TECHNICAL REPORT

ISO/IEC TR 20000-9

First edition
2015-02-15

Information technology — Service management —

Part 9: Guidance on the application of ISO/IEC 20000-1 to cloud services

Technologies de l'information — Gestion des services —
Partie 9: Application de l'ISO/IEC 20000-1 au services de cloud

Reference number
ISO/IEC TR 20000-9:2015(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 40, *IT Service Management and IT Governance*.

ISO/IEC 20000 consists of the following parts, under the general title *Information technology — Service management*:

— *Part 1: Service management system requirements*

— *Part 2: Guidance on the application of service management systems*

— *Part 3: Guidance on scope definition and applicability of* ISO/IEC 20000-1

— *Part 4: Process reference model* [Technical Report]

— *Part 5: Exemplar implementation plan for* ISO/IEC 20000-1 [Technical Report]

— *Part 9: Guidance on the application of* ISO/IEC 20000-1 *to cloud services* [Technical Report]

— *Part 10: Concepts and terminology* [Technical Report]

The following parts are under preparation:

— *Part 6: Requirements for bodies providing audit and certification of service management systems*[1]

— *Part 11: Guidance on the relationship between* ISO/IEC 20000-1:2011 *and related service management frameworks* [Technical Report]

Introduction

ISO/IEC 20000 is the International Standard for service management. It is based on practical industry experience and includes information to support identifying, planning, designing, changing, deploying, operating, supporting, and improving services for the business and customers. ISO/IEC 20000-1 specifies a service management system (SMS) as the means to achieve the integrated management of the service management policies, objectives, plans, processes, process interfaces, documentation, and resources. A key focus of the SMS is to fulfil the service requirements and to deliver value.

The implementation and coordinated integration of an SMS provides ongoing control, greater effectiveness, efficiency and opportunities for continual improvement. It enables an organization to work effectively with a shared vision.

The guidance in this part of ISO/IEC 20000 can be used by organizations that are involved in the provision or management of services that include cloud services. It can also be of interest to organizations that are faced with changes to their existing services and support arrangements as part of a move to cloud computing. ISO/IEC 20000 can be used by service providers that offer dedicated or shared services to internal and external customers.

Key benefits of adopting ISO/IEC 20000 for service providers that offer cloud services can include:

a) greater credibility with internal or external customers of the organization, through delivery of reliable and cost effective services;

b) the opportunity to build a service management system that is based on a tried and proven best practice approach;

c) ongoing control, greater effectiveness and efficiency as well as prioritized continual improvement of services and processes;

d) improved communication within the cloud service provider organization, including a greater understanding by service management and specialist technical personnel of each other's viewpoints;

e) improved communication between the cloud service provider organization and cloud customers and users;

Cloud services primarily focus on enabling access to shared resources, physical or virtual, that are scalable with on-demand self-service provisioning and administration. The cloud services can be used without the cloud customer having any knowledge of the location and other details of the infrastructure supporting those services. These services and resources can include networks, servers and storage systems and applications that can be rapidly provisioned and released with minimal management effort or service provider interaction. Typical attributes of cloud environments include the ability to support dynamic establishment and modification of services and capabilities in a multi-provider environment and a focus on automation to reduce manual intervention.

The delivery and management of cloud services can require coordinated integration to ensure visibility and control of all the elements that contribute to services, including technology, processes, people and partners, or suppliers.

An SMS that conforms to the requirements specified in ISO/IEC 20000-1 can be a powerful tool for service providers delivering cloud services to achieve high service quality, delivery of value, increased agility, and reduced risk.

An SMS can be integrated with an information security management system based in ISO/IEC 27001, which includes requirements for information security in more detail than those specified in ISO/IEC 20000-1.

Information technology — Service management —

Part 9: Guidance on the application of ISO/IEC 20000-1 to cloud services

1 Scope

This part of ISO/IEC 20000 provides guidance on the use of ISO/IEC 20000-1:2011 for service providers delivering cloud services. It is applicable to different categories of cloud service, such as those defined in ISO/IEC 17788/ITU-T Y.3500 and ISO/IEC 17789/ITU-T Y.3502, including, but not limited to, the following:

a) infrastructure as a service (IaaS);

b) platform as a service (PaaS);

c) software as a service (SaaS).

It is also applicable to public, private, community, and hybrid cloud deployment models.

The applicability of ISO/IEC 20000-1 is independent of the type of technology or service model used to deliver the services. All requirements in ISO/IEC 20000-1 can be applicable to cloud service providers.

The structure of this part of ISO/IEC 20000 does not follow the structure of ISO/IEC 20000-1. The guidance is presented as a set of scenarios that can address many of the typical activities of a cloud service provider. The guidance in this part of ISO/IEC 20000 can also be useful for customers of cloud service providers.

This part of ISO/IEC 20000 can be used as guidance for a cloud service provider in designing, managing, or improving an SMS to support cloud services.

This part of ISO/IEC 20000 does not add any requirements to those stated in ISO/IEC 20000-1 and does not state explicitly how evidence can be provided to an assessor or auditor. The scope of this part of ISO/IEC 20000 excludes any specifications for products or tools.

NOTE Additional guidance on the application of ISO/IEC 20000-1 can be found in ISO/IEC 20000-2:2012.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 20000-1:2011, *Information technology — Service management — Part 1: Service management system requirements*

ISO/IEC/TR 20000-10:2012, *Information technology — Service management — Concepts and vocabulary*

3 Terms and definitions

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

4 Applying ISO/IEC 20000-1 to cloud services

4.1 Delivering and managing cloud services

A cloud service provider should define the services using terminology that customers and other interested parties, such as suppliers, can understand. For cloud services this should take into account that many cloud customers can have little knowledge or understanding of technology. Defining different cloud services or providing a cloud service with several different options can help both service providers and customers make the best decision about which services are best aligned to their service requirements.

Alignment between services delivered, service requirements, contractual obligations, business needs and customer requirements can enable cloud service providers and their customers to establish and maintain a successful relationship. Cloud service providers and cloud customers can share responsibility for the relationship and each party should take the necessary actions to achieve the results desired by the customer.

Unambiguous service definitions can reduce discrepancies between customer expectations and service provider intention for the service. The service provider can find it easier to perform service management activities with the knowledge that the customer understands what is being delivered.

By fulfilling the requirements specified in ISO/IEC 20000-1, the cloud service provider should be able to deliver services in alignment with both service targets and customer expectations.

The cloud service provider wishing to demonstrate conformity to ISO/IEC 20000-1 should review its applicability using the guidance provided in ISO/IEC 20000-3.

NOTE 1 Cloud service providers might find it helpful to refer to ISO/IEC 17788, which provides an overview of cloud computing along with a set of terms and definitions.

