BS ISO/IEC 20000-2:2012

BSI Standards Publication

Information technology — Service management

Part 2: Guidance on the application of service management systems

raising standards worldwide™

National foreword

This British Standard is the UK implementation of ISO/IEC 20000-2:2012. It supersedes BS ISO/IEC 20000-2:2005 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/15/-/8, IT service management.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

ISBN 978 0 580 63608 0

ICS 03.080.99; 35.020

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 March 2012.

Amendments issued since publication

Date	Text affected

BS ISO/IEC 20000-2:2012

INTERNATIONAL STANDARD

ISO/IEC 20000-2

Second edition
2012-02-15

Information technology — Service management —

Part 2: Guidance on the application of service management systems

Technologies de l'information — Gestion des services —

Partie 2: Directives relatives à l'application des systèmes de management des services

Reference number
ISO/IEC 20000-2:2012(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

Contents

Page

Figures and Tables

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 20000-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 7, *Software and systems engineering*.

This second edition cancels and replaces the first edition (ISO/IEC 20000-2:2005), which has been technically revised. The major differences are as follows:

— closer alignment to ISO 9001 and ISO/IEC 27001;

— changes in terminology to reflect international usage;

— new guidance on governance of processes operated by other parties;

— more guidance on defining the scope of the SMS;

— more guidance on continual improvement of the SMS and services;

— more guidance on the design and transition of new or changed services.

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* [Technical Report]

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

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

Introduction

This part of ISO/IEC 20000 provides guidance on the application of service management systems (SMS) based on ISO/IEC 20000-1. 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 intent of this part of ISO/IEC 20000 is to enable organizations and individuals to interpret ISO/IEC 20000-1 more accurately, and therefore use it more effectively.

An SMS is defined in ISO/IEC 20000-1 as a management system to direct, monitor and control the service management activities of the service provider. The SMS should include what is required for the planning, design, transition, delivery and improvement of services. At a minimum this includes service management policies, objectives, plans, processes, process interfaces, documentation and resources. The SMS encompasses all the processes as an over-arching management system, with the service management processes as part of the SMS.

Coordinated integration and implementation 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 operation of processes as specified in Clauses 5 to 9 requires personnel to be well organized and coordinated. Appropriate tools may be used to enable the service management processes to be effective and efficient. The most effectual organizations consider the impact of the SMS through all stages of the service lifecycle, from planning and design to transition and operation, including continual improvement.

This part of ISO/IEC 20000 provides examples and suggestions to enable organizations to interpret and apply ISO/IEC 20000-1, including references to other parts of ISO/IEC 20000 and other relevant standards.

Users of International Standards are responsible for their correct application. It is important for organizations and individuals using ISO/IEC 20000 to understand the points listed below.

— ISO/IEC 20000-1 does not purport to include all necessary statutory and regulatory requirements, or all contractual obligations of the service provider. Conformity to ISO/IEC 20000-1 does not of itself confer immunity from statutory obligations.

— ISO/IEC 20000-1 is applicable to internal and external, large and small, and commercial and non-commercial service providers.

— ISO/IEC 20000-1 promotes the adoption of an integrated process approach when planning, establishing, implementing, operating, monitoring, measuring, reviewing, maintaining and improving an SMS for the design, transition, improvement and delivery of services that fulfil service requirements.

ISO/IEC 20000 promotes the application of the methodology known as “Plan-Do-Check-Act” (PDCA) to the SMS and the services. The PDCA methodology, shown in Figure 1, can be briefly described as follows:

Plan: establishing, documenting and agreeing the SMS including the policies, objectives, plans and processes necessary to design and deliver services in accordance with business needs, customer requirements and the service provider's policies.

Do: implementing and operating the SMS for the design, transition, delivery and improvement of the services.

Check: monitoring, measuring and reviewing the SMS and the services against the plans, policies, objectives and requirements and reporting the results.

Act: taking actions to continually improve performance of the SMS. This includes the service management processes and the services.

When used within an SMS, the following are the most important aspects of an integrated process approach and the PDCA methodology:

a) understanding and fulfilling the service requirements to achieve customer satisfaction;

b) establishing the policy and objectives for service management;

c) designing and delivering services based on the SMS that add value for the customer;

d) monitoring, measuring and reviewing performance of the SMS and the services;

e) continually improving the SMS and the services based on objective measurements.

Where other management systems are present, the implementation of an SMS, with the adoption of a process approach and the PDCA methodology, enables the service provider to align or fully integrate the organization's management systems. For example, it is possible to integrate ISO/IEC 20000 with a quality management system based upon ISO 9001 and/or an information security management system based upon ISO/IEC 27001. An integrated management system approach increases efficiency, establishes clear accountability and traceability and enhances organizational planning, communication and control.

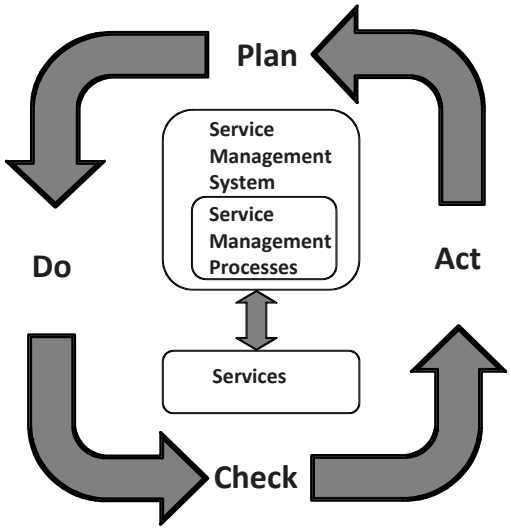

Figure 1 — PDCA methodology applied to service management

As stated in ISO/IEC 20000-1:

"ISO/IEC 20000 can be used by:

a) *an organization seeking services from service providers and requiring assurance that their service requirements will be fulfilled;*

b) *an organization that requires a consistent approach by all their service providers, including those in a supply chain;*

c) *the service provider that intends to demonstrate its capability for the design, transition, delivery and improvement of services that fulfil service requirements;*

d) *a service provider to monitor, measure and review its service management processes and services;*

e) *a service provider to improve the design, transition, delivery and improvement of services through the effective implementation and operation of the SMS;*

f) *an assessor as the criteria for a conformity assessment of a service provider's SMS to the requirements in this part of ISO/IEC 20000."*

This part of ISO/IEC 20000 can be used by an organization looking for guidance on how to improve service management, whether or not it is interested in seeking certification.

Information technology — Service management —

Part 2:
Guidance on the application of service management systems

1 Scope

1.1 General

This part of ISO/IEC 20000 provides guidance on the application of an SMS based on ISO/IEC 20000-1. This part of ISO/IEC 20000 provides examples and suggestions to enable organizations to interpret and apply ISO/IEC 20000-1, including references to other parts of ISO/IEC 20000 and other relevant standards. This part of ISO/IEC 20000 is independent of specific best practice frameworks and the service provider can apply a combination of generally accepted guidance and their own techniques.

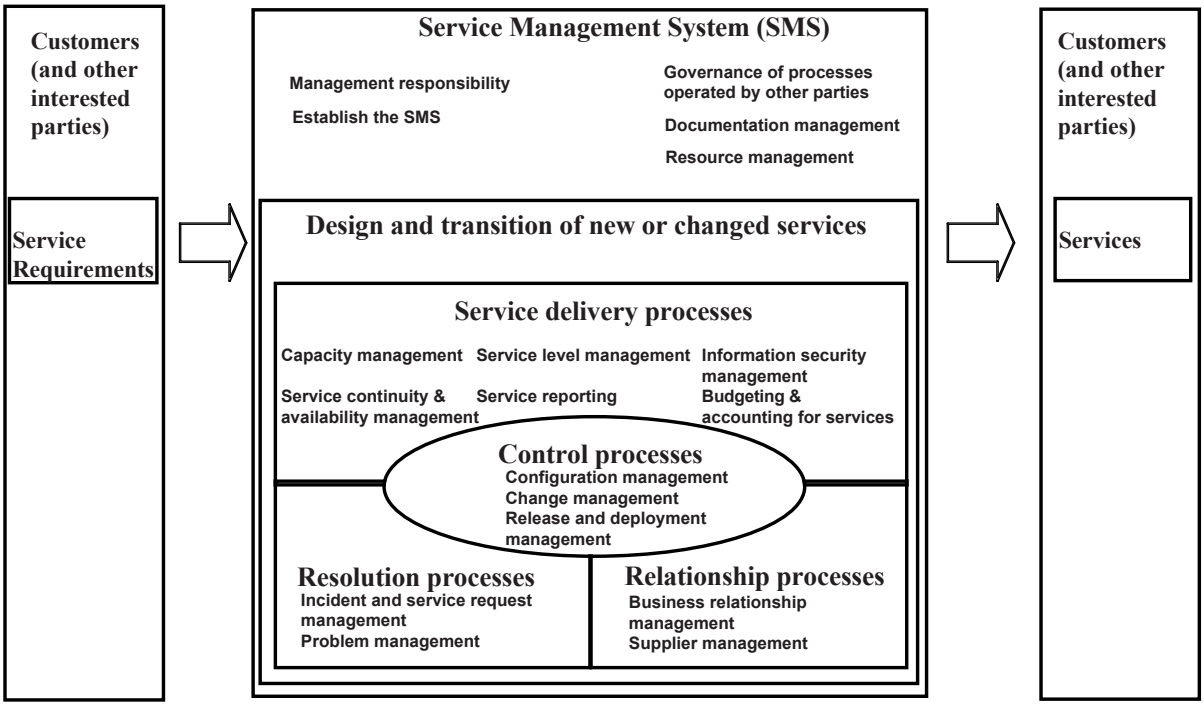

Figure 2 — Service management system

Figure 2 shows the processes from Clauses 6 to 9 in the central box. The Clause 5 design and transition of new or changed services process surrounds the Clause 6 to 9 processes. This shows that the new or changed services are operated by the processes in the central box. When there are no new or changed services to which Clause 5 applies, all services can be delivered directly by Clauses 6 to 9.

