ISO/IEC 20000-1:2018 clause number
Resources Resources are referred to in many clauses because it is vital to ensure that the appropriate level of resources are available, co-ordinated and used in the SMS. Responsibility for this is ultimately with top management and the level and capability of resources is one of the items reviewed at the management review. Resources are detailed in plans for achieving objectives, for the SMS and the services. For new or changed services, resources are detailed in the plan and design stages with prioritization taking into account available resources. One of the potential criteria for targets for opportunities for improvement is utilization of resources. Resources are also mentioned in some definitions in ISO/IEC 20000-1:2018, Clause 3. There is a clause in ISO/IEC 20000-1 called 'Resources' which concerns the determination and provision of resources. It is present in all management system standards but in ISO/IEC 20000-1, the four types of resources have been introduced in addition to a specific mention of the SMS and the services. This clause is about all types of resources. Some organizations do not classify resources within the four types in ISO/IEC 20000-1 (e.g. buildings and associated utilities can be classified as technical resources). See further explanation in this table for the four types of resource (human, technical, information and financial) with examples of each. Capacity management is a specific service management process. It is driven from the demand information as stated in the note in ISO/IEC 20000-1:2018, 8.4.2 "Demand management is responsible for understanding current and future customer demand for services. Capacity management works with demand management to plan and provide sufficient capacity to meet the demand." Capacity management usually focuses on technical capacity which includes the technical and information resources. The capacity planning for human capacity is usually done at a strategic level by management and the human resources department. Similarly for the financial capacity with the finance department. Human resource capacity takes into account the availability of internal resources and the need for the use of external resources. The human and financial resource capacity takes into account the demand information for the technical and information resource requirements. It can therefore be seen that there is a close relationship between clauses for resources and capacity management.	5.1 g) 6.2.2 b), 6.3 e) 7.1 8.2.1, 8.2.2 8.4.2, 8.4.3 8.5.2.1 c), 8.5.2.2 b) 9.3 d) 10.2 a)
Human resources Human resources are those people required for the operation of the SMS and the services. Human resources are also referred to as 'persons' in many places in ISO/IEC 20000-1. Top management need to direct and support "persons to contribute to the effectiveness of the SMS and the services." It is important to ensure that the persons operating the SMS have the necessary competencies and awareness. For example:	5.1 j) 6.3 e) 7.1, 7.2, 7.3, 7.5.1, 7.6 8.4.3 8.5.2.1 c), 8.5.2.2 b) 8.6.2 8.7.3.1 9.3 j)

Table 7 *(continued)*

Topic	ISO/IEC 20000-1:2018 clause number
— the extent of documented information required for an SMS can vary depending on various criteria, including the "competence of persons"; — knowledge needs to be "relevant, usable and available to appropriate persons"; — instructions for the fulfilment of service requests need to be "available to persons involved in service request fulfilment". The information security policy and its applicability to the SMS and the services need to be communicated to appropriate persons.	
Technical resources Technical resources can include: — hardware; — software; — office based equipment (e.g. photocopier, scanner, printer); — buildings and associated utilities; — transportation resources. For example, many organizations use cloud-based technical resources. Although these are usually not owned by the organization, the planning for their use and how much capacity is needed can impact the licence requirements. Other outsourced functions require similar planning.	6.3 e) 7.1 8.4.3 8.5.2.1 c), 8.5.2.2 b) 9.3 j)
Information resources Information resources are of two types: a) documents of any type: paper-based or electronic (e.g. policies, processes, records, reports); b) data of any type or purpose (e.g. organization data, customer data). Information resources need to be considered in demand and capacity management. There needs to be sufficient capacity to hold the documents in an electronic document repository or a secure filing space for paper-based information. The demand for this needs to be forecast in demand management. The volume of data needs to be considered for network and storage capacity. For all type of information resource, information security risks are identified and relevant controls put in place.	6.3 e) 7.1 8.4.2, 8.4.3 8.5.2.1 c), 8.5.2.2 b) 8.7.3 9.3 j)
Financial resources Financial resources are the budget that is available for the operation of the SMS and the services. Financial resources are mentioned in many places with the other resources. The main requirements regarding financial resources are in the clause covering budgeting and accounting for services. The financial impact of changes is considered in change management.	6.3 e) 7.1 8.4.1, 8.4.3 8.5.1.3, 8.5.2.1 c), 8.5.2.2 b) 9.3 j)