NOTE 2 Cloud service providers might find it helpful to refer to ISO/IEC 17789, which specifies the cloud computing reference architecture.

4.2 Scenarios

The scenarios in this part of ISO/IEC 20000 describe the service lifecycle utilizing terminology and examples familiar to cloud service providers.

Each scenario includes references to the most relevant requirements specified by ISO/IEC 20000-1. There can be additional considerations for each of the scenarios beyond those referenced. Each scenario includes recommendations and examples of how the referenced clauses in ISO/IEC 20000-1 can be applicable to cloud services.

All processes specified in ISO/IEC 20000-1 have been included in one or more of the scenarios described in this part of ISO/IEC 20000.

5 Scenarios

5.1 Identify the context for service management of cloud services

S01	**Identify the context for service management of cloud services**
Description	A cloud service provider should understand the business and technical context for managing and delivering cloud services. A cloud service provider should ensure that its services, including cloud services, achieve business objectives and customer requirements while adhering to the service provider's principles, rules, and necessary statutory requirements, regulatory requirements and contractual obligations.
Outcomes	— The business and technical environment and context for cloud service delivery is defined and communicated.

S01	Identify the context for service management of cloud services
Applicable clauses in ISO/IEC 20000-1	— Clause 4.1, Management responsibility — Clause 7.1, Business relationship management
Guidance on the application to cloud services	Service providers and customers should seek opportunities to create value with cloud services while optimizing resources and risk. To realize the benefits of delivering cloud services, effective decision-making regarding the context and scope of the SMS and services should be incorporated into the cloud service provider's strategy and plan. Risk management, cost models, service delivery planning and any impact on other activities of the service provider and customer should be taken into consideration. The ability to ensure governance of any processes operated by other parties, such as suppliers, should be considered in regard to cloud services. The cloud service provider should determine what categories of cloud services to provide based on the market demand, opportunities and its own capability. Multi-tenancy, location and other attributes of cloud services can introduce new governance requirements, management and maintenance issues for service providers and customers that should be considered. Agreements and contracts can become more complicated for cloud services where the customer and supplier are located in different countries and different jurisdictions.
Examples	Typical service management objectives of cloud service providers can include: — optimize the cost of cloud services and technology; — offer a more effective and economic method of providing higher quality services at a lower cost; — generate business value from cloud service investments through innovation and value creation; — achieve operational excellence through the reliable and efficient management of cloud services; — maintain cloud service related risk at an acceptable level; — comply with relevant laws, regulations and contractual agreements. The cloud service provider should consider any statutory and regulatory requirements, as well as financial, safety, data protection, information security, privacy, intellectual property, business continuity and sustainability policies and objectives.

Scenario 1: Identify the context for service management of cloud services

5.2 Establish strategy and plan for management of cloud services

S02	Establish strategy and plan for management of cloud services
Description	The service management plan should define the way the cloud service provider intends to provide services. A service strategy can also define how the cloud service provider intends to provide services to achieve both the desired outcomes for the customer and the service provider's own objectives, within known limitations and documented constraints. The purpose of strategy and planning is to define and plan how the cloud service provider intends to deliver value for its own organization as well as for different customers and interested parties using the service provider's capabilities and resources.
Outcomes	— Service management plans are structured to cascade down from a top-level plan to detailed plans for operation and improvement of the SMS and delivery of the services. — Service management and process specific policies (examples include: information security policy, change management policy, release policy). — Defined and agreed service management objectives.

S02	Establish strategy and plan for management of cloud services
Applicable clauses in ISO/IEC 20000-1	— Clause 4.1, Management responsibility — Clause 4.3, Documentation management — Clause 4.4, Resource management — Clause 4.5.1, Define scope — Clause 4.5.2, Plan the SMS — Clause 5.2, Plan new or changed services — Clause 6.4, Budgeting and accounting for services — Clause 6.6, Information security management — Clause 7.1, Business relationship management
Guidance on the application to cloud services	Cloud service provider's top management should: — define desired outcomes and service management objectives to deliver those desired outcomes and service management objectives; — define what services and capabilities are needed to deliver those desired outcomes and service management objectives; — determine how the service provider and customer(s) will know if desired outcomes have been achieved; — agree measurement and reporting of delivery against plan and desired outcomes; — assess and analyse the current state – what exists and what can be leveraged/reused; — analyse customers, suppliers, competitors, regulatory requirements and contractual obligations, policies. When the desired outcomes have been defined, the next step should be to determine the services and service components needed to deliver those outcomes. The services should be categorized in a way that captures the service requirements for people (e.g., skills and competencies), process, technology and organizational structure. The service management plan can then further categorize and schedule the delivery of the agreed services, including improvements, into releases. These releases should have agreed timeframes and targets. Resources should be allocated to achieve the agreed release targets. The service management plan should make it possible to easily identify dependencies between different services or service components, to facilitate decisions about priority and resourcing and to accurately measure delivery of business value. Service components include all components, both technical and non-technical, necessary to deliver and manage the service. Examples of how dependencies between service components should be considered in regard to planning can include:
	a) agreements and contracts with suppliers which should be in place before the service is commercially available; b) training for service support personnel which should be completed before the service is commercially available; c) allocation of specialist personnel across multiple projects; d) dependencies on hardware components being in place before service components can be implemented.

S02	Establish strategy and plan for management of cloud services
Examples	The service provider's top management should understand the business objectives, constraints, risks and priorities in developing the strategy for cloud services. Considerations should include the resources and capabilities of the service provider and other interested parties such as cloud service partners, as well as other service requirements. Top management should prioritise the cloud services to be introduced, changed or retired. In addition to improving service quality, reducing cost and risk, top management should identify strategic opportunities to optimise services through innovation, increasing standardization, sharing, automation and self-service provisioning. There can be significant opportunities for growth from increases in competitive advantage, geographical reach, innovation, value creation and customer satisfaction. When the desired business outcomes are understood, the service provider can prioritise the services, including the capabilities and resources used to plan, design, transition and deliver those services. The service provider can then invest accordingly. Strategies and plans for introducing, changing or retiring cloud services should consider the following: a) changes to the business environment; b) the context of use of the cloud services including the typical roles of users who will access the cloud services, the types of user computing devices and geographical locations; c) changes to the existing services, changes to any cloud services plus any service capabilities and resources required to deliver all the services across the catalogue of services; d) standard mechanisms to provide access to the cloud services; e) the impact on the service management system and its resources and capabilities such as organizational aspects, processes, documentation, education, training, competence of personnel; f) automation, self-service provisioning and administration; g) sharing geographically distributed computing resources that can change dynamically; h) automatic provisioning of resources in any quantity at any time, subject to constraints of service agreements; i) pooling resources in a location independent fashion, in order to serve multiple customers through multi-tenancy; j) maintenance of shared services that potentially impact many organizations, their customers and large volumes of users; k) requirements for transparency and access to customer information to enable customers to optimize and validate their cloud services.