The interfaces between the service management processes and the relationships between different components of the SMS may be implemented differently by different service providers. The nature of the relationship between the service provider and the customer can also influence how the SMS is implemented to fulfil the requirements of ISO/IEC 20000-1. For these reasons the interfaces between processes are not represented in Figure 2.

1.2 Application

The service provider is accountable for the SMS and therefore cannot ask another party to fulfil the requirements of Clause 4 of ISO/IEC 20000-1:2011. For example, the service provider cannot ask another party to provide the top management and demonstrate top management commitment or to demonstrate the governance of processes operated by other parties.

Some activities in Clause 4 may be performed by another party under the management of the service provider. For example, service providers can engage other parties to conduct internal audits on their behalf. Another example is where a service provider asks another party to create the initial service management plan. The plan, once created and agreed, is the direct responsibility of and is maintained by the service provider. In these examples, the service provider is using other parties for specific short-term activities. The service provider has accountability, authorities and responsibilities for the SMS. The service provider can therefore demonstrate evidence of fulfilling all of the requirements of Clause 4 of ISO/IEC 20000-1:2011.

The service provider can show evidence of fulfilling all requirements directly or can show evidence of fulfilling most of the requirements directly as well as the governance of processes operated by other parties. If the service provider relies on other parties for operation of the majority of the processes in Clauses 5 to 9, the service provider is unlikely to be able to demonstrate governance of the processes. However, if other parties operate only a minority of the processes, the service provider can normally fulfil the requirements specified in ISO/IEC 20000-1.

The defined, agreed and documented accountability, authorities and responsibilities for the SMS are readily accessible to both the service provider and other relevant parties. To fulfil the requirements of ISO/IEC 20000-1 the service provider can agree changes to the terms of existing contracts or other documented agreements.

ISO/IEC 20000 excludes the specification of, or specific guidance about, any product or tool. However, organizations can use this part of ISO/IEC 20000 to help them use or develop products or tools that support operation of the SMS.

2 Normative references

The following documents are indispensable for the application 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*

3 Terms and definitions

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

4 Service management system general requirements

4.1 Management responsibility

4.1.1 Management commitment

4.1.1.1 Top management responsibilities

Top management should be the management who direct, monitor and control the service provider at the highest level.

Top management should be aware that fulfilling the requirements of ISO/IEC 20000-1 includes:

a) demonstrating their commitment to be involved at all stages of the SMS, starting with the planning and establishment of the SMS and continuing through the operation, monitoring, measurement, review, maintenance and continual improvement of the SMS;

b) demonstrating their accountabilities and responsibilities for the SMS;

c) ensuring that the service requirements, scope of the SMS, service management policy and objectives are understood and acknowledged by all interested parties of the SMS;

d) ensuring that the service management plan is created, implemented, maintained and aligned with business objectives;

e) ensuring the provision of adequate resources to fulfil the service management objectives and to adhere to the service management policy;

f) ensuring that the performance of the SMS is reported to the top management level;

g) achieving the objectives of service management, including when these vary due to changing business needs or service requirements;

h) ensuring that risks to services are minimised, e.g. by assessing risks associated with changes and taking action.

Top management should also ensure that all service lifecyle stages are delivered to the agreed levels, as defined in the service requirements. The service lifecycle includes planning, implementation, operation, monitoring, measurement, review, maintenance and continual improvement. The service lifecycle also includes transfer of the service to a customer or a different party or eventual removal of the service.

Top management should be aware that they are accountable for ensuring that the SMS and the services delivered by the SMS are assessed and reviewed. Assessments should include the service provider's own reviews and internal audits, as well as external audits. Further information about management reviews can be found in Clause 4.5 of this part of ISO/IEC 20000.

4.1.1.2 Evidence of top management commitment

Without management commitment, it is possible that management decisions can be made that conflict with requirements for an effective SMS. Examples can include reallocation of resources to other projects, lack of communication about the SMS and unresolved conflicts in process design.

There should be evidence of management commitment and accountability available for review by an assessor. Top management should be able to provide evidence based on records of their involvement in:

a) regular meetings about the SMS, e.g. chairing planning meetings so that the SMS remains aligned with business needs and new or changed service requirements;

b) ensuring the SMS includes a definition of the scope, the service management policy, service management objectives and the service management plan;

c) approval of the service management policy, service management objectives and of the service management plan;

d) approval of processes and procedures consistent with, and supportive of, the SMS policies.

Top management approval of the service management plan is important because the plan can have implications for commitments to the customer, planning activities for suppliers and the allocation of resources for improvements and other changes.

The alignment between policies, processes and procedures enables top management direction to be cascaded to all service provider personnel. This should align management decisions with the way the service provider's personnel operate on a day to day basis.

4.1.1.3 Top management communications

Top management should be actively involved in an ongoing programme of communications. Communications should be directed by approved communications procedures as described in Clause 4.1.3.2.

Top management should be actively involved in an ongoing programme of communications to explain how the established SMS is aligned with business objectives and customer expectations. This is important to the success of the SMS because personnel who understand the purpose and importance of the SMS are less likely to resist changes due to fear or lack of knowledge. Top management communications about the SMS can be an opportunity for the service provider to motivate their own organization. Additionally, an appreciation of the importance of the SMS by both management and personnel, should reduce the risk or likelihood that decisions will be made or solutions delivered that are in contradiction with the SMS.

The programme of communications should explain the following:

a) organizational changes, policies, standards, vision and mission as well as business targets;

b) business needs, e.g. the relationship between the SMS and the services delivered, as well as how these support the defined organizational goals and objectives;

c) how the established SMS is aligned with business objectives and customer expectations;

d) how the service management policy, service management objectives and service management plan support fulfilment of service requirements;

e) customer requirements, e.g. service targets, predicted capacity based upon predicted demand, information security and service continuity to support business continuity;

f) statutory requirements, such as working hours, health and safety and data protection, which vary by country;

g) regulatory requirements, e.g. that records are kept for a specific period of time;

h) contractual requirements, e.g. a requirement to sign a non-disclosure agreement before having access to the service provider's information;

i) documented agreements with the customer;

j) regular analysis of data gathered through measurement of the SMS and components, e.g. process measurements.

Additionally, communications can be an opportunity for the service provider to motivate their own organization.

A programme of communications is important to the success of the SMS because personnel who understand the purpose and importance of the SMS are less likely to resist changes due to fear or lack of knowledge. Communications should generate an appreciation of the importance of the SMS by both management and personnel and reduce the risk or likelihood that decisions will be made or solutions delivered that are in contradiction with the SMS.

The outcome of these communications activities should be that people understand their role in service management and how they contribute to fulfilling the service requirements and meeting the service management objectives.

4.1.1.4 Service management objectives

Top management should define the agreed objectives for service management. Objectives should be aligned with the business objectives and with the service management policy.

For example, generic service management objectives can include the following:

a) enable increased business agility through faster delivery of new or changed services;

b) reduce unplanned non-availability for business critical services;

c) optimize the cost of the services delivered through operational efficiency;

d) increase quality of services while reducing risk.

Actual service management objectives should be defined so that achievements against the objectives can be accurately measured. Measurement should also enable opportunities for improvement to be prioritized.

Objectives should be a key input into the service management plan. The plan should identify actions for achievement of the objectives and alignment with other components of the SMS.

Service management objectives should be reviewed at regular intervals to enable top management to decide how and when they should be revised.

The service provider should ensure that the effectiveness of each component of the SMS is measured to assess the effectiveness of support for the service management objectives. For example, measurement of the effectiveness of the support of the objectives by a specific process. The measurements should also demonstrate value of the SMS in supporting the business objectives.

The service provider can find it useful to measure the contributions of individuals towards achievement of the objectives. This will facilitate personnel supporting the SMS to work in an integrated way toward the same goals.

4.1.1.5 Service management plan

The service management plan should facilitate the coordination of all SMS initiatives to ensure the achievement of the service management objectives. The plan and policies should also be aligned.

The plan can be a powerful mechanism for enabling end to end visibility and control. It should also prevent incompatible initiatives from being approved or implemented. The plan should enable the utilization of resources and capabilities to be as efficient and effective as possible.

The plan should be communicated to all interested parties. This should ensure a common understanding of the scope of initiatives, the tasks, timeframes and allocated responsibilities. Allocated responsibilities should be included in the performance measurements of everyone involved in the SMS, including those involved in initiatives of the service management plan.

The plan should not be considered to be completed when the SMS is implemented. It should exist indefinitely by being amended to accommodate the changing business needs, customer requirements or priorities of the service provider.

The service management plan can consist of one single plan or a programme of coordinated changes managed centrally with some changes implemented locally.

The service provider should always be aware of the need to keep all changes implemented locally under the overall management of the service management plan. For example, an improvement to a process may be performed locally, under the local control process owner, but it is included in the centrally managed overall programme.

Plans for a specific purpose, e.g. for the service continuity and availability management process, may be referenced from the overall service management plan rather than included within it. The specialist plans and their alignment with the overall plan should be reviewed at a frequency that is suitable for the rate of change. This should be at least annually.

Any changes resulting from reviews or changes to service requirements or individual plans should be documented in the overall service management plan. For example, office hours changing to full 24 hour operation, replacement technology or changes to skills.