5.9 How are suppliers managed within an SMS?

In ISO/IEC 20000-1, an organization can use internal suppliers, external suppliers or customers acting as a supplier to provide or operate their services, service components or processes. What specifically is meant by these three types of supplier and how is each managed? Is it possible to have no suppliers? How are multi-supplier environments managed? ISO/IEC 20000-1:2018**,** 8.2.3, Control of parties involved in the service lifecycle, and ISO/IEC 20000-1:2018, 8.3.4, Supplier management, are closely related but what is the difference and the relationship? See Table 8.

Table 8 — The three types of suppliers within an SMS

Topic	ISO/IEC 20000-1:2018 clause number
The three types of suppliers **— External supplier** "External supplier" is defined in ISO/IEC 20000-1:2018, 3.2.4 as "another party that is external to the organization that enters into a contract to contribute to the planning, design, transition, delivery or improvement of a service, service component or process 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." External suppliers can include those that supply products or services that can appear not to be directly related to the services themselves, such as facilities management, hardware suppliers or cloud storage suppliers. Agreements with external suppliers will be in the form of contracts. **— Internal supplier** "Internal supplier" is defined in ISO/IEC 20000-1:2018, 3.2.8 as "part of a larger organization that is outside the scope of the SMS that enters into a documented agreement to contribute to the planning, design, transition, delivery or improvement of a service, service component or process EXAMPLE Procurement, infrastructure, finance, human resources, facilities. Note 1 to entry: The internal supplier and the organization in the scope of the SMS are both part of the same larger organization." Typically, this situation will arise in a large organization where part of the organization is in the scope of the SMS (e.g. the IT service department). Other parts of the organization outside of this SMS scope can contribute to the operation of the SMS (e.g. the project team who work on service design and transition). It is the other parts of the organization who are classed as an internal supplier. An agreement with an internal supplier is usually known as an operational level agreement (OLA). **— Customer acting as a supplier** "Customer acting as a supplier" is not a defined term. This is where the organization has a customer who also happens to be a supplier. The customer acting as a supplier can be internal to the organization or external. For example, an organization provides network security services to their customer and the customer provides data centre services to the organization. There needs to be one or more documented agreements to define both services in terms of the service level targets, other commitments, activities and interfaces between the organization and the customer acting as a supplier.	8.2.3 8.3.4

Table 8 *(continued)*

Topic	ISO/IEC 20000-1:2018 clause number
The difference between control of parties involved in the service lifecycle and supplier management The requirements for the management of suppliers and the control of parties involved in the service lifecycle are closely related but have different requirements and focus. Control of parties involved in the service lifecycle is not about managing the suppliers. It starts by stating that accountability is retained by the organization for all requirements in ISO/IEC 20000-1, regardless of which party is performing activities. This implies that there needs to be clarity in the form of documentation for all activities about which party is involved. It then moves on to a requirement which is part of the procurement process about selection and evaluation criteria for other parties. However, it is important to note that ISO/IEC 20000-1 excludes the procurement of suppliers. The only "shall not" statement in the document is included to ensure that other parties are not providing or operating all services or all service components or all processes. If this is the case, the organization has little to do in their SMS and it would not be possible to demonstrate control or accountability. The integration of services, service components and processes in the SMS from all parties is critical in ensuring the successful operation of the SMS to meet the service requirements for the customers. The controls for other parties (the three types of suppliers) are defined and applied according to the role of the other party. If the other party is operating processes of the SMS, then the control is on the process performance. If the other party is providing or operating services or service components, then the control is about the effectiveness of these. "Supplier management" is about management, monitoring performance against agreements and taking action if needed. For an external supplier, there are more requirements and the need for a documented contract. For an internal supplier or a customer acting as a supplier, there are fewer requirements and a need for a documented agreement. If there are lead suppliers with sub-contracted suppliers, the requirements are only for the lead suppliers. The organization does not need to control or manage the sub-contracted suppliers but expects the lead suppliers to do this. Refer to ISO/IEC 20000-2 and ISO/IEC 20000-3 for further information.	8.2.3 8.3.4
How to manage a multi-supplier environment with a service integrator? Managing a multi-supplier environment managed by a service integrator is known as service integration and management (SIAM). SIAM separates any contract management from business relationship and supplier performance management. This can all potentially be assumed to sit in the supplier management remit. However, in SIAM, the contract management is with the customer who contracts all suppliers and the business relationship management is with the service integrator. In a SIAM model, the suppliers are known as service providers. Refer to ISO/IEC TS 20000-14 for further information about SIAM and the SMS.	8.3.2 8.3.4
Is it possible to have no suppliers? It is common for an organization to have no internal suppliers or customers acting as a supplier. However, it is rare that there are no external suppliers. This depends on the scope of the SMS and the type of services. For an IT service scope, there will be suppliers for hardware, software and possibly also to provide outsourced services such as a service desk. Even with the use of cloud services for all IT work, the cloud service provider is a supplier and there will be hardware infrastructure too. If there really are no suppliers, the service management plan can state that there are no suppliers.	8.3.4