Scenario 2: Establish strategy and plan for management of cloud services

5.3 Provide a catalogue of cloud services

S03	Provide a catalogue of cloud services
Description	A catalogue of cloud services should be made available to prospective and existing cloud customers. If applicable, this can also be part of a general catalogue of services. Information should be provided to communicate any relevant options for use of the services. The catalogue can be either specific to cloud services or can include both cloud and other services.
Outcomes	— Catalogue of cloud services that is understandable to the parties involved.
Applicable clauses in ISO/IEC 20000-1	— Clause 4.3, Documentation Management — Clause 6.1, Service level management — Clause 7.1, Business relationship management

S03	Provide a catalogue of cloud services
Guidance on the application to cloud services	A catalogue should be defined that contains cloud and potentially other services. For example, customers receiving both cloud and other services from a service provider can find it easier if the service provider has combined all services offered into a single catalogue. This catalogue should be aligned with the requirements specified in ISO/IEC 20000-1, 6.1. The catalogue of services should be the foundation both for the definition of cloud services to be provided and for the contracts and SLAs between the service provider and the cloud customer. The cloud service provider should have visibility of the dependencies between services and service components which can be technical and non-technical and that are necessary to deliver and manage the services. Cloud services and the service components can be grouped together into categories that possess some characteristics in common with each other. This can help to structure the catalogue of services and can minimise duplication of information.
Examples	A cloud service provider offering cloud services to the general public has defined a catalogue with all the available service offerings using terms aligned to the customer's expectation of the services. It has been published on the internet so that the customer can select the desired services using a self-service mechanism. Apart from the standard content for a catalogue of services described in ISO/IEC 20000-2:2012, 6.1.3.2, the cloud service provider in this example also defines other aspects of the cloud service, including: a) cloud service category, such as IaaS, PaaS, SaaS; b) service deployment options; c) applicable policies, e.g. data retention policies; d) applicable standards e.g. minimum technical configuration standards; e) information security policies and procedures, e.g. privileged user access, risk control, and access control for other parties; f) controls to support statutory and regulatory compliance; g) controls to support contractual obligations; h) ordering and provisioning procedures; i) relevant financial information, including pricing, accounting and billing methods; j) resources and data location; k) legal issues, i.e. privacy and data protection; Examples of components that a cloud service can depend on include: — functional components such as hardware, software, documentation, communications; — resources required for implementation, i.e. human, financial, information and technical resources. Information about the cost of increasing service levels or adding additional resources has been included in the catalogue of cloud services. Information about the minimum periods of service provision or the cost of the early termination of a service has also been included.

Scenario 3: Provide a catalogue of cloud services

5.4 Identify and manage service requirements for cloud services

S04	Identify and manage service requirements for cloud services
Description	The service requirements should be identified and documented for the SMS and the cloud services. Activities are identified to manage the service requirements for the service provider and interested parties that have a valid interest in the cloud services.

S04	Identify and manage service requirements for cloud services
Outcomes	— The service requirements for the SMS are defined. — The pre-requisites for deployment to the cloud service customer are specified. — The required characteristics and context for the use of cloud services, delivery and operations are specified. — Service requirements are traceable to their source.
Applicable clauses in ISO/IEC 20000-1	— Clause 4, General requirements — Clause 5.2, Plan new or changed services — Clause 5.3, Design and development of new or changed services — Clause 6.1, Service level requirements — Clause 7.1, Business relationship management — Clause 7.2, Supplier management — Clause 9.1, Configuration management — Clause 9.2, Change management
Guidance on the application to cloud services	ISO/IEC 20000-1, 7.1, Business relationship management, specifies requirements for the identification and documentation of the customers, users and interested parties of the services. This usefully provides a visible record of the services used by each customer, as well as the estimated number of users of each service. The service provider should communicate with customers, users and interested parties to promote an understanding of the cloud services and to establish that their requirements for cloud services are documented accurately. ISO/IEC 20000-1, 4.5.2, Plan the SMS, specifies requirements for defining the statutory, regulatory requirements and contractual obligations for services. If the cloud service customer is located in a different country and/or different jurisdiction to the cloud service provider there can be different statutory and regulatory requirements. ISO/IEC 20000-1, Clause 4.5.2 also specifies requirements for identification of any known limitations which can impact the SMS, or the outcome of management decisions and technical decisions. The cloud service provider should analyse the service requirements and maintain all relevant documentation, including traceability of each requirement to the originating source of the requirement. To enable service requirements to be traceable to their source, functional requirements can be classified for different types of capability based on the resources used. Examples include: application capability, platform capability and infrastructure capability. The service requirements should include the definition of the anticipated customer interaction with the cloud services, the cloud service delivery models, cloud deployment models, operational and support scenarios and environments.
Examples	Examples of customer communications for a cloud service can include: — Establishing the service requirements: The customer checks a box that confirms they understand the terms of the agreement and the details about the service to be delivered; — Establishing the statutory, regulatory requirements and contractual obligations: The customer checks a box that confirms they have read and understood the statutory, regulatory requirements and contractual obligations that apply to users of the cloud service; — Communication: The customer receives an automated notification that includes a link to information on the service provider's website with a call to action; Service requirements for the quality of cloud service delivery are described by various terms and criteria, including functionality, availability, scalability, resilience, information security, privacy, portability, interoperability, performance and maintainability.

S04	Identify and manage service requirements for cloud services
	Examples of functional requirements for users include: set up and administer users, login, data entry, browse, search, report, payment and support for business activities. To achieve the required functionality, some service components can need to be integrated. Examples of functional requirements that support the management of cloud services include: — Business support: budgeting, accounting and charging for cloud services and assets; — Administration support: administration of user identities and profiles, monitoring of service activity and usage, event handling and problem reporting, provisioning and maintenance — Information security: authentication, authorization, auditing, validation, encryption, privacy.