The contents of the service management plan should include:

a) an introduction;

b) a description of the organizational functions of the service provider;

c) priorities of initiatives;

d) expected outcomes aligned to business objectives;

e) performance measures;

f) service targets;

g) project plans;

h) tasks and dependencies;

i) benefits realisation achieved as the result of previously implemented improvements;

j) timeframes and persons responsible for carrying out the initiatives of the plan;

k) risks and risk mitigation options.

Risks to the service management plan should be identified, assessed and managed both initially and as part of the PDCA methodology. The risk assessment should cover the inputs, outputs, activities and the responsibility and accountability for mitigation of risks. The plan should also be designed to ensure the agreed objectives and service requirements will be achieved.

4.1.1.6 Resources to support the service management plan

The resources necessary to achieve the service management objectives should be documented in the service management plan. The following should be considered:

a) human resourcing should take into account the skills and experience of the individuals and not just be based solely on the number of people;

b) technical resources, e.g. infrastructure and capacity to achieve the required performance;

c) tools to support the processes in the SMS;

d) office accommodation, other facilities and facilities for service continuity;

e) data and information, e.g. details of customer requirements, the customer's business plans, the service provider's business needs, service management policies, performance measurements and other reports;

f) financial resources, budgeted at a level of detail suitable to manage the planning, implementation, operation and improvement of the SMS;

g) quantity and availability of the personnel of the service provider, and their hours worked;

h) processes, procedures and timescales for the introduction, retention and succession planning of suitably skilled personnel.

4.1.1.7 Contents of the service requirements

Clause 3.34 of ISO/IEC 20000-1 includes the needs of the business, the customer and the users of the service and needs of the service provider in the definition of service requirements. Top management should be responsible for ensuring that the services delivered fulfil the agreed service requirements.

Both the customer's requirements and the business needs should be documented, monitored, reviewed and managed to ensure ongoing alignment with new or changed services as well as with services in the live environment.

Service requirements should include required service targets and quality expectations. The needs of the service provider should include details of resource and capability requirements. The service requirements are an input into the SMS, shown in Figure 2.

Examples of service requirements can include:

a) a service in use, including the service level requirements;

b) quality criteria for the design of new or changed services;

c) priorities for the business criticality of services;

d) requirements for availability;

e) regulatory requirements;

f) information security requirements.

4.1.1.8 The role of top management in agreeing and meeting service requirements

Top management should ensure that the service requirements are defined in terms of:

a) desired results that customers expect e.g. improved effectiveness, efficiency, satisfaction;

b) the constraints that the service will remove;

c) functionality of a service from the customer's perspective, including the needs of the users of the service, often referred to as 'fit for purpose';

d) patterns of business activity and demand that the service should support;

e) assurance that the service and products will be provided or will meet certain agreed specifications, often referred to as warranty.

A typical characteristic of warranty is that it is defined in terms of service continuity, availability, capacity and security. For example, warranty ensures that the service will remain fit for purpose even at degraded service levels due to major disruptions or disasters. Warranty should also ensure security for the services.

The needs of the users of the service should be defined within the context of the needs of the customer. This should describe the benefit a user will gain from using the service as part of performing their work activities. Examples are given below.

EXAMPLE 1 Removing constraints. A desired change to a service may enable users to access a service remotely instead of only from fixed locations.

EXAMPLE 2 Functionality. A desired improvement in the processing time for business transactions.

EXAMPLE 3 Performance. A user may need to process one procurement transaction per minute and 50 transactions in an hour.

4.1.1.9 Service provider's needs

From the service provider's viewpoint, the service requirements should include those listed below.

a) Requirements to ensure delivery of the business needs and wider interests of the organization that owns the service provider organization. For example, the requirements to fulfil policies, standards, statutory and regulatory requirements, and contractual obligations.

b) Scope of the SMS to direct, monitor and control an integrated set of service management processes and activities. This includes the requirements for assets, capabilities and resources required for the design, transition, delivery and improvement of services. For example, the organizational units, people, process, information and technology required to support the SMS.

c) Known limitations of the SMS, for example human, technical, information and financial resource constraints.

d) Requirements for the measurement, auditing, reporting and improving of services delivered against the defined business objectives.

e) Requirements for the measurement, auditing, reporting and improving the effectiveness of the SMS.

4.1.1.10 Conflicting requirements

If the service provider establishes that a conflict in requirements has occurred, action should be taken. Examples of conflicts in requirements include the following.

a) If there are conflicts between customer requirements and customer business needs, the conflict should be resolved by the customer, e.g. a customer requirement that is in conflict with the strategic direction of the business. Alternatively, the service provider can analyse the differences and propose revised service requirements.

b) Conflicts between customer requirements and the service provider's own business needs can occur when customer requirements are unrealistic in terms of priorities, costs or funds available. The nature of the conflict and why requirements are unrealistic should be clearly communicated to the customer.

c) Service requirements conflicting with any statutory or regulatory requirements, or contractual obligations should be resolved. For example, the distribution of software can be restricted by a licence agreement in a way not compatible with the customer's requirements for access to new versions of software.

The service provider should ensure that any risks arising from conflicts are assessed and quantified in order to identify methods of minimizing risks. The assessment should include the risk to customer satisfaction and the ability to meet customer requirements and objectives.

Conflicts and their potential impact should be documented and discussed with the customer so that they can be resolved. If a conflict is identified after the design of the service is agreed the conflict should be resolved as a corrective action or as an opportunity for improvement.

4.1.1.11 Risks to the service

Top management should ensure that risks to the SMS and the services are identified, documented and assessed. Risks to a service can include the failure to fulfil regulatory and statutory requirements or contractual obligations. For example, failure to meet software licence requirements or failure to provide proof of financial probity.

Top management should also ensure that all identified risks are managed, including ensuring that:

a) options are developed and documented to manage identified risks;

b) preferred options are agreed with the customer;

c) agreed options for risk mitigation are implemented when necessary.

NOTE The service provider will find the requirements and advice in ISO 31000 on risk management helpful.

4.1.2 Service management policy

4.1.2.1 Guidelines for the service management policy

The service management policy should be specific to the service provider's circumstances and have a customer focus. The policy should not be a generic, broadly applicable statement. Instead, the policy should reflect the circumstances and objectives of the service provider.

The policy should be based on the agreed scope of the SMS and therefore supportive of the service provider's service management objectives and the service management plan.

The policy should represent top management direction and commitment to fulfil service requirements. The policy should also ensure the fulfilment of the requirements for the design and transition of new or changed service process in Clause 5 of ISO/IEC 20000-1:2011.

The policy should give clear top management direction to the service provider's managers and personnel.

EXAMPLE 1 Services are aligned to the business objectives of the customer.

EXAMPLE 2 Changes to processes or procedures are only made through the change management process.

EXAMPLE 3 Roles and responsibilities for the service management processes are defined and documented in a consistent manner and personnel performance is measured against achievement of those responsibilities.

The service management policy should be structured so that it can be used to assess whether the service provider's service management objectives are being fulfilled. For example, it should be possible to demonstrate a link between the service management policy and what is being done to achieve the service provider's service management objectives. The service management policy should be structured to enable measurement of adherence to the policy.

The service provider should also be able to demonstrate that this link between the service provider's objectives and the service management policy has been effective since the service management policy was originally agreed.

The service management policy should clearly define levels of authority, e.g. making it possible to determine whether an improvement initiative should be approved by an individual process owner or by top management.

The service management policy should be communicated and understood within the service provider's own organization. The service management policy can also be made available to the customer and suppliers as required. References to the policy being discussed, understood and used appropriately can be used as evidence of fulfilment of this requirement. For example, meeting minutes, personnel surveys, supplier contracts, sub-contractor agreements, requests for change to the policy or requests for clarification, policy impact on processes, procedures and behaviours during standard and unplanned operations, customer surveys, supplier surveys.

Top management should also be responsible for ensuring that the service management policy is reviewed at suitable intervals, at least annually. This should identify any deficiencies and ensure continual alignment with business needs and customer requirements. Quality criteria applied during the review of the service management policy should take into consideration the following:

a) the validity of the policy against service requirements;

b) the adequacy of the review frequency;

c) the alignment between the policy and the service management objectives;

d) the alignment between the policy and the service management plan;

e) the alignment between the policy and the service management processes;

f) whether the review is documented, approved, tracked, appropriate and practicable;

g) the adequacy of the framework for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the SMS;

h) remediation and improvement actions identified in previous reviews and audits of the SMS.

4.1.2.2 Improvements and other changes to the policy

Following a review of the service management policy, if a deficiency is found, top management should ensure that it is corrected. Deficiencies should be corrected either as a change to the policy, service management objectives, plan, processes or procedures.

The policy should also be updated to reflect any changes to the service management objectives or to the scope of the SMS.

4.1.3 Authority, responsibility and communication

4.1.3.1 Authority and responsibility

The service provider should ensure that the authorities and responsibilities for all aspects of the SMS are defined. Role descriptions should be agreed, allocated to individuals, communicated to all personnel and kept up to date through a document management procedure. The service provider should ensure that all personnel are encouraged to establish and maintain an awareness of how their activities contribute to the achievement of the service management objectives.

4.1.3.2 Communication procedures

Top management should be accountable for ensuring that communication procedures are designed, transitioned, implemented and used. Top management may delegate the actual design of the procedures. However, they should approve them in advance of implementation and enforce their use. Top management should be actively involved in the communication procedures.

Top management should understand the value of personnel awareness, motivation and participation in effective service management and continual improvement. The communication procedures should encourage personnel motivation. For example, communicating the successful results of personnel participation in improvement activities can have a significant motivational effect.

Communication procedures should cover at a minimum the method of delivery, the timing and/or frequency and the audience. The procedures should also cover escalation mechanisms, contact details, distribution list maintenance, communication methods, tools and information access, schedules and responsibilities.