5.10 Where is project management used within an SMS?

Terms such as project, project manager or project management are not specifically stated in the requirements of ISO/IEC 20000-1 which focuses on service management. However, service management does involve planning, resourcing, acceptance criteria, testing and measurement of success. All of these are referencing activities and techniques from project management. See Table 9.

Table 9 — Project management within an SMS

Topic	ISO/IEC 20000-1:2018 clause number
Implementing ISO/IEC 20000-1 Striving to work to the requirements of ISO/IEC 20000-1 and being certified against them are two different things. Whatever the organization's objective, using a recognised project management methodology significantly improves the chances of a successful ISO/IEC 20000-1 implementation. Some things to consider are: — timescales: whether the requirement for implementing and operating to ISO/IEC 20000-1 requirements is customer or business driven, a date for this is agreed; — resourcing: recruitment and training is planned. Does the organization have enough staff with the right skill levels to implement and manage an operation that adheres to ISO/IEC 20000-1 requirements? (e.g. process owners, process managers); — costs: a budget is agreed including costs of recruitment and training, service management toolsets, monitoring and reporting tools and external auditors (if the SMS is to be certified); — project management: internal project progress and compliance reviews are planned. If certification is required, a certification body needs to be engaged to perform the required certification audits. Evidence of the operation of all required processes is made available. Assigning a project manager, with a strong service management background, is likely to increase an organization's chances of success. Refer to ISO/IEC TS 20000-5 for guidance on implementing and improving an SMS. Also refer to ISO 21502 for guidance on project management.	4.4
Operating the SMS In order to operate the SMS and meet ISO/IEC 20000-1 requirements, planning, resourcing, funding and control for project related activities is agreed as part of any budgeting and forecasting activities. Project-related activities are typically about new services, changes to services or transfer of services into the live environment. There are often other projects in a service management environment such as an update to the service management tool set. Additionally, all service managers benefit from training and experience in project management to support the management of budgets, resources and planning of the SMS and the services. It can be beneficial to have a service management office which works in a similar way to a project management office (PMO) to support the service manager and any project managers working within the service environment.	6.3 7.1, 7.2, 7.4 8.2.2 8.4.1 8.5.1, 8.5.2, 8.5.3
Project changes Those changes that have the potential to have a major impact, as defined in the change management policy, are likely to require project management to scope, plan and implement the change. Major impact can be defined as those that are high risk, above a budget threshold, introducing new technology or where additional skills or effort is required. The service design and transition process in ISO/IEC 20000-1 is split into project stages:	8.1 8.5.1, 8.5.2

Table 9 *(continued)*

Topic	ISO/IEC 20000-1:2018 clause number
— plan new or changed services; — design; — build and transition. Activities required to complete such changes need significant planning and using a project manager to scope the project, plan the activities and monitor the progress increases the chances of a successful change implementation. The project needs to consider roles and skills required for any new solution that requires testing.	
Continual improvement Significant improvements require detailed planning and management with a project manager.	10.2

5.11 What is organizational change management and how does it fit within an SMS?

Organizational change management (OCM) is the human side of managing change and business transformation. Using various techniques, OCM helps those impacted by change to understand, accept and adapt to the change in their environment and work. Whatever the source of OCM, it is important to ensure the objectives of the activities are tied to the overall strategy of the change. See Table 10.