Scenario 4: Identify and manage service requirements for cloud services

5.5 Design and develop a new cloud service

S05	Design and develop a new cloud service
Description	As with other types of services, a new cloud service should be planned, designed and developed in preparation for transition into the live environment.
Outcomes	— A new cloud service is designed. — Updated catalogue of services, including the new cloud service.
Applicable clauses in ISO/IEC 20000-1	— Clause 5.1, General (Design and transition of new or changed services) — Clause 5.3, Design and development of new or changed services — Clause 5.4, Transition of new or changed services — Clause 6.1, Service level management — Clause 6.3, Service continuity and availability management — Clause 6.5, Capacity management — Clause 6.6, Information security management — Clause 7.1, Business relationship management — Clause 7.2, Supplier management — Clause 9.1, Configuration management — Clause 9.2, Change management — Clause 9.3, Release and deployment management

S05	Design and develop a new cloud service
Guidance on the application to cloud services	The SMS facilitates the coordination of all the components required for the design and development of the cloud services. ISO/IEC 20000-1, 5.4, Transition of new or changed services, specifies requirements that apply to the planning, design, development and transition of a new or changed cloud service. Changes to the new cloud service as well as changes to existing services should be controlled by the change management process. Cloud services can introduce considerations such as resource sharing, so resource allocation and multi-tenancy can become very important aspects. The cloud service provider should be aware that the processes specified in ISO/IEC 20000-1, Clause 6 (service level management, service continuity and availability management, capacity management and information security management) should be taken into account during the design of cloud services. For example, a) during service design, existing service level agreements can be reviewed to determine whether they can be reused for the new service or whether a new service level agreement should be developed; b) the service continuity and availability of the new service should be designed to ensure that the delivered availability can fulfil the service requirements; c) the design should consider the capacity requirements for the new service; d) the design should consider the information security aspects of resource sharing and privacy issues. The cloud customer can expect cloud services to be easily scalable and accessible whenever and wherever they are used, making activities of resource planning and allocation, capacity management or performance monitoring especially relevant to cloud services. For the transition of new or changed cloud services into the operational environment, the requirements specified in ISO/IEC 20000-1, 5.3 and 5.4 should be considered. The cloud service provider should ensure that the services fulfil the agreed service requirements and are tested against the documented design. If the cloud services are acceptable they should be deployed into the live environment using the release and deployment management process specified in ISO/IEC 20000-1, 9.3. The catalogue of services should be updated with details of the new service and the dependencies between services and service components should be identified. This can also be useful to identify where some service components support more than one service. The configuration management database (CMDB) should be updated with details of any new or changed configuration items.
Examples	A cloud service provider is designing and developing a service for a medium-sized global organization that wishes to concentrate on its own core area of business rather than delivering the service itself. The cloud customer wishes to use its existing business software applications to avoid migration and training costs. However, they want the service provider to host these applications for them as a private cloud service. For this example, the service requirements for the cloud service include:

S05	Design and develop a new cloud service
	— remote access to the business software applications hosted as a cloud service; — no data allowed to be stored outside the customer's home country; — secure storage access to the cloud customer's data and records from both the cloud customer's offices and for personnel working outside of the office; — at least the same or better transaction response times are guaranteed; — cloud service transaction response time monitoring; — data processing to be done as part of normal activities; — self-service support for the customer on demand to increase efficiency; — an easily scaled cloud service that can meet rapid changes in business demand; — an efficient transition to live operation with a minimum investment by the customer. The design and development requirements specified in ISO/IEC 20000-1, 5.3, should be considered for a new cloud service. Examples of the design aspects to consider for the design of a new cloud service to fulfil the service requirements include: a) the identification of policies and standards, contractual obligations, and other constraints; b) the approach to meeting statutory and regulatory requirements of all countries where the service is provided; c) the design of the new cloud service and the capabilities required to deliver it; d) authorities and responsibilities for delivery of the new cloud service; e) resource sharing with other organizations; f) new or changed agreements and contracts to align with the service requirements including service targets for incident resolution, changes and service request fulfilment; g) the functional components needed to engage in the cloud service activities including business support, administration and information security components; h) procedures, measures and knowledge required for delivery and operation of the new cloud service; i) provision of and access to service reports that enable the different parties to verify and evaluate the quality of service, as well as identify opportunities for improvement; j) plans to fulfil specific business and cloud service continuity requirements; k) criteria for information security and integrity of infrastructure, data and communications; l) protection of personnel and customer data; m) procedures for archiving, back-up, recovery and controlling access to software products and methods of control for virus protection; n) availability of archived data, such as logs or backups, according to agreed requirements and applicable policies; o) automation and tools required for the development, transition, operation and improvement of the new cloud service, including self-service; p) standard service and configuration changes required to support any onboarding activities; q) resource requirements to perform the activities to develop, transition, deliver and maintain the new cloud service including human, finance, information and technical resources; r) risks of introducing cloud services and management of the risks;

S05	Design and develop a new cloud service
	Examples of the design aspects to consider for changes to the design of the SMS include: — the identification of policies, standards, rules, practices and conventions and methodologies that are applicable for the delivery of all cloud services; — authorities and role definitions for managing cloud services, including the cloud service provider, cloud customer and supplier roles; — new or changed human resource requirements, including requirements for appropriate education, training, skills and experience to manage, operate and improve cloud services.

Scenario 5: Design and develop a new or changed cloud service

5.6 Establish a service relationship with the cloud customer

S06	Establish a service relationship with the cloud customer
Description	The relationship between the cloud service provider and the cloud customer should be defined and agreed. A communication procedure should be established and responsibilities for management of customer satisfaction should be assigned. Other relationships between the cloud service provider and interested parties should be defined, agreed and maintained.
Outcomes	— Define relationship between the cloud service provider and the different groups of customers. — Communications between the cloud service provider and cloud customer. — Customer satisfaction measurement and identification of opportunities for improvement.
Applicable clauses in ISO/IEC 20000-1	— Clause 6.1, Service level management — Clause 7.1, Business relationship management
Guidance on the application to cloud services	ISO/IEC 20000-1 specifies requirements for a communication structure and procedures, which should be defined to manage the relationship with the customer. An individual should be designated to manage the customer relationship and customer satisfaction, regardless of whether the cloud service provider owns the service or is acting as a service broker. This can be challenging to implement, e.g. a cloud service offered to the general public and with many customers. In this situation the 'designated individual' can be a team of service provider personnel sharing a common identity, accessible via a single communication point, e.g. 'customer support'. NOTE: ISO/IEC 17788, 2.5, defines a cloud broker as "a person or an organization that negotiates the relationship between cloud customers and cloud service providers for management of the delivery, use and performance of cloud services."
Examples	A cloud service provider offering software as a service has defined different communication procedures for each market space and/or customer group. It has defined several customer profiles and customer accounts, simplifying the management of the customers, their contracts and accountability. These procedures have been automated to ensure maximum efficiency and effectiveness, to support flexibility and ease of use for the customer and to aid the agility of the cloud service provider. The cloud service provider has also defined procedures to review the performance of the services delivered to the cloud customer and to manage customer satisfaction and complaints. The procedures can differ by customer profile. For example, a high value customer can in some cases have an individual relationship manager with face-to-face meetings and tailored reporting. Alternatively, a single relationship manager may look after many customers using options for remote communication and automated checklists.