Communication procedures should include the following.

a) the method of delivery;

b) the timing and frequency;

c) the audience for specific communications;

d) escalation mechanisms;

e) contact details for audience of communication;

f) distribution list maintenance;

g) communication methods;

h) tools and information access;

i) schedules and responsibilities.

Communication may take different forms and will be dependent on the culture or the organization, the individual being communicated with and that person's role in the organization.

Top management communications methods can include personnel orientation material, briefings and workshops, internal personnel publications, email, social media, or personnel feedback forums.

4.1.4 Management representative

4.1.4.1 Understanding of responsibilities

The management representative should be the member of the service provider's management team who has the authority to ensure that the SMS is established, used, improved over time and in alignment with the changing needs of the business. This authority should include ensuring the service management processes have appropriate interfaces with one another and are integrated with the rest of the SMS.

The service provider should ensure it is clear which person is the management representative and that the management representative's responsibilities and authority levels are understood by:

a) process owners, who have the authority and responsibility for ensuring that the process, its interfaces to other processes and integration within the SMS are documented, adhered to, measured and improved;

b) service owners, who have the authority and responsibility for a service throughout its lifecycle, including design, transition, implementation, improvement, and retirement;

c) other service provider personnel;

d) internal groups;

e) suppliers, including lead suppliers;

f) the customer.

NOTE For examples on interfaces between service management processes and integration with other components of the SMS, please see Annex A in this part of ISO/IEC 20000.

4.1.4.2 Responsibilities

The management representative should be responsible for ensuring that the following are achieved:

a) all aspects of the management responsibilities specified in ISO/IEC 20000-1 are performed, including those required by top management;

b) service requirements are documented;

c) the SMS and the definition of scope fulfil the service provider's own needs, the needs of the customer and users of the services;

d) the scope and details of the SMS are checked at suitable intervals to ensure that the service requirements continue to be fulfilled, e.g. if the needs of the customer change, it is possible that the SMS or the scope of the SMS also needs to change;

e) the service management policy and objectives are used as the basis for decisions during initial planning of the processes to the design of the processes and operation and improvement of the processes;

f) design of the processes starts with identification of the inputs and outputs and any activities performed as part of the processes;

g) the policy and objectives dictate the criteria for prioritizing the improvements to service management processes;

h) service management processes have appropriate and effective interfaces with one another and are integrated with the rest of the SMS;

i) the PDCA methodology is implemented and used for continual improvement of the SMS and services;

j) internal audits and assessments of the SMS are carried out at regular intervals, in order to measure the ability of the SMS to achieve service management objectives and to fulfil service requirements.

4.1.4.3 Asset management

Top management should be aware that ISO/IEC 20000-1 requires that all assets used to deliver services are managed according to relevant statutory, regulatory and financial requirements and contractual obligations. Assets should be managed by effective procedures.

Examples of assets that should be managed include software licences, mobile devices, infrastructure components, people, contracts, procedures and other documents. Service providers should be able to accurately identify the location, status and other relevant details about assets.

Top management should be aware that asset management requires an accurate configuration management database (CMDB), or equivalent means of record keeping, to be established and used effectively. Information in the CMDB should be kept current by effective service management processes, e.g. changes to the CMDB to be approved via the change management process.

Statutory requirements can include privacy and data protection laws as well as intellectual property and copyright laws. Other statutory requirements can relate to the protection of customer information assets or protection of financial information.

Regulatory requirements and contractual obligations can include ensuring assets comply with business licence requirements and standards, e.g. security standards for encryption of sensitive information on laptops.

NOTE The service provider will find the ISO/IEC 19770 series on software asset management helpful.

4.1.4.4 Reporting by the management representative

Reports to top management should include but not be limited to the topics in Clause 4.1.4.2. For example, the reports should identify continual improvement opportunities achieved using the PDCA methodology. This should be based on reports of the performance of the SMS and services.

The frequency and level of detail of reports should be suitable for the level of activity, categories of change and seriousness of any issues and risks identified by the management representative. Options for changes to correct deficiencies should be provided to assist the prioritization of action and the subsequent decision made by top management.

Reports to top management should clearly articulate the value delivered by the SMS in support of the business objectives.

4.2 Governance of processes operated by other parties

4.2.1 Guidance on processes operated by other parties

The service provider should be aware that it can fulfil the requirements of ISO/IEC 20000-1 by demonstrating governance of the processes operated by other parties, for a minority of the processes.

The service provider should be able to identify all service management processes or parts of processes that are operated by other parties. The service provider should have end-to-end visibility of the performance of other parties operating any of the processes in Clauses 5 to 9.

The service provider should be able to demonstrate control of all parties operating processes in the SMS, and this should be supported by all contracts and other documented agreements.

4.2.2 Other parties

Other parties include:

a) internal groups who are organizational units inside the same organization as the service provider, but not within the direct control of the service provider, e.g. a data centre or a specialist security team;

b) a customer acting as a supplier, e.g. the customer performing some of the activities of incident and service request management;

c) suppliers, e.g. outsourcing of the testing done as part of the release and deployment management process.

Suppliers can also be lead suppliers with responsibilities for managing sub-contracted suppliers.

4.2.3 Demonstration of accountability and authority

The service provider should demonstrate process accountability and authority by providing evidence such as that described below.

a) The service provider's accountability for effectiveness of the service management processes operated by the service provider or another party, e.g. the matrix of decision makers, proof of authorisation levels within the service provider's own organization.

b) That the service provider has the power to require adherence to a process. For example, establishing the information security policy, using controls, detecting breaches and initiating corrective actions. Another example includes providing evidence that practices have been changed at the request of the service provider.

c) Analysis of process records, including measurements by the service provider. For example, considering a complete set of incident records or an incident report and taking decisions based on the content, even if the incident records are provided by another party that operates the incident management process.

d) Controlling the definition of all processes in the SMS, including any processes in Clauses 5 to 9 operated by other parties. This includes the interfaces between each process. For example, documenting, agreeing and operating the interfaces and dependencies of the change management process with the configuration management process. Additional detail is provided in Clause 4.2.4.

e) Controlling the planning of and setting priorities for improvements to all processes in Clauses 4 to 9 of ISO/IEC 20000-1:2011. For example, assessing and prioritizing an improvement in the capacity management process, even if the process is operated by another party.

The service provider can request other parties to operate processes designed and documented by the service provider. Alternatively, the service provider can approve the processes that the other parties design, document and operate.

The service provider should be aware that if it relies on other parties for operation of the majority of its processes, it is unlikely that it will be possible to demonstrate adequate governance of the processes.

NOTE The governance of processes operated by other parties is described in ISO/IEC TR 20000-3:2009.

4.2.4 Process performance and compliance

The service provider should ensure each process described in Clauses 5 to 9 delivers the desired outcomes and contributes to meeting the service management objectives.

Governance of processes operated by other parties should include a definition of the process, including:

a) identification of process ownership, e.g. what group or manager within the service provider's organization is responsible for the process;

b) responsibility for operation, e.g. what group or manager is responsible for the operation of the process;

c) the objective of the process, outcomes of the process and contribution to service requirements and service management objectives being met;

d) process inputs and outputs and which party generates these;

e) definition of the interfaces to other processes, including the service management processes, e.g. data passed between processes or the handover of activities or information from one party to another;

f) definition of the interfaces between processes and other components of the SMS, e.g. between the processes and the service management policy and objectives;

g) the frequency and method by which information passes to and from each process;

h) documents and records required by the service provider for governance of processes operated by other parties and who generates these;

i) clear accountabilities and responsibilities for all required activities.

The definition of interfaces between SMS components should include the methods by which the service management processes are established and continually improved to support the service management policy and objectives, and the changing needs of the business. For example, how the SMS components including processes should be measured against their alignment with and support of the service management policy.

4.2.5 Determining process performance and compliance

The service provider should ensure that all processes are effective by:

a) documenting and agreeing with the other parties the frequency and format of documents and records to be made available to the service provider and to other parties;

b) establishing the review cycle and criteria for process assessments;

c) conducting an assessment of the process against the requirements of ISO/IEC 20000-1;

d) defining the obligations of other parties within the process review activity;

e) analysis of process performance;

f) analysis of interfaces between processes or parts of processes operated by other parties and other processes, as well as policies and plans;

g) analysis of alignment between processes or parts of processes operated by other parties and service management objectives;

h) setting priorities and planning activities for improvements or corrections to optimise processes.

4.2.6 Controlling the planning and prioritization of process improvements

The service provider should be able to demonstrate that they control the priority given to improvements of all processes, including those operated by other parties.

EXAMPLE 1 A proposed improvement to the change management process can be considered to have greater benefits to the organization than a proposed improvement to the release and deployment management process. The prioritization of process improvements should be aligned with the business objectives and the service requirements.

EXAMPLE 2 An improvement to the incident management process operated by another party should be directed by the business objectives and service requirements of the service provider and the service provider's organization.

4.3 Documentation management

4.3.1 Establish and maintain documents

4.3.1.1 Documents as evidence

The service provider should ensure that evidence is available for any audit of the SMS. Much of the evidence should exist in the form of documents. Documents may be any type, form or medium suitable for their purpose, e.g. paper based, electronic files, in a database or word-processor.

The following documents can be considered as evidence for an audit of the SMS:

a) service management policies, objectives and plans;

b) process and procedure documents;

c) a catalogue of services;

d) service documents including designs, requirements specifications, SLAs, acceptance criteria and service reviews;

e) contractual documents, including specification of requirements and change control;

f) audit planning activities and reports;

g) documents describing or associated with a particular change, such as change planning activities.