Table 10 — Organizational change management within an SMS

Topic	ISO/IEC 20000-1:2018 clause number
Organizational change management OCM is not directly addressed in ISO/IEC 20000-1. It can usefully be included in the activities of establishing an SMS and demonstrating leadership and commitment as this can require change in how the organization operates, as well as how it views service delivery. The same logic follows when addressing planning and support of the SMS. The change in an organization to adapt a service culture attitude will benefit from engaging in an OCM programme. Specifically, consideration is focused on the competence, awareness and communication requirements. The implementation of these requirements can fall within the generic definition of OCM and its various techniques. Typical techniques include communication, active involvement in the change, training, support and feedback. Utilizing these techniques can improve not only the success of the change but also the overall efficiency and sustainability of the change. Successful OCM requires coordination between the change programme, leadership and the various interested parties. Some organizations can have specific personnel who specialize in OCM while others utilize resources from human resources or individual managers. In all these areas, senior leadership and interested parties' involvement are critical – their guidance through communication as well as their own actions will reinforce the importance of the changes and create the necessary awareness and buy-in. In addition, it is good to have time for celebration as changes are embedded in the organizational culture.	4.4 5.1 6 7 8.1 8.5.1, 8.5.2
Organizational change management challenges There are several challenges that an organization can face as they either develop a new SMS or improve an existing SMS. These challenges are defined in ISO/IEC TS 20000-5:2022, Table 2. The table includes the key considerations in overcoming the challenges with the relevant clauses from ISO/IEC 20000-1 to illustrate where the challenges can arise and how the organization can address the requirements. Specific challenges addressed in ISO/IEC TS 20000-5 include: a) improving support for implementing an SMS; b) waning support for an SMS; c) buy-in issues; d) cultural resistance; e) shadow IT; f) escalating costs; g) mergers, acquisitions and transfers; h) checklist mentality; i) unrealistic implementation timescales. Refer to ISO/IEC TS 20000-5 and ISO/TS 10020 for further guidance on OCM.	**Other references:** 4.4 8.5.2

Table 10 *(continued)*

Topic	ISO/IEC 20000-1:2018 clause number
Specific process areas where OCM can be used Several process areas in ISO/IEC 20000-1 can include OCM activities as the process requirements are being fulfilled: — change management: depending on the type of change, it can be prudent to include OCM activities that will support the change as well as the impact to the organization; — plan new or changed services: the impact on the SMS, other services, planned changes, customers, users and other interested parties are to be considered. The plan can include the OCM activities in the design, build and transition; — release and deployment management: this includes not only the technical details and activities but also ensures training, communication and overall readiness of the organization to accept and utilize the change when it is deployed; — incident management and problem management: potential causes of incidents and problems can be human behaviour, if the behaviour has not been learned (e.g. a process change) or understood (e.g. reverting to previous ways of working). In each of these areas, OCM activities are designed to overcome resistance and to foster a culture of continual improvement.	8.5.1, 8.5.2, 8.5.3 8.6.1, 8.6.3
Performance evaluation and improvement The impact and effectiveness of the OCM programme is reviewed in the same way as any other element of the SMS. In the evaluation, it is useful to consider the following points: — measurable behavioural change; — amount of recurrence (e.g. are there incidents or other measurable evidence that shows that behaviour has or has not changed?); — effectiveness of various OCM activities; — timing of the OCM activities (e.g. too early, too late, too many other changes at the same time). As a result of the evaluation, consider improvements to the OCM activities (e.g. more resource investment, improved or additional training around OCM). OCM is not an activity that is only done once but an activity that needs to be monitored and assessed to ensure the required changes are solidified in the organization.	9 10

5.12 How do change management activities operate within an SMS?

Change management is critical for any organization. Without this, changes will be uncontrolled and are likely to lead to service incidents and down-time. An organization uses change management to add, remove or transfer services provided. Change management is linked to many other processes. How do these links with other processes work? What is the relationship with service management objectives? What about new methods of change, release and deployment such as continuous integration, continuous delivery/deployment and Agile techniques? See Table 11.