S06	Establish a service relationship with the cloud customer
	Examples of interested parties and their relationship with the cloud service provider can include: — A cloud service broker role that acquires cloud services and builds relationships on behalf of the cloud customer; — A cloud service developer role that is responsible for designing, developing, testing, the implementing and maintaining of a cloud service; — A cloud service auditor role that is responsible for conducting an audit of the provision and use of the cloud services and reporting the audit results.

Scenario 6: Establish a service relationship with the cloud customer

5.7 Establish a cloud service agreement

S07	Establish a cloud service agreement
Description	A subscription to one or more cloud services in the catalogue of services is formally agreed between the cloud service provider and the cloud customer. The subscription includes a documented agreement of terms and conditions for use of the cloud service. For cloud services that are not subscription based, a documented agreement should still be put in place. Examples of non-subscription based services can include private clouds operated by an internal service provider or customized services. The cloud service agreement can include one or more SLAs setting the agreed service targets, workload characteristics and exceptions to be monitored and reported. It can also include other information such as responsibilities of each party, termination conditions and charges.
Outcomes	— Cloud service agreement, signed and agreed by all parties.
Applicable clauses in ISO/IEC 20000-1	— Clause 6.1, Service level management — Clause 7.1, Business relationship management — Clause 9.2, Change management.
Guidance on the application to cloud services	Cloud services can be delivered to many different types of customers with different service requirements. The cloud customer can match the entries in the cloud service provider's catalogue of services with its service requirements. A cloud service agreement should be signed, referencing one or more SLAs between the cloud service provider and the customer. The cloud service agreement should define the rights and responsibilities of all parties and the quality of the services delivered. For some cloud services, the terms of the SLAs can be negotiable and can include the specific requirements of a particular cloud customer. SLAs should fulfil the requirements specified in ISO/IEC 20000-1, 6.1. The SLA can refer to both cloud and other services. Where a customer uses several different cloud services, the cloud service provider can sign either a global service delivery agreement or multiple agreements with the customer.

S07	Establish a cloud service agreement
	When a cloud service involves parties in addition to the service provider, the cloud service agreement and/or the SLA should define the roles which should be performed by each of the parties, their responsibilities and their dependencies. The agreed service in the agreement between the cloud service provider and the customer should be the responsibility of the cloud service provider. The cloud service provider should ensure that the SLAs, if considered a legally binding contract, comply with all statutory and regulatory requirements applicable to the cloud service provider, the service delivered and the requirements agreed with the cloud customer. ISO/IEC 20000-1 specifies all the changes to the documented service requirements, catalogue of services, SLAs and other documented agreements to be controlled by the cloud service provider's change management process. For example, general terms of the service that have been accepted by the customer should not be changed by the cloud service provider without customer agreement and/or notification.
Examples	A cloud service provider has standardized all services and has defined three different product offerings in its catalogue, covering different service options to support the varied business needs of different customers. For each of them, the cloud service provider has defined a specific SLA. Each cloud customer chooses the option that is most suitable to fulfil their service requirements. Two of the options do not allow changes during the term of an agreement. The third option includes customizable conditions to meet specialized requirements. The customer's decision can be based on the ability of the cloud service to fulfil service requirements, plus other criteria such as agreement duration, cost, location of data, etc. All three SLA options define the quality of service in objective and quantifiable terms, including information security, handling of performance failures and, where relevant, the terms of any licences. They include information about: — charges and penalties; — statutory and regulatory compliance, including privacy; — service continuity planning; — limitations to transaction response times; — the location and management of information; — record-keeping policies; — intellectual property and data access rights; — liability in the event of an incident, for example, an information security incident resulting in loss of data; — dispute resolution procedures; — exit process, detailing the termination of use of the service; — cloud service provider responsibilities, e.g. backup/restore tasks. — service targets; — resource scaling and related costs; — resource capacity and availability; — rights and responsibilities of the cloud service provider, cloud customer and interested parties;

S07	Establish a cloud service agreement
	The cloud service provider should include the terms and conditions for an orderly termination of the agreement, including aspects such as the return of data owned by the cloud customer, or the agreement end dates. Terms and conditions can also be referenced in policies that apply to the cloud services in the catalogue. The customer should commit to follow these policies as part of their responsibilities, which can be a legally binding contract. The cloud service provider has also set up an interface between the service level management process and the budgeting and accounting for services process to ensure compliance with all financial commitments agreed with its own suppliers, e.g. the issue of penalties due to failure to achieve agreed targets.

Scenario 7: Establish a cloud service agreement

5.8 Onboarding the customer

S08	Onboarding the customer
Description	The cloud service provider should prepare the cloud services and resources for delivery to the cloud customer. The activities should include planning and deploying changes to the SMS, transition plans, the processes and interfaces and the cloud services, if required. In order to manage and administer the cloud services effectively the activities should include registration of users, managing access and knowledge transfer.
Outcomes	— The cloud service is configured according to the service requirements; — The cloud customer and users are set up and ready to manage, administer and use the cloud services effectively.
Applicable clauses in ISO/IEC 20000-1	— Clause 4.3, Documentation Management — Clause 6.1, Service level management — Clause 6.3, Service continuity and availability management — Clause 6.4, Budgeting and accounting for services — Clause 6.5, Capacity management — Clause 6.6, Information security management — Clause 7.1 Business relationship management — Clause 7.2, Supplier management — Clause 8.1, Incident and service request management — Clause 8.2, Problem management — Clause 9.1, Configuration management — Clause 9.2, Change management — Clause 9.3 Release and deployment management

S08	Onboarding the customer
Guidance on the application to cloud services	Onboarding of the customer can include a range of activities such as defining dedicated or multi-tenant environments, allocating resources, registering users and assigning permissions, configuring an access channel for the service or configuring management and monitoring interfaces for the administrators. The cloud service provider and cloud customer should agree the specific service requirements that will enable both administration and use of the service by the cloud customer. For public cloud customers this can consist of an online form and agreement. Standard service and configuration changes should have been tested prior to deployment of the cloud service. During the onboarding activities these standard changes can be applied to integrate the cloud service with the customer's existing services and systems. Any standard configuration changes should be tested as part of service transiton, per the requirements specified in ISO/IEC 20000-1, Clause 5, design and transition of new or changed services,.
Examples	A cloud service provider has designed and deployed a software based service offering (SaaS) that is offered as a private or public deployment model. As each new customer is acquired, the cloud service provider plans the onboarding activities for each cloud customer. If the customer selects a public cloud offering, specific activities can be performed by the cloud customer. The basic onboarding activities are tested and verified as part of the transition of the new cloud service. The cloud service provider's onboarding activities for a specific new cloud customer include: a) agreeing specific service requirements for administration and use of the cloud service. The customer decides to use a public cloud service in a multi-tenancy environment rather than a dedicated environment. b) setting up the cloud service according to the agreed service requirements includes: — addition of the customer to the multi-tenant environments; — allocation of resources to support the predicted demand; — establishing the authentication and authorization for customers, cloud service administrators and users; — configuring an access channel for the service or configuring management functions; — information security activities including the authentication and authorization of the cloud customer and administrators, providing the customer with the information security policy and the approach to managing information assets; — configuring monitoring interfaces for the administrators; — verifying the services against the customers' service requirements. c) providing access to online application training for the cloud customer's personnel, including users and administrators; d) providing technical documentation to the cloud customer to support the cloud customer's responsibilities for the service. The cloud customer performs the following activities: — move application components into the cloud service environment (IaaS, PaaS); — configure the cloud application to meet specific customer requirements (SaaS);