The service provider should be aware that some documents, such as policies, are required by ISO/IEC 20000-1 to fulfil the requirements of specific processes. In addition, an organization may wish to consider additional documents, including policies, to provide further clarity or ensure effective operation or improvement of the SMS and delivery of the services.

Records are a special type of document and should also be made available as evidence.

4.3.1.2 Production of documents, including records

The service provider should understand that an effective procedure is essential for the production of documents, including records. This includes the use of a naming and numbering system that aligns with the

purpose and revision history of documents. The use of templates and standardised format can reduce the effort of creating, accessing, updating and using the content.

There should be evidence of an acceptance procedure for documents in accordance with the roles and responsibilities for documents defined in the SMS.

The service provider should also understand that documents, such as SLAs, policies and plans, can be interdependent, e.g. an information security policy defining what information can be stored on mobile devices or a server that supports the delivery of an email service. These interdependencies should be understood and managed when changes are made to documents.

Records, which show what has actually been done or what has happened, do not always require an acceptance procedure, e.g. an incident record. An incident record should be updated as the incident is progressed to closure. To operate an acceptance procedure each time an incident record is updated would cause unacceptable delays in the resolution of incidents.

NOTE Documents and records need not be unique to the SMS. Provided they meet the requirements of ISO/IEC 20000-1, they may also cover the requirements of standards such as ISO 9001 or ISO/IEC 27001.

4.3.2 Control of documents

Control of documents should be recognised as essential. Control of documents should include periodic review, with updating or archiving if necessary. The review should be at least annual. Documents should be protected from damage, e.g. due to poor environmental conditions and hardware malfunction.

Control can provide visibility of the impacts of changes, e.g. a change to an SLA which impacts contracts with other parties or the availability requirements. The service provider should ensure that documents are controlled through the use of:

a) version naming and numbering;

b) assigned responsibility for writing, editing, reviewing, approving, updating, removing and archiving documents;

c) change records that indicate the date, author, approval of change and nature of revisions;

d) assessment of changes to identified documents by the change management process prior to approval;

e) identification of the relationships between specific documents and other components of the SMS;

f) document access control mechanisms and distribution;

g) a procedure to approve documents for use;

h) a procedure to review and update as necessary and re-approve documents;

i) a procedure to ensure that documents of external origin determined by the service provider to be necessary for the planning and operation of the SMS are identified and their distribution controlled;

j) a procedure to ensure that documents are disposed of in accordance with the information security policy and regulatory and statutory requirements;

k) a procedure for archiving out-of-date documents.

To achieve control of documents, techniques from document management, knowledge management, change management and configuration management can be used, e.g. a policy on how document versions are shown.

The service provider should identify those documents subject to the document control procedures. This can include documents of external origin such as standards, regulations or customer documents. The service provider should distinguish between the different types of control to be applied to different types of items, e.g. between those of internal and external origin or documents requiring different security due to the different content.

Documents that should be controlled include all those listed in Clause 4.3.1.1. Many documents are classed as CIs, which are therefore also controlled through the configuration management process. Where document control is achieved by electronic means, special attention should be given to appropriate approval, access, distribution, media, and archiving procedures.

NOTE 1 The service provider will find ISO 9001:2008, Clauses 4.2.3 and 4.2.4 helpful.

NOTE 2 For further information, see ISO/IEC TR 20000-4:2010, Clause 5.10, Information item management process.

4.3.3 Control of records

Records associated with the SMS should be aligned to the requirements of ISO/IEC 20000-1, statutory and regulatory requirements and contractual obligations. For example, retention of records, archival and disposal practices. Records that should be retained include the record of document reviews and the tracking of review comments to resolution. These requirements and obligations should influence the design of the SMS.

Any conflicts between the statutory and regulatory requirements or contractual obligations and the requirements of ISO/IEC 20000-1, should be resolved. This should apply to all records that are created and used as part of the SMS. This includes but is not limited to documentation, logs and database records, known error records, CIs, incident records and request for change records.

Records established to provide evidence of conformity to requirements and of the effective operation of the SMS should be controlled. The organization should establish a documented procedure to define the controls needed for the identification, storage, protection, retrieval, retention and disposition of records. Records should remain legible, readily identifiable and retrievable.

NOTE Further information on record management can be found in ISO/IEC 15489-1.

4.4 Resource management

4.4.1 Provision of resources

4.4.1.1 Resources to implement the SMS

The service provider should make available all resources agreed in the plan to establish, implement, maintain and improve the SMS and the agreed services. The resources include at least the following:

a) human resources, e.g. people to design, implement and operate the SMS, top management and personnel involved in the management of the SMS and services;

b) technical resources, e.g. infrastructure and sufficient capacity to achieve the service requirements, tools to support the processes in the SMS, office accommodation and facilities and service continuity facilities;

c) information, e.g. details of customer requirements, the customer's business needs and business plans, the service provider's business needs, service management policies, measures and other reports;

d) financial resources, including both funds for projects and funds for continuing operation of the SMS.

4.4.1.2 Approval of resources

Procedures should exist to approve the use of agreed resources, such as people, infrastructure, tools and funds. These include:

a) funds to be agreed and budgeted in advance of the implementation of the service management plan;

b) allocation of people required for the project to implement the service management plan and for the longer term continual improvements and day to day operation of the processes;

c) identification and development of skills, approved recruitment and/or by training existing people;

d) identification, agreement and approval of new roles and technologies;

e) the required infrastructure which can include office and data centre facilities, telecommunications such as local LAN and WAN access points, servers, storage, and power and cooling distribution;

f) service management tools which may include tools for monitoring or measuring and service reporting or support of specific processes.

EXAMPLE Resourcing procedures can be supported by specific capacity modelling tools or by information taken from a CMDB. Although tools are not a requirement for ISO/IEC 20000-1 they can make processes more effective and efficient. Tools can assist with providing evidence of conformance to the requirements of ISO/IEC 20000-1.

4.4.2 Human resources

4.4.2.1 General

The service provider's commitment to provision of resources should include defining what each role and individual contributes to the SMS and the service. The service provider should also define and agree the levels of authority and responsibility for each type of role. This includes the competence, education, training, skills and experience required for each role. The service provider should define, agree and communicate this information within the service provider's organization. Where it is deemed relevant, the service provider should also communicate this information to other parties.

The service provider should understand the risks arising from uncertainty as to which roles, and therefore which individuals, have particular levels and types of authority and responsibility. When the level of authority, accountability and responsibility of each role has been defined, this information should become an integrated component of the SMS. The service provider can find a responsibility matrix, e.g. RACI useful to document authority, accountability and responsibility. Once the information becomes a component of the SMS it should then be included in the SMS review cycle.

Resources should include the top management who have overall responsibility and accountability for the SMS and the services delivered by the SMS. This resource requirement will continue indefinitely after the SMS implementation project.

The authorities and responsibilities for each service management process in the SMS should include:

a) a process owner, responsible for:

   1) the design of the process;
   2) ensuring adherence to the process;
   3) the measurement and improvement of the process;

b) a process manager, responsible for the operation of the process and the management of the process management resources;

c) personnel who perform the procedures of the process.

Other roles that are specific to individual service management processes are described in Clauses 5 to 9 of this part of ISO/IEC 20000.

NOTE It is acceptable practice for a single individual to have more than one service management role, particularly for smaller organizations.

4.4.2.2 Competence, skills, training and experience

The competence required for a role should be based on analysis of the specific characteristics and requirements of that role. This should include but not be limited to: education, training, skills and experience.

The competence required for each role relevant to the fulfilment of Clause 4.4.2 of ISO/IEC 20000-1:2011 should be identified. The level and type of responsibility and authority of a role should also be taken into consideration. This includes the roles of top management.

The service provider should also give consideration to the workload involved in each role and how each role will change over time. The allocation of roles and responsibilities to individuals should take these aspects of the role into account when allocating roles and responsibilities.

The service provider should allocate roles to individuals who meet the capability criteria for that role to be performed successfully.

A decision on the suitability of an individual for a role should be based on a comparison of the actual competence and required competence for that role. Where there is a disparity between the agreed competence requirements and the competencies of the individual being considered for, or already in a role, the service provider should ensure that the disparity is corrected.

Disparities may be corrected by several methods, e.g. the individual is provided with education and training to correct the disparity. Alternatively, the service provider may allow for missing skills or experience to be gained through the person working with another who already has the correct skills and experience. After this corrective action has been taken, the service provider should re-assess the competence of the individual or individuals to check that the actions taken have corrected the disparity.

Service providers should align the key performance indicators and/or key result areas of personnel to the achievement of the service management objectives. By doing this, personnel will not only be made aware of their obligations, but better understand how they can contribute to the desired service outcomes.

The service provider should establish and keep current records of competence, including education, training, skills and experience. The service provider should ensure that personnel are aware of how they contribute to the achievement of service management objectives.

There should be a documented procedure to ensure that the personnel records are kept up to date.

4.5 Establish and improve the SMS

4.5.1 Define scope

The service provider should establish whether ISO/IEC 20000-1 is applicable to their circumstances early in the planning stage. Similarly, the service provider should define the scope of the SMS early in the planning stage. The service provider should be aware that neglecting either of these activities can lead to a failed or inefficient SMS that does not fulfil the requirements of ISO/IEC 20000-1.

For the SMS to be effective, the service provider should continually improve the SMS and the services using the PDCA methodology. The scope of the SMS should be understood before improving the SMS.

When defining the scope of the SMS the following parameters should be considered:

a) organizational units providing services, e.g. a single department, group of departments or all departments;

b) services offered, e.g. a single, group of, or all services, financial services, retail services, email services;

c) geographical location from which the service provider delivers the services, e.g. a single office or group of offices, regional, national or global;

d) customers and their locations, e.g. one customer, many customers, external or internal customers;

e) technology used to provide the services.