Table 11 — Change management and related processes within an SMS

Topic	ISO/IEC 20000-1:2018 clause number
Change management Change management and its activities are prevalent throughout ISO/IEC 20000-1. In a technical arena, there can be a tendency for change management to focus on the hardware and software assets. Supporting documentation often needs to be considered when infrastructure changes are being assessed, particularly those that are required for implementation activities (e.g. technical work plans). Change management can also be used for non-technical changes. A change request is raised for any change activity within the scope of the policy, whether it is directly through the change management process or to request a new or changed service via service design and transition. A change assessment, which includes interested parties, provides some assurance that the request for change has been properly assessed and any adverse risks nullified or mitigated, before being approved. The assessment needs to take into account many factors including the overall service management policy and objectives. (e.g. will the change requested fit within this policy and objectives? If there are objectives about climate change, will this change fit with that objective and not add to the carbon usage of the services?). When implemented fully within the culture of an organization, change management reduces the probability of unauthorized changes and the possibility of new incidents or poorly assessed changes, benefitting the cost and quality of service delivery. With a change management culture, changes to the organization, technology, methods or services can be managed more efficiently and effectively.	8.5.1, 8.5.2
Change management policy ISO/IEC 20000-1 requires a change management policy to be drafted which defines those components under the control of change management. The policy also includes categories of change and how they are to be managed. Contents include: a) in scope (e.g. laptops, servers, software in production), changes to environment (e.g. move to new server room, reduction of energy usage), changes to methods (e.g. move to use of DevOps or Agile techniques); b) out of scope (e.g. keyboards, software in test status); c) change categories (e.g. normal change using the change management process, project change using the service design and transition process, emergency change using the emergency change procedure). Major impact change criteria always include removal/decommission of a service and transfer of a service into or out of the organization. Other criteria can be added (e.g. high risk, estimated costs above budget threshold, new technology). These major impact changes are managed by the service design and transition process. Some organizations also use change management for organizational changes and all document changes. This needs to be clear in the policy. The change management policy needs to be aligned to the service management policy and take into account the service management objectives. Other statements that can be included in a change management policy are:	8.5.1 8.5.2

Table 11 *(continued)*

Topic	ISO/IEC 20000-1:2018 clause number
— the change management process owner is accountable for all activities within the change management process; — the criteria for prioritization of changes takes into account business needs, available resources, service management policy and objectives; — change management maintains delegated responsibility for assessing the impact of minor changes on behalf of other key process areas referring to process owners where necessary; — change management maintains and communicates a forward schedule of change to meet the customer and business needs in conjunction with all other identified interested parties; — a change advisory board operates to assess the impact of changes referred to it; — the procedure for raising and progressing change requests is documented and published to all staff and other identified interested parties; — change management publishes reports that demonstrate the efficiency and effectiveness of the change management process.	
Plan the services Planning the services involves gathering large amounts of information in order to collate the service portfolio and service catalogue of the organization. Requirements for all services and changes to services are gathered. Criticality, dependency and duplication of services are identified. Changes are proposed where they are needed to align the services in the portfolio with the service management policy, service management objectives and service requirements, taking into consideration known limitations and risks. The limitations can be on resource availability, technical capability or budget. Changes generated from the planning of the services will go into change management and be allocated to be managed through the change management process or the service design and transition process according to the change management policy. Prioritization of all changes will be according to criteria set by the organization. ISO/IEC 20000-1:2018, 8.2.2, states that this aligns "with business needs and service management objectives, taking into consideration available resources."	8.2.2
Change management, configuration management and release and deployment management To maintain an accurate picture of configuration items (CIs), all changes to the configuration baseline go through the change management process. Configuration information is updated following deployment of a change to a CI. Change management provides interested parties such as the service desk with details of planned changes and their deployment dates allowing the service desk analysts to identify new incidents related to deployed changes and escalate accordingly. Change management, in conjunction with release and deployment management, can help to ensure that the deployment is successful (e.g. ensuring the correct versions when deploying updated applications). Work instructions or procedures can assist planning and decision making during deployment of a change. A DevOps method can be used which includes continuous integration, continuous delivery/deployment (CI/CD) approaches and automatic provision/release of resources (e.g. servers as code). An Agile method can mean frequent releases after iterative and incremental ways of working. Refer to ISO/IEC TS 20000-15 for further guidance on the use of Agile and DevOps with an SMS.	8.2.6 8.5.1, 8.5.3