S08	Onboarding the customer
	— move data to the cloud service environment, with appropriate information security controls; — establish secure network communications between the customer's environment and the cloud service; — perform standard configuration changes to integrate the cloud service with the customer's existing services and systems ; — integration of the cloud service administration capabilities with the customer's existing operational support systems; — coordinate training and awareness activities for the cloud customer's personnel; — information security activities including the authentication and authorization for users; — verification against the service requirements and any applicable legal requirements.

Scenario 8: Onboarding the customer

5.9 Deliver and operate the cloud services

S09	Deliver and operate the cloud services
Description	Once the onboarding of a cloud service has been completed, the delivery of the cloud service begins. The service should be delivered, used, operated and reported on according to the terms of any agreement and associated SLA to fulfil the service targets. The cloud service provider reports and reviews service achievements as well as any non-conformities against the SLA with the customer and interested parties, such as a cloud service partner. See scenario S10 of this part of ISO/IEC 20000 for monitoring and reporting cloud services. The cloud service provider delivers customer support for service requests from customers, resolves incidents and problems and addresses non-conformities. These activities can include change requests, maintenance and service upgrades.
Outcomes	— The cloud service is delivered to the customer to fulfil the service requirements. — Cloud customers receive support for the service as agreed. — The cloud provider reports and reviews the performance of the service and SLAs with the customer. — Activities are performed to maintain and update the cloud services.

S09	Deliver and operate the cloud services
Applicable requirements in ISO/IEC 20000-1	— Clause 4.2, Governance of processes operated by other parties — Clause 4.3, Documentation management — Clause 4.4, Resource management — Clause 4.5.3, Implement and operate the SMS (Do) — Clause 6.1, Service level management — Clause 6.2, Service reporting — Clause 6.3, Service continuity and availability management — Clause 6.4, Budgeting and accounting for services — Clause 6.5, Capacity management — Clause 6.6, Information security management — Clause 7.1, Business relationship management — Clause 7.2, Supplier management — Clause 8.1, Incident and service request management — Clause 8.2, Problem management — Clause 9.1, Configuration management — Clause 9.2, Change management — Clause 9.3 Release and deployment management
Guidance on the application to cloud services	The cloud service should be delivered and operated according the requirements specified in Clause 4.5.3 implement and operate the SMS (Do), in ISO/IEC 20000-1. The SMS facilitates the coordination of all the components required for the operation of the cloud services, including the processes, the agreements, the policies, the plans and the human, technical, financial and information resources. The service level management process in ISO/IEC 20000-1,6.1 coordinates activities of the service provider and interested parties to deliver the cloud services according to the SLA and service requirements. Cloud customers need a clear understanding of the available cloud service offerings, including what support is available, how support is provided and what procedures and customer obligations exist for accessing support for each service. Cloud service providers can utilize other parties to support the delivery of cloud services to the customer. The other parties can be suppliers, internal groups or customers acting as suppliers. For example, a cloud service provider can utilize a supplier to manage incidents for the service and to provide a service desk. Suppliers that are external to the cloud service provider should be managed using supplier management requirements specified in ISO/IEC 20000-1, 7.2. Internal groups that are in the same organization as the cloud service provider but outside the scope of the SMS, or customers acting as a supplier should be managed with the support of a documented agreement according to the requirements specified in ISO/IEC 20000-1,6.1. Whenever several cloud suppliers are involved in the delivery and management of a service, aspects such as confidentiality, portability (at the data, system or service level) and service interoperability should be considered. In order to ensure that all suppliers manage information security and quality of services in alignment with SLAs between the customer and the service provider, the cloud service provider should have governance of all processes or parts of processes operated by other parties according to the requirements specified in ISO/IEC 20000-1, 4.2. Measurement of deliverables against originally defined service requirements and any amendments or changes, as documented in the SLA or other agreement, should determine whether or how well requirements have been met and whether services have been improved. Service acceptance criteria can support this measurement.

S09	Deliver and operate the cloud services
Examples	The SMS provides the cloud service provider with the visibility and control of all the service components for a specific service, including the infrastructure components, the documents (for example agreed service targets, policies, configuration information), resources, suppliers, monitoring data and analysis, incident, problem and change records, etc. The cloud service provider conducts risk analysis and identifies existing and potential risks to the service, which can then be prioritized and addressed through the change management process. As cloud customers are added and subtracted, or service requirements evolve, or incidents and problems occur, the cloud service provider should address any required changes through the change management process. Examples of how the SMS supports the delivery and operation of the cloud services can include: a) management of the availability, continuity, capacity and information security requirements for the service; b) managing the suppliers, both external or internal, that are involved in the cloud service delivery; c) management of ongoing changes and releases with potential impact to the service; d) regular review of adherence to policies with potential impact to the service, as well as consideration of any changes required to policies to reflect identified opportunities for improvement or evolving service requirements; e) reviews of service reports, including service performance and customer satisfaction. The cloud customer can also participate in the operation of the service, for example: a) access: the cloud customer can have an administrator with access to a management interface which gives them specific capabilities to contribute to service delivery, such as the addition or removal of user access; b) service reports: the cloud customer can have the ability to define their own scheduled and ad hoc reporting requirements through an administrative interface; c) change management: the cloud customer can require to be included in the change management process or can request to be notified of significant changes that can impact their service availability; d) incident and service request management: the cloud customer should be informed of progress and expected service restoration times for any incidents which have been logged or which impact the cloud customer's service availability. This information can be delivered via a relationship manager, an online dashboard or the cloud service provider service desk.

Scenario 9: Deliver and operate the cloud services

5.10 Monitor and report cloud services

S010	Monitor and report cloud services
Description	The cloud service provider should monitor the fulfilment of the service requirements and objectives agreed in the SLA including service targets, customer satisfaction, workload characteristics and exceptions to the SLA. This includes activities to monitor and report the service performance, capacity, availability, information security and/or continuity of the cloud service.