The scope statement should not include the names of other parties contributing to the delivery of the service.

The service provider should take the guidance of ISO/IEC TR 20000-3 into account when planning how to fulfil the requirements of ISO/IEC 20000-1. This gives advice on defining the scope of the SMS and checking the applicability of ISO/IEC 20000-1 to the service provider's circumstances.

4.5.2 Plan the SMS (Plan)

4.5.2.1 Important planning aspects

The plan for the SMS should cover all aspects of service management and delivery of services and include but not be limited to the aspects given below.

a) The service management objectives. The service provider's prioritized objectives in implementing the necessary changes and improvements should be unambiguous.

b) The service management plan. Where possible the plan should be sub-divided into stages, with benefits identified for each stage.

c) The service provider's service management policy. For example, policies related to all sub-plans such as change management policies, information security policies, service continuity policies. Defining policies early in the planning of the SMS enables verification of the scope of the SMS and makes it possible to identify important considerations.

d) Service requirements. Policies, standards or business key performance indicators should be compatible with service requirements and should meet customer requirements and business needs. For example, service requirements should not result in a nonconformity to an information security policy, putting the entire business at risk.

e) Known limitations which can impact the SMS. For example, the service provider's personnel having insufficient skills in how to implement and manage the SMS. The plan should identify appropriate actions such as providing training and awareness, hiring new personnel with the relevant skills and experience and using the expertise of other parties to mentor personnel.

4.5.2.2 Alignment of planning and agreements

The service management plan should include the agreement and documentation of service requirements. The service targets should be documented in both the plan and agreements between the service provider and relevant groups. The agreements should take into consideration the aspects listed below.

a) Customer, e.g. SLAs, requirements of new or changed services. This should be considered even if the documented agreement with a customer is not a legally binding contract.

b) Internal groups, e.g. operational level agreements with a facilities group, systems development group, human resources group, or finance group. This cannot be a legally binding contract because the service provider and internal groups are part of the same legal entity. However, the internal groups may not be part of the service provider's direct line management. Internal groups can be an important aspect of defining the scope of the SMS as they can contribute a significant portion of the overall service.

c) Suppliers and lead suppliers, e.g. service or resource subcontracts.

d) Other standards, regulatory and statutory requirements, e.g. industry-specific, such as medical, automotive, telecommunications or country-specific compliance to laws for software licensing.

4.5.2.3 Management roles, authorities and responsibilities

The management roles, authorities and responsibilities within the scope of the SMS should be documented in both the service management plan, process documentation and relevant agreements, including:

a) all roles for which management are individually or collectively accountable and responsible;

b) management representative, including any limits on the authority of this role, and the relationship to the top management that this person represents;

c) service or process owners.

The authorities and responsibilities for the roles in the SMS should be checked to ensure that there are no conflicts of interest e.g. the same role proposing and also approving a change. The framework of authorities, responsibilities and process roles in the plan should include the details of which role is accountable and responsible for all components of the SMS.

4.5.2.4 Process interfaces

The information on interfaces between processes should include the type, method and frequency of information passed from one process to another process. The service provider should be aware that this is an important part of their process definition and ensures that the processes and the SMS will function effectively and efficiently.

Clause 5 of ISO/IEC 20000-1:2011 includes requirements for interfaces between the processes in Clauses 6 to 9 and the design and transition of new or changed services.

Requirements for new or changed services include the project stage at which service requirements are defined and when the service is designed and transitioned. The service provider should be aware that effective project management is important for managing some interfaces. The interface between the SMS and any projects should be defined, agreed and recorded in the plan.

The integrated components of the SMS, including processes, policies, objectives and plans, should be measured so that the efficiency and effectiveness of the SMS and the services can be identified, managed and improved.

In order to facilitate integration and interoperability between the customer and service provider the service provider can establish standardized process descriptions. Process descriptions define the purpose, outcomes, activities, policies, roles and responsibilities, information items and interfaces for each service management process within the SMS. Each process can also require documented procedures or work instructions to further define how to undertake activities.

The service provider should be aware that overall management and coordination of the SMS is particularly important when it is being improved or changed for any other reason. Changes to the processes that form part of the SMS should only be made after the impact of the change on the rest of the SMS is understood and is considered acceptable. This includes the impact on other processes or the organization's service delivery capability.

EXAMPLE Changes to parameters or targets used in the incident and service request management process can have an unintended and detrimental effect on other processes, such as the service level management (SLM), reporting and information security management (ISM) processes.

Understanding the interdependencies between processes and between all components of the SMS can reduce risk and enable effective management of the SMS. Examples of interfaces between service management processes and of integration within the SMS can be found in Annex A of this part of ISO/IEC 20000.

4.5.3 Implement and operate the SMS (Do)

The service provider should implement and operate the SMS in alignment with the service management plan and as a means of achieving the service management objectives.

The service provider should be aware of the benefits of ensuring that the authorities and responsibilities of both the service provider and customer are documented and agreed for activities that impact both parties.

The service provider should be aware that a person who is appropriate for the planning and initial implementation is not always suitable for the operation of the SMS. Different skills are required for planning, implementation and operation.

4.5.4 Monitor and review the SMS (Check)

4.5.4.1 General

The service provider should monitor, measure and review the service management objectives and plan the necessary activities to ensure they are being achieved. Top management should be aware of the outcomes of reviews. If changes to the service management plan and objectives are considered necessary, these changes should be approved in accordance with the change management process.

In accordance with the PDCA methodology, the service provider should regularly identify, collect, analyse, and report information on the processes and the services delivered. These activities should support effective management of the SMS and the services, and should enable the ability to objectively demonstrate the quality and value of the services delivered.

NOTE See ISO/IEC 15939 for further information on measurement, ISO/IEC 15504 for process assessment and performance evaluation, ISO/IEC 14598 for product evaluation and ISO/IEC 9126 Parts 2 and 3 for examples of software product metrics.

4.5.4.2 Internal audit

The service provider should ensure internal audits are performed according to a documented procedure that includes authorities and responsibilities for the audits. Those responsible for carrying out internal audits should be suitably knowledgeable and independent of the areas being audited, e.g. they should not audit their own work. The roles required should be documented. They can include a project manager, the sponsor, the steering committee, other interested parties and the independent auditors.

There should be an agreed internal audit programme identifying when each service and which clauses of ISO/IEC 20000-1 are to be audited. There should be a rationale for the planning decisions, including why services or clauses of ISO/IEC 20000-1 are included or excluded for each internal audit. Factors that should be taken into account include the degree of risk involved in a process, its frequency of operation and its past history.

The intervals at which internal audits are performed should be planned and not only done when there are known risks or other issues. The interval selected should take into account the rate of change of the:

a) SMS and services;

b) customer requirements and customer's organization;

c) service provider personnel and organization;

d) technology used for delivery of the service;

e) major changes to service management tools, when tools are used.

Management should ensure that audits are completed to plan, unless rescheduled for documented reasons.

Internal audits of the SMS should include an assessment of the scope of the SMS and that the SMS is still effective for delivery of the services agreed with the customer. This should include checking that the service management policy still provides the correct management direction and that the objectives are met within the timescales expected. The internal audit should review the plans and report against the performance of the SMS.

Using a timeframe consistent with the audit frequency, the internal auditors should provide details on any nonconformities. The service provider should then use the results of the internal audit to identify and prioritize actions.

Any previous audit results should be taken into account. For example, where a concern was identified the plans should include ensuring that the cause of concern be re-audited at the next internal audit. The internal audit should check that any identified and agreed corrective or preventive actions have been implemented to the timescales agreed. The internal audit should also check that the agreed actions have indeed resulted in the predicted improvement.

Nonconformities should be analysed to determine any root causes. The actions arising from audits should include preventive actions in respect to any root causes identified. Actions should have clear and agreed owners and timescales, to help ensure that they are completed effectively and on time. Follow up activities on identified nonconformities should include verification that actions have been taken. Results of actions taken should be reported to top management.

4.5.4.3 Management review

The SMS should be reviewed at planned intervals to check that the SMS continues to enable the fulfilment of changing business needs and service requirements. This should be performed at least annually. However, some service providers operate in a rapidly changing environment and should review the SMS more frequently. The review should include the actual scope against the defined scope of the SMS, suitability of current plans compared to the current needs of the customer and of the customer's business needs.

Specifically, the review can be performed against:

a) performance of the SMS against policies, plans and objectives;

b) measurement of process key performance indicators (KPIs);

c) the results of internal and external audits;

d) a review of continual improvement activities aligned with business objectives;

e) post implementation reviews of changes;

f) industry best practice;

g) customer satisfaction survey results;

h) desired business outcomes.

NOTE See ISO/IEC 15504 Parts 2 and 3 for requirements and guides for process assessment.

4.5.5 Maintain and Improve the SMS (Act)

4.5.5.1 General

A strategic approach to service improvement should be made by establishing a policy on continual improvement of the SMS and the services. The policy should include a definition of the agreed evaluation criteria for accepting and prioritizing improvement opportunities.

All of the services delivered to the customer, the service management processes and the SMS in its entirety should be subject to continual improvement. To facilitate this more readily the service provider may find it useful to build continual improvement activities into the service management process documentation. The service provider may also find it helpful to align the measurement of SMS components and personnel performance targets against continual improvement achievements.

Any nonconformities identified through assessments, audits or other means should be addressed and actions taken to eliminate the causes of both identified and potential nonconformities.

4.5.5.2 Management of improvements

Continual improvement is one of the core concepts of ISO/IEC 20000. A documented procedure identifying the authorities and responsibilities for all improvement activities should be used. This procedure should ensure that opportunities for improvement are effectively identified, evaluated, prioritized, approved, implemented, managed and measured.