Table 11 *(continued)*

Topic	ISO/IEC 20000-1:2018 clause number
Changes to external supplier contracts External supplier contracts are reviewed on a regular basis. In some organizations, this is managed through the change management process. But in many organizations, contract changes are managed using a different process. For either method, an assessment of the impact of the contract changes on the SMS and the services is completed before any approval of the contract change is made.	8.3.4.1

5.13 Is it possible to be creative and innovative within an SMS?

ISO/IEC 20000-1 does not require creativity or innovation in any of its requirements but that does not mean the organization cannot innovate and meet the requirements creatively. It is the culture of the organization, the guidance of organizational leadership and the capabilities of organizational staff that will support and promote creativity and innovation. See Table 12.

Table 12 — Creativity and innovation within an SMS

Topic	ISO/IEC 20000-1:2018 clause number
Creativity and innovation in the organization The requirements specified in ISO/IEC 20000-1 define what needs to be in place and requires evidence to demonstrate conformity. How the organization develops its SMS, including its policies, objectives and plans, is up to the organization. This allows the organization to create an SMS that supports their culture and organizational environment. Therefore, if creativity and innovation are key objectives or part of the culture, then those qualities and characteristics will be reflected in the development and ongoing management of their SMS. Creativity and innovation also depend directly on the members of the organization. Having the correct resources (properly trained, attitudes and characteristics that fit within the corporate culture) as well as emphasizing and rewarding actions of staff that contribute to the effectiveness of the SMS and services, are two areas where the organization and staff can show creativity and innovation. Additionally, the various management roles can be supported with autonomy, authority and skills to encourage creativity and innovation. Support from the organization is needed to allow for creativity and innovation (e.g. time, financial and technical resources, autonomy). The organization's support for creativity and innovation can be defined in the service management policy, objectives or service management plan. An organization that supports creativity and innovation also needs to consider the risks and opportunities that can arise from this and have the necessary mitigations and controls in place. There is a note in ISO/IEC 20000-1:2018,10.2, for continual improvement stating, "Improvements can include reactive and pro-active actions such as correction, corrective action, preventive action, enhancements, innovation and re-organization." This is the only mention of innovation in the document, and it is found in a Note, not a requirement. It is important to understand that innovation can drive improvements. Any areas of weakness can benefit from an innovative approach to resolving and strengthening the area for the future. There are many areas within an SMS where creativity and innovation can play a part to improve the SMS and service delivery for the customers. Creativity and innovation can be taught to a point, but it then becomes a personal characteristic of the individual. However, "rampant" creativity and innovation has been shown to be unsustainable as an overall business model (for example, many start-up organizations reorganize once their product/service has stabilized). Care needs to be taken here that the requirements of ISO/IEC 20000-1 are still met through potential business model changes.	4.4"rampant 5.1 g), 5.1 j), 5.1 l) 6 7 10.2