S010	Monitor and report cloud services
	The activities include discovering and monitoring resources, monitoring cloud operations and events and generating reports. The monitoring activities can benefit both the service provider itself and the customer. For example, the service provider can use monitoring activities to raise alerts when capacity is nearing a threshold and an action needs to be taken to ensure the service does not become unavailable for customers. The service reporting provided to a cloud customer can indicate the true usage of the cloud services to enable the consideration of any adjustments. These can include improved training and awareness for users, resource optimization, consumption based pricing, or renegotiating the service level agreement to reflect evolving service requirements.
Outcomes	— Cloud service performance and aspects of cloud service delivery are reported and available to interested parties. — Measurements of cloud service performance and usage are available to the service provider and interested parties, including the cloud customer. — Abnormal occurrences, events and incidents are visible to interested parties.
Applicable requirements in ISO/IEC 20000-1	— Clause 4.3, Documentation management — Clause 4.5.4, Monitor and review the SMS (Check) — Clause 4.5.5, Maintain and improve the SMS (Act) — Clause 6.1, Service level management — Clause 6.2, Service reporting — Clause 6.3, Service continuity and availability management — Clause 6.5, Service capacity — Clause 6.6, Information security management — Clause 8.2, Problem management — Clause 9.1, Configuration management — Clause 9.2, Change management — Clause 9.3, Release and deployment management
Guidance on the application to cloud services	The cloud service provider should make service reports available so that the cloud customer can compare the services and SLA against agreed service targets. This reporting can be made available through a website for many customers or can be tailored for different customers as agreed in an SLA or other agreement. Cloud service providers should store the monitoring data for an agreed period of time, allowing the customer to examine or download it. The data retention policy for monitoring data and service reports should be defined and agreed in the SLA. The cloud service provider should also produce internal reports, for its own use, as a decision support tool for the management and improvement of cloud services. Monitoring of cloud services can be complex. An increase in complexity can lead to greater risk and higher costs due to the number of components to be controlled. The cloud service provider can automate service level monitoring activities in order to facilitate opportunities for improvement to be identified, e.g. improvements in productivity or customer satisfaction. The cloud service provider should ensure the existence of a procedure to monitor all parts of the service, including those which are delivered by other parties, to measure performance against service level targets.

S010	Monitor and report cloud services
	Other service management processes are involved in monitoring and providing input to service reports, e.g. capacity management, incident management, information security management, service continuity and availability management. The service reports should be used to enable decisions to be made for the prioritization of improvements. Any improvements identified should be managed using the requirements specified in ISO/IEC 20000-1, 4.5.5, Maintain and improve (Act). The requirements specified in ISO/IEC 20000-1, 4.5.4, Monitor and review the SMS (Check), should be used for management reviews and internal audits of the SMS and the cloud services. Any corrections or improvements identified should be controlled using the requirements specified in ISO/IEC 20000-1, 4.5.5, Maintain and improve (Act). For example, the internal audit can identify that a process is not being followed which is impacting the service levels and a corrective action can be undertaken to ensure the process is followed consistently.
Examples	For operational cloud services, certain conditions should be identified that demand immediate notification of the event to the impacted customer, e.g. an intrusion detection or invocation of the continuity plan in the event of a disaster. Regular monthly service reports can also include the following: — cloud service provider internal operational reports. For example, number of incidents, problems, average speed of dealing with customer issues, etc.; — cloud service reports to the customer. For example, status report issued against agreed high level measures, such as percentage availability of the service; — service level target reports, including agreed measurements over an agreed timescale for the targets defined in the SLA or other agreement; — service performance. These measures should be represented from the customer perspective rather than technical details about servers and backend measures; — service availability targets, such as, —service downtime as a percentage of expected uptime; —financial - invoice issued to customer on time; —invoice paid on time; —customer - customer satisfaction; —service changes - additional service usage or changes to the service contract.

Scenario 10: Monitor and report cloud services

5.11 Manage resources for cloud services

S11	Manage resources for cloud services
Description	Within the context of an existing agreement, the cloud customer can request the allocation or release of resources according to the agreement. Resources, as specified in ISO/IEC 20000-1, can include human, technical, financial or information resources.
Outcomes	— New configuration of the service with the updated resources. — Updated cost profile.

S11	Manage resources for cloud services
Applicable clauses in ISO/IEC 20000-1	— Clause 4.2, Governance of processes operated by other parties — Clause 4.3, Documentation management — Clause 4.4, Resource management — Clause 4.1.1, Management commitment — Clause 4.5.5.2, Management of improvements — Clause 6.4, Budgeting and accounting for services — Clause 6.5, Capacity management — Clause 8.1, Incident and service request management — Clause 9.1, Configuration management — Clause 9.2, Change management — Clause 9.3, Release and deployment management
Guidance on the application to cloud services	The cloud service provider should identify the need for additional resources or the release of resources, through service reports as well as plans to add new customers or increase the number of users. The cloud service provider can request additional resources or the release of resources through the change management process. If these are standard changes, they can be made through the incident and service request management process. Configuration records should be updated with the revised resource allocation and any updated interfaces to other configuration items. Cloud resources should either be added or removed using the release and deployment management process once the requested change has been fully tested and approved for implementation. Service capacity should be adequate to meet customer demand. The capacity management process can ensure that the cloud service provider can fulfil the customer's expectation of the elasticity of cloud services. The allocated capacity for the cloud service can be automatically recovered or surrendered by the cloud customer when no longer utilized. The cloud service provider should develop a capacity plan to ensure that demand driven capacity can be successfully maintained. The capacity plan should consider human, technical, information and financial resources. It should also identify capacity growth patterns in order to facilitate the appropriate scaling of cloud resources. The potentially complex calculation of demand across all users and all customers can be supported by the service reporting process and the integrated information flow from individual service management processes and the SMS. The revised cost profile for services with a revised capacity allocation should be calculated and notification provided to the customer.

S11	Manage resources for cloud services
Examples	An IaaS provider offers infrastructure resources as a cloud service. The cloud customer should be able to request additional resources or services on demand and also surrender unused resources or services when they are no longer used. The cloud service provider should have procedures for the budgeting and accounting of the provisioning and de-provisioning of resources and services. There are no requirements for charging specified in ISO/IEC 20000-1. However, in order to charge accurately for cloud services, the cloud service provider should perform the activities of the budgeting and accounting for services process as specified in ISO/IEC 20000-1, 6.4. These include documented policies and procedures for at least the following service components: assets, including licences; shared resources; overheads; operating expenses; personnel and facilities. The cloud service provider should also measure the consumption of services and calculate the cost of services. The cloud service provider can also report service utilization to the cloud customer for use in the cloud customer's own accounting procedures. The automation of service delivery can effectively increase the responsiveness of cloud service providers by enabling the 'on demand' usage of services. This can only be achieved if the cloud service provider understands the expected workload and utilization requirements of the service.