Inputs to manage continual improvement should include:

a) relevant directives from top management;

b) root causes identified as a result of audits and reviews, both of the SMS and of individual services;

c) suggestions from the customer, other parties and from within the service provider's organization;

d) problem records;

e) tests of plans, e.g. service continuity tests;

f) delivery of value/service requirements, e.g. prioritizing improvement activities based upon business criticality of services;

g) optimized resource utilization or risk reduction, e.g. opportunities for increased efficiency or improved automation.

NOTE 1 Further guidance can be found in ISO/IEC TR 20000-4.

NOTE 2 A process model and assessment method for system engineering and software development is in ISO/IEC 15504, Parts 5 and 6.

5 Design and transition of new or changed services

5.1 General

5.1.1 Intent of the requirements

The design and transition of new or changed services process should establish and implement plans to control the delivery of new or changed services. The process should be applied to new or changed services that are either high risk or have a potentially major impact on services or the customer.

5.1.2 Concepts

This process should provide a mechanism for managing the design and transition of new or changed services. The process works closely with the change management process. CIs developed or changed in the process should be controlled through the configuration management process via the change management process. The new or changed service should be deployed through the release and deployment management process.

Requirements for new or changed services should be identified by the customer or interested parties of a service, in order to fulfil a business need or effect an improvement to the way the service is delivered to the customer. The service provider should decide when to use this process, based on a change management policy that includes the criteria for determining the usage of the process. Each service provider can have a different policy and use different criteria to determine to what changes Clause 5 would apply. The removal of services, transfer of services and new services or changes with a potential to have a major impact should be managed by the design and transition of new or changed services process. The service provider should understand the risks associated with each new or changed service proposed. Risks should take into account the circumstances of both the service provider and the customer, including the customer's business activities. Actions should be taken to minimize the risks of new or changed services.

5.1.3 Explanation of requirements

The design and transition of new or changed services process is intended for changes that require additional levels of visibility and control to manage higher levels of risk and impact. The three control processes, configuration management, change management and release and deployment management, are at the core of managing all changes to the SMS and the services. However, a complex project with interfaces to the SMS and tasks or deliverables outside the scope of the SMS. can often require the additional layer of control the design and transition of new or changed services process provides.

For each service provider, the criteria used to determine which types of change are appropriate to be managed through the design and transition of new or changed services process is likely to be different. For example, criteria may include a change to a service impacting more than a specific number of users or locations. Another example may include any change that could put the service provider at risk of being penalized under data protection legislation.

The design and transition of new or changed services process should define and manage the relevant interfaces with the control processes in Clause 9. The design and transition of new or changed services process should work with the control processes in Clause 9 to ensure optimal risk management and delivery of a solution that meets all the service requirements. The CIs affected by the new or changed services should be controlled by the configuration management process. The assessment, approval, scheduling and reviewing of new or changed services should be controlled by the change management process. All new or changed services should be deployed into the live environment using the release and deployment management process.

5.2 Plan new or changed services

5.2.1 The need for new or changed services

The need for a new service or a change to a service can originate from the customer, the service provider, internal groups or suppliers. The purpose of the new or changed service can be to satisfy business needs and customer requirements or to improve the effectiveness of the service.

5.2.2 Changes with major impact on service or customer

This process should apply to those changes that have the potential to have a major impact on services and therefore also on the customer. Such changes to services need the additional activities provided by application of Clause 5, to reduce the risk associated with the change.

A change where the impact on services or the customer is sufficiently low can be managed only through the control processes. The majority of changes handled by the service provider should fall into this latter category.

5.2.3 Policy on changes with major impact

The changes that are in scope of Clause 5 should be identified using a change management policy developed as part of the change management process. The policy should include criteria for the identification of higher risk changes that have the potential to have a major impact on the services or the customer. The policy should be based on the service provider's specific needs and an assessment of the risks to their services. The policy

should take into consideration that the proposal for a new or changed service may originate from a variety of sources and for a variety of reasons.

The policy should be documented and agreed by top management and the process owners most directly involved in the new or changed services process.

The criteria in the change management policy should always include both the removal of an existing service or the transfer of a service to be delivered by another party. For each service provider, the other criteria are likely to be different.

Changes with a potentially major impact can include:

a) a change to a service impacting more than a specific number of users or locations;

b) a change that could put the service provider at risk of being penalized under data protection legislation;

c) a new service or a new customer for an existing service;

d) a major difference to how the service is to be provided or delivered, e.g. location, hardware platform;

e) rollout of a new operating system or software application or a major release of existing software.

The service provider should also take into consideration changes that can be required to the SMS, including changes to the scope of the SMS as a result of new or changed services. For example, identification of risks to the service targets agreed with the customer, changes to supplier management procedures or documented agreements with other parties that have an impact on existing or planned services.

5.2.4 Managing change as a project

Any new or changed services to which Clause 5 applies should be managed as a project due to the size, risks and scope of the changes. The service provider should consider the potential financial, organizational and technical impact of the new or changed service, plus the potential impact on the SMS.

The service provider should ensure a strong coordination between the change management process and the project management roles and authorities, from the earliest possible stage of the project.

The service provider should ensure the project takes into consideration:

a) the impact on existing support arrangements, e.g. the service provider's operational procedures;

b) the impact on the existing service levels and the ability of the service provider to manage the impact;

c) supplier support agreements, contracts and documented agreements with other parties which can be affected by the changes or additions to the service;

d) customer requirements of the existing service, including outputs such as reporting which can be affected by the additions or changes to the service;

e) deployment tools and methods.

5.2.5 Contributions from other parties

Another party can provide service components for the new or changed services. The new or changed service can involve the acquisition of software, infrastructure, specialised skills or other service components.

When another party is involved in the new or changed services, the service provider should do a thorough review. The review should evaluate the capability of the other party to fulfil their commitments, including the agreed service requirements. The review should also evaluate the risk to the existing services and support environment.

In order to accept the service into the live environment, it can be necessary to specify requirements, such as number of support personnel, technology, testing or documentation.

5.2.6 Risk Assessment

The service provider should be aware of the importance of assessing risks, issues and mitigation efforts early in the process and then at each stage from planning through to acceptance into the live environment.

The results of risk assessments should be used to develop acceptance criteria during the planning stage.

5.2.7 Service acceptance criteria

The service acceptance criteria contained within the plan should include:

a) the service provider's requirements to be met in order for the service provider to accept the new or changed services from the project;

b) a checklist for handover of the new or changed service, e.g. knowledge transfer, documentation, capacity, availability, continuity and security required for support of the new or changed service;

c) the requirements of the customer, such as communication schedules, awareness training and documentation.

Where risks to the service, SMS or the customer’s business activities are unacceptable and cannot be mitigated, the new or changed service should be rejected.

5.2.8 Service removal

If a service is to be removed, this should be planned and documented in a service removal plan. The plan should include:

a) the conditions where removal applies;

b) the objectives and success factors of the removal;

c) governance of processes operated by other parties;

d) roles and responsibilities for all interested parties, e.g. customers, suppliers, internal groups;

e) constraints, risks and issues;

f) milestones and deliverables;

g) activity breakdown and description of each activity;

h) agreed completion criteria for the removal and of the end of service provider’s responsibility;

i) the date when the service is no longer available to the users and the date when the service is removed;

j) how interfaces between the service to be removed and other services will be handled by the other services;

k) a review of information security arrangements including removal of sensitive information.

The service provider should ensure that the details of any outstanding incidents, problems, user requests and requests for change have been agreed with the customer. This agreement with the customer should include any resulting actions.

Ownership of all data, documentation and system components should be agreed. If required, arrangements for access to the data or other service components should be agreed, planned and implemented. Arrangements for archiving, disposal or transfer should also be agreed.

Any changes to documents required as a result of service removal should also be identified and those changes made through the change management process.

The service management objectives, activities and outcome of removal of a service should be documented in a written agreement with the customer. This agreement should include end of service date and changes to roles and responsibilities. The agreement should also include how the service provider will manage end user data, customer specific information, service documentation and the affected infrastructure, applications and licences. The written agreement can be called the agreed service removal acceptance criteria.

Where all or part of the service is to be transferred to another party, the aim should be that service to the user continues with no unnecessary interruption. The service provider should work with the customer and the other party, to identify any risks to service continuity or quality, in advance of the transfer. The service provider should issue a detailed task list of the steps required, followed by a documented evaluation of the result.

5.3 Design and development of new or changed services

5.3.1 Activities performed by the service provider, customer and other parties

The service provider should be involved from early in a project to deliver new or changed services. Early involvement can avoid design decisions that result in a service where the required functions and features are unsuitable when actually in operation. Early involvement by the service provider should ensure that the requirements agreed with the customer include criteria for the quality for the new or changed service, including at least:

a) service levels, response and other aspects of performance;

b) service reliability and resilience;

c) security controls;

d) suitability for required service continuity;

e) cost-benefit criteria to change or for a new version to be released and deployed;

f) ease of use.

5.3.2 Risk management

During the design stage the service provider should consider the results of the initial risk assessment completed during the planning stage. The design should be influenced by the risks identified in that assessment. During the design stage the service provider should consider which of the identified risks will be acceptable when a new or changed service moves into the live environment. This should take into account the potential impact of a particular risk, including on the:

a) service being designed;

b) potential impact of the risk on the service provider's other services;

c) the customers reliant on new and existing services.

When a potential nonconformity to the agreed quality and functional requirements of the service is identified, the service provider should mitigate the risk. For example, by changing the design or ensuring the risks are understood and accepted by the interested parties.

Acceptance of the service into the live environment should be based on an understanding of the potential impact of a service that does not meet the acceptance criteria. This should include an understanding of the impact on other services. The risk assessment and risk management guidance provided in Clauses 5.2.6 and 5.3.2 should influence the development of acceptance criteria. The following should be considered:

EXAMPLE 1 Fix now: a delay in the transition into operational running to allow correction of the deficiencies.