Table 12 *(continued)*

Topic	ISO/IEC 20000-1:2018 clause number
Service design, build and transition Service design, build and transition is directly related to creativity and innovation. How a service is designed, developed and delivered is completely up to the organization to decide and they can use all the resources (design, methodology, technology, etc.) at their disposal to deliver to the requirements. Even the requirement-gathering process can be innovatively completed. It is often the case that the creative and innovative thinking has been done before a new service or a major change is proposed as a change to the change management process. This initial work can be in the form of a strategy, requirements-gathering at a high level and high-level design. Only after these activities can a request for a new or changed service come into the SMS. Another approach is "design thinking": designing with the end in mind (what is the goal?) before gathering requirements. This is a creative and innovative method which is customer-centric, and which includes the steps of understanding the problem without bias; developing possible solutions; prototyping, testing and refining; and implementing. The ISO/IEC 20000-1 requirements that support design thinking and customer-centricity include: a) service level management, business relationship management, service design and transition; b) capacity management, service availability management, service continuity management and information security management; c) change management, release and deployment management. While multiple processes have been listed, each with its own set of requirements, it is the amalgamation of these processes that allow for the innovative design. The process requirements can be shown to be met via the design thinking flow. One other approach is the use of Agile methodologies where user stories direct the development of the service and its functionality. Those user stories allow the service provider to develop minimal viable products and services to ensure the desired functionality is achieved – thus there is a shorter development time with small increments of functionality delivered more frequently ensuring value is achieved from an early stage. Refer to ISO/IEC TS 20000-15 for more information on how to incorporate Agile and DevOps into an SMS.	8.5.2
Change management Traditionally, change management is a process with a goal to support change and to mitigate risks. To mitigate risk, changes are documented, assessed and then approved before going forward to ensure the change is understood and to mitigate any detrimental impact. Typically, supporting activities such as a change advisory board (CAB), are used but there is no formal requirement for this in ISO/IEC 20000-1. How the organization fulfils the requirements of ISO/IEC 20000-1 is where creativity and innovation come into play. Consider how to expedite changes (e.g. use of Agile/DevOps methodology; peer review and approvals; automated testing; continuous integration/continuous delivery; use of pre-approved change models). When looking to expedite change, the key is to always mitigate risk, therefore the risk tolerance of the organization will dictate how change is handled.	6.1 8.5.1
UN Sustainable Development Goal 9 Industry, Innovation and Infrastructure SDG 9 aims to build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation. While the SDG is measured from an outcome basis, the targets and indicators point to the development of solutions that move the capabilities forward from a technical view. When this relates to a technology-based service, whatever the technology, it will need to be managed and delivered to meet the user's needs. ISO/IEC 20000-1 can support that management and operational delivery with the use of creative and innovative solutions.	4.4

5.14 How does continuous learning and feedback relate to an SMS?

Creating a culture of continuous learning and feedback is essential for any organization that wants to grow, innovate and adapt to changing markets and customer needs. This means fostering a mindset and a practice of ongoing improvement, collaboration and communication among employees and managers. How is this related to an SMS and ISO/IEC 20000-1? See Table 13.

Table 13 — Continuous learning and feedback within an SMS

Topic	ISO/IEC 20000-1:2018 clause number
Goals and values When establishing an SMS, the goals and values are established in the early stages through the use of policies and objectives derived from understanding the context of the organization. From this, the competence, learning and feedback mechanisms can be derived.	4 5 6
Competence Management needs to understand the competencies required to operate the SMS. Competence required for each role is identified along with the current skills, education, experience and any training that are potentially required. It is also important to engage with staff to identify their learning methods, what challenges they face and their ideas. From this, a learning and feedback plan can be put in place covering various methods such as coaching, mentoring, on-line courses etc. Gaps in competence can show up during the operation of the SMS (e.g. inefficient or incorrect resolution of an incident or new skills required to change to new technology). In this case, the staff member is provided with additional training or mentoring alongside a skilled individual. Leadership and planning are key competences when implementing an SMS. Knowledge of the organization's structure, roles and responsibilities for key staff and relevant competence are critical. Management ensures that staff are competent and their competence is monitored and improved. This can be supported by ensuring all personal objectives are clearly linked to the service management objectives.	7.2
Awareness Those personnel supporting the SMS are made aware of the service management policy, objectives and the services within the scope of the SMS. Staff are also made aware of how they contribute to the success of the SMS and service delivery. Top management establish the policies that involve awareness and commitment from staff. Evidence of staff awareness of these policies and objectives can be recorded. However, the actual "physical" involvement in achieving the objectives is a clearer way of demonstrating awareness and understanding.	7.3
Monitoring, measurement, analysis and evaluation ISO/IEC 20000-1:2018, Clauses 9 and 10, require an organization to be able to demonstrate that it continually reviews and improves its performance, in terms of the SMS and the services it delivers, to meet customer requirements. It is important to gather feedback from employees and from customers that can be used to update the continuous learning plan. The organization determines what areas to monitor and measure and which methods are most suitable to ensure that the SMS is properly evaluated. To maintain, support and improve the SMS, the following activities are performed: a) data are monitored and measured on the SMS and the services delivered (e.g. risks raised and mitigated, service targets met or not met, failed changes); b) data are analyzed, considering possible seasonal trends or expected fluctuations (e.g. extra network capacity for end of year accounting); c) evaluation of the results and feedback leads to improvement identification or other actions (e.g. additional learning for the staff involved in failed changes or where service targets are not being met on a regular basis).	9.1