Scenario 11: Manage resources for cloud services

5.12 Check and improve the SMS and cloud services

S12	Check and improve the SMS and cloud services
Description	The SMS and the cloud services should be reviewed regularly, in order to identify and prioritize opportunities for improvement. Improvements to the SMS can include improvements to the infrastructure, the policies, the agreements and contracts, skills and competencies of personnel, documentation, efficiency and effectiveness of processes or process interfaces, better allocation of resources, etc. Improvements to the cloud service can include improved reliability, functionality, or customer satisfaction. Improvements should be prioritized against defined criteria including business objectives, the cloud service provider's capability and service requirements. Check the fulfilment of cloud service requirements based upon customer feedback, performance measurement, internal audit, management reviews, industry trends or competitive service differentiation, etc. Evaluate service delivery against defined business outcomes and identify opportunities to improve operational efficiency, or realign the services with evolving service targets. Ensure the approved improvements are incorporated into the service management plan. Initiate an improvement project using design and transition of new or changed services process (ISO/IEC 20000-1, Clause 5) or change management process (ISO/IEC 20000-1, 9.2), per criteria defined in change management policy.
Outcomes	— Prioritized improvements to services, processes, policies, skills and competencies, technology, communication, etc., in alignment with business objectives and customer requirements.
Applicable clauses in ISO/IEC 20000-1	— Clause 4.1.2, Service management policy — Clause 4.2, Governance of processes operated by other parties — Clause 4.3, Documentation management — Clause 4.4.1, Provision of resources — Clause 4.5.4, Monitor and review the SMS (Check) — Clause 4.5.5, Maintain and improve the SMS (Act)

S12	Check and improve the SMS and cloud services
	— Clause 5, Design and transition of new or changed services — Clause 6.2, Service reporting — Clause 7.1, Business relationship management — Clause 8.2, Problem management — Clause 9.1, Configuration management — Clause 9.2, Change management — Clause 9.3, Release and deployment management
Guidance on the application to cloud services	Both the SMS and the cloud services should be checked using internal audit and management review, as well as agreed service measurements, including performance and customer satisfaction. Market analysis can also be useful as an input to management reviews. Opportunities for improvement can also be identified through the review of information provided by service reporting, from analysis of the results of customer satisfaction surveys as well as other sources, such as analysis of the marketplace. Improvements should be managed using the requirements specified in ISO/IEC 20000-1, 4.5.5, Maintain and improve the SMS (Act), according to the policy on service improvement. The criteria used for the evaluation of improvements should include consideration of the impact of the improvements on other components of the SMS or on other services, e.g., multi-tenants in cloud services, other non-cloud services. Improvements which are approved should be prioritized, added to the service management plan and controlled using the change management process. Changes with a major impact on customers, the SMS or services should be managed using the design and transition of new or changed services process specified in ISO/IEC 20000-1, Clause 5.
Examples	The cloud service provider in this example understands the importance of continual improvement and innovation to facilitate reduced risk, lower costs, improved quality and competitive advantage. Continual improvement is built into the operation of each process within the SMS and prioritization of improvements are coordinated by individual process owners. Decisions for the prioritization of improvements to individual services are coordinated by the role within the service provider allocated responsibility for the service. Prioritization of improvements having a potential impact across multiple components of the SMS and/or services are coordinated by the senior responsible owner of the SMS or a designated group. Prioritized improvements are reviewed against business objectives and resource capabilities. Results of implemented improvements are also measured and reviewed. Examples of benefits from implemented improvements include: — improved communication, resource allocation and better knowledge management resulting in increased operational efficiency and effectiveness; — better understanding of the cost of services resulting in more cost effective solutions; — improvements identified for one process or service being leveraged to improve other areas of the service provider organization, working effectively with a shared vision; — reduced risk through improved adherence to the change management policy and more comprehensive risk assessment; — improved service reliability, functionality and customer satisfaction resulting in greater profitability and competitive advantage; — enhanced customer experience with the cloud service.

Scenario 12: Check and improve the SMS and cloud services

5.13 Terminate a cloud service contract

S13	Terminate a cloud service contract
Description	The cloud service provider and the cloud customer agree to terminate a cloud service contract and its associated service delivery. The termination of a contract, or early termination, should be managed in accordance with the terms and conditions outlined within the contract, SLA or other agreement.
Outcomes	— Termination of the cloud service contract to the mutual satisfaction of the parties. — Orderly termination of the service delivery as defined in the exit procedure.
Applicable clauses in ISO/IEC 20000-1	— Clause 4.3, Documentation management — Clause 4.4, Resource management — Clause 5, Design and transition of new or changed services — Clause 6.1, Service level management — Clause 6.4, Budgeting and accounting for services — Clause 6.5, Capacity management; — Clause 6.6, Information security management; — Clause 7.1, Business relationship management — Clause 7.2, Supplier management — Clause 9.1, Configuration management — Clause 9.2, Change management — Clause 9.3, Release and deployment management
Guidance on the application to cloud services	The design and transition of new or changed services process, as specified in ISO/IEC 20000-1, Clause 5, is also used to coordinate changes such as the end of the service. The termination of a contract should be managed through the design and transition of new or changed services process, as removal of a service is classified as a change with potential to have a major impact on services or the customer. This process has defined interfaces with the configuration management, change management and release and deployment management processes. Termination should cover both the expected end of a service in accordance with any contracts and any early termination of the service. Either the cloud customer or cloud service provider can terminate the service. The cloud service provider can terminate the service under specific circumstances which should be listed in the terms of the agreement, e.g. misuse of the service. The cloud customer can terminate the contract under specific circumstances which should be listed in the terms of the contract, e.g. with a one week notice period. The cloud service provider should follow an exit procedure that identifies the steps to be taken by both cloud service provider and cloud customer, from both a business and a technical point of view. An orderly termination of the service should include reversibility options, including data retrieval by the cloud customer and backup storage with the cloud service provider, until the customer confirms that the data is no longer required. When the exit procedure has been completed, the cloud customer should cease to consume resources and the customer environment should be cleared. For external customers, if legally permitted, all information relating to the customer should be deleted from the service provider's infrastructure (e.g. data, logs, or monitoring data). Configuration, capacity and financial records should be updated to reflect the termination of the service. At the end of the exit activities, the service provider should provide the customer with written confirmation that the exit criteria have been fulfilled and that the customer's data has been removed from the service provider's systems.