Table 13 *(continued)*

Topic	ISO/IEC 20000-1:2018 clause number
Improvement Once improvement opportunities have been identified and reported, the organization decides how to respond. Nonconformities found from audits or other activities are also actioned in this phase. For all of these, feedback can lead to further continuous learning for all or some staff.	10.1 10.2

5.15 How does remote working impact the SMS?

The COVID-19 pandemic forced many organizations to operate in a work-from-home/remote/hybrid service delivery model. Though this shift to a new way of working was forced by the pandemic, service provider organizations and their employees soon realized the multi-dimensional value of remote working. Realizing the benefits and success of balancing strategies by service providers, this scenario has made a non-reversible shift in mindset across the industry even after the end of the COVID-19 pandemic. Integrating remote working considerations into the SMS ensures that IT services remain effective, secure and reliable in the face of changing work environments and evolving business needs. The specific details of how remote working is addressed will depend on the organization's unique context, remote working policies and the nature of the services provided. See Table 14.

Table 14 — Remote working within an SMS

Topic	ISO/IEC 20000-1:2018 clause number
Scope and objectives When defining the scope of the SMS and setting service management objectives, consider the inclusion of remote working arrangements and their impact on service delivery and support with a focus on: — communication and collaboration; — technology and infrastructure; — security and data protection; — employee well-being and engagement; — legal and regulatory considerations; — customer expectations and requirements; — business and service continuity with disaster recovery; — risk assessment; — resource allocation, training and skill development; — supplier management.	4 6.2

Table 14 *(continued)*

Topic	ISO/IEC 20000-1:2018 clause number
Leadership and commitment For success, it is important for top management to demonstrate commitment to supporting remote working initiatives and to ensure that they align with the organization's service management strategy. This includes providing resources, technology, appropriate equipment and guidance to facilitate successful remote working arrangements. A clear remote working policy that defines expectations, responsibilities and security measures aids the success. Line management ensures that remote workers have access to the necessary resources, tools and technology to perform their roles effectively and deliver services remotely. Line management also ensures that any remote working information security policies are implemented and adhered to. This includes addressing data protection, privacy and security measures to protect organizational information and assets. The organization monitors the effectiveness of remote working arrangements and evaluates their impact on service delivery, customer satisfaction and employee performance.	5
Human resources Remote working, while being beneficial in many senses to individuals, can also pose various people-related risks: — less motivation leading to reduced productivity; — lack of collaboration; — poor visibility of work within the teams; — insufficient control; — reduced knowledge sharing; — inability to build a team culture; — difficulty in onboarding and training new employees. In addition to these risks, remote working also brings opportunities such as: — possibility of hiring capable resources across the global market; — contract renegotiations for optimizing costs; — better people availability at different times for working in multiple time zones; — optimizing facility costs. The service provider can establish new/enhanced people policies, technical environments and newer ways of working to optimize the benefits of remote working.	5.1 g), 5.1 j), 5.3 6.3 e) 7.1, 7.2