EXAMPLE 2 Fix later: acceptance with caveats so that correction of deficiencies is made after an agreed interval.

EXAMPLE 3 Do not fix: acceptance with other services changed to accommodate the deficiencies of the new or changed service.

EXAMPLE 4 Cannot fix: acceptance but an agreement that deficiencies cannot or need not be corrected.

NOTE See ISO/IEC 31000 for further information on risk management.

5.3.3 Service Design Activities

5.3.3.1 Design planning

The design of the new or changed service should also be planned, taking into consideration the following:

a) focus on fulfilling the agreed business needs and customer requirements, which should be documented as part of the requirements within the project scope;

b) it should be linked to the change management process to ensure that the plans are communicated and approved by the interested parties and that any impact on CIs is understood and accepted;

c) to ensure that CIs for the new or changed services are planned and controlled;

d) to ensure the timescales for the project are taken into consideration in the schedule of change;

e) take into consideration the cost of delivering and ongoing management of the service, e.g. the service design should result in effective support without excessive resource or technical overhead;

f) take into consideration the organizational, technical and commercial impact of delivering the new or changed services;

g) ensure that the service design makes the best use of the existing organization and technology and causes the minimum disruption to existing commercial arrangements;

h) be carried out in such a way that the design enables agreed levels of service for the new or changed services to be met in a way which is manageable for the service provider's organization;

i) assess the suitability of the new or changed service to the existing processes in place within the service provider's organization for managing, measuring and reporting service levels.

The service provider's plan for the new or changed services should include the dependencies, time and resource constraints which can affect any of the required activities. Where the service provider is dependent upon activities to be performed by external parties, the plan should note these dependencies. Activities that may be performed as dependencies include testing and validation. The plans should also provide for contingencies in the event that the timescales are not met.

The service provider should ensure that the human, technical, information and financial resources and service management capabilities required to conduct all activities are identified and can be provided. Where these resources and capabilities do not exist within the service provider's organization, it should be understood what steps need to be taken in order to provide them, including the lead-times for their delivery. The scope of planning should include the initial design, development and transition activities through to delivery of the new or changed service.

5.3.3.2 Design and develop services

The design of the service should be documented and agreed prior to development. The design should take into account current service requirements, information security considerations, service resilience and resource capacity projections for growth during the anticipated life of the service.

Design and development of new or changed services should adopt project management methods and techniques. There should be traceability between the requirements, the design, and the testing of new or changed services.

The service design should be agreed with all affected or interested parties prior to development. Such parties should include those responsible for providing existing services that can be impacted, and those responsible for providing any of the resources required.

During the course of the project, if any changes are agreed then the design should be updated and approved. Prior to live operation, the service should be tested against each requirement of the specification, and the outcomes recorded.

Design and development should include the following items, as appropriate:

a) the activities of design and implementation, transition, operation and maintenance for acceptance of services, including the identification of, or reference to:

   1) development activities to be carried out;
   2) required inputs to each activity;
   3) required outputs from each activity;
   4) management and supporting activities to be carried out;
   5) required team training;
   6) planning for the control of product and service provision;

b) the organization of the project resources, including the team structure, responsibilities, use of suppliers, and resources to be used;

c) organizational and technical interfaces between different individuals or groups, such as sub-project teams, suppliers, partners, users, customer representatives, and quality assurance representatives;

d) the analysis of the possible risks, assumptions, dependencies, and challenges associated with the design and development;

e) the schedule identifying:

   1) the stages of the change, the activities to be performed;
   2) the associated resources and timing;
   3) the associated dependencies;
   4) the milestones;
   5) verification and validation activities;

f) the identification of standards, rules, practices and conventions, methodology, life cycle model, statutory and regulatory requirements, contractual obligations, and other constraints;

g) tools and techniques for service development;

h) facilities such as hardware and software required for service development;

i) configuration management practices;

j) method of controlling non-conforming software and hardware products;

k) methods of control for software and hardware used to support service development;

l) procedures for archiving, back-up, recovery, and controlling access to software products; and methods of control for virus protection.

If the service provider cannot control the design or development of a service or service component the service provider should conduct an assessment to ensure that it meets expectations. For example, the functional and non-functional features of a commercial off-the-shelf product should be assessed against requirements and expectations. Any required set up or customization of the product should be planned and designed.

A document used for design and development planning may be a single document, a part of another document, or composed of several documents.

Planning should be reviewed periodically and any plans amended if appropriate.

5.4 Transition of new or changed services

The transition of new or changed services should be coordinated with the change management process, the release and deployment management process and the configuration management process. Adopting this approach should ensure that the control of changes applies to the transition of the new or changed service.

The transition of services should include the build, test and acceptance of the new or changed services followed by making the new or changed services operational through the release and deployment management process.

The transition should be reviewed with the customer and interested parties to establish that it is ready for live operation. The resulting decision should be recorded, together with the customer's acceptance of the new or changed service into live operation. The transition should continue until it is agreed that any remaining activities are part of normal live operation. Following the completion of the transition, the service provider should report to interested parties on the outcomes achieved by the new or changed services against the planned outcomes.

Service acceptance criteria should be reviewed by the service provider and other interested parties. Where there are outstanding acceptance criteria which have not been met prior to the transition of a service, it should be decided whether the absence of these criteria presents a significant risk to the service. Where the risk is significant, the transition should be delayed. However, where there is mitigation of the risk or the risk is not significant, it may be decided to proceed with the transition. In this instance, the outstanding actions and their owners should be recorded on the service acceptance criteria statement and the steps should be taken to ensure that these actions are fulfilled.

The service provider should record the acceptance by the customer and interested parties of the new or changed services against agreed acceptance criteria.

5.5 Documents and records

The documents and records, that should be produced and retained by the design and transition of new or changed services process should include:

a) service requirements for the new or changed service;

b) risk assessment for each request for a new or changed service;

c) plan for the design, development and transition of the new or changed service;

d) a plan for any services to be removed;

e) an evaluation report of other parties contributing to the new or changed service;

f) design specification for the new or changed service;

g) service acceptance criteria;

h) transition report, describing the outcome achieved against the outcome expected.

It is critical that the process has access to the policy on new or changes services in the scope of Clause 5 developed and maintained as part of the change management process.

5.6 Authorities and responsibilities

In addition to the process owner, process manager and personnel performing the procedures of the process as described in Clause 4.4.2.1, authorities and responsibilities required within the design and transition of new or changed services process should include:

a) a new or changed services manager, usually a project manager, responsible for delivery and management of project deliverables and ensuring fulfilment of service acceptance criteria;

b) a group who can evaluate the impact of the proposed new or changed service on the SMS from multiple perspectives, including policies, objectives and processes.

c) a group, which may be the same as above, who can be involved in planning of all new or changed service requirements and acceptance of delivery of a new or changed service;

d) customer and business representatives, responsible for the documentation and agreement of all new or changed services requirements and acceptance of delivery of new or changed service.

6 Service delivery processes

6.1 Service level management

6.1.1 Intent of the requirements

The SLM process should ensure that an agreed service is provided and that service targets are met. Specific and measurable targets should be developed for all services. The SLM process ensures that agreed services and service targets are documented in a way that is easily understood by the customer.

6.1.2 Concepts

The SLM process should define, agree, document, monitor, report and review the services delivered. In order to ensure that delivery of the services is achievable, managed and in alignment with customer requirements and business needs, the SLM process works closely with the business relationship management (BRM) process and the supplier management process.

The SLM process should enable the integration between the supplier management process, delivering services to the service provider and the BRM process.

The SLM process works closely with both the supplier management and the BRM processes to ensure that delivered services and service targets are aligned with business needs and customer requirements.

The supplier management process should ensure that the service targets agreed with suppliers are aligned with the SLM process, as well as other required management information to ensure that service reviews can be performed.

The SLM process should also provide the supplier management process with details of changes that affect any agreements with suppliers. For example, new service requirements that mean a contract with a supplier has to be changed. Other examples include changes to processes and procedures that affect the interface between the service provider who is responsible for the governance of processes and suppliers who are operating processes on behalf of the service provider.

The SLM process should provide the BRM process with agreed service targets to meet customer requirements, as well as other required management information to ensure that customer service reviews can be performed.

The SLM process should negotiate, agree and document requirements for new or changed services through service level requirements documents, and should then manage and review them through the service lifecycle, creating signed SLAs for operational services.

NOTE Examples of interfaces between the SLM process and other processes in the SMS are described in Annex A of this part of ISO/IEC 20000.

6.1.3 Explanation of requirements

6.1.3.1 Documentation of service commitments

SLAs may need to be supported by agreements with suppliers external to the service provider's organization, or with internal groups. These supporting agreements with suppliers can be known as underpinning contracts.

Supporting agreements with internal groups can be known as operational level agreements. These cannot be legally binding on either party but can be treated as if they are. The combined constraints of all agreements supporting an SLA should be considered before the SLA is finalized.

The service provider should monitor and measure service performance achievements of all operational services against targets in SLAs, operational level agreements or other performance agreements and produce service reports. Service reviews should be conducted and service improvement plans created at regular intervals, at least annually.

6.1.3.2 Catalogue of services

The service provider should define all services in a catalogue, using terms that are aligned to the customer’s view of services and understandable by those without a detailed technical understanding. The catalogue of services should collate and present all service definitions. The scope of each service defined should be relevant to the customer’s business activities. The catalogue should hold information common to all or most services, in order to simplify the SLAs, as described in Clause 6.1.3.4 of this part of ISO/IEC 20000. The catalogue of services should include a variety of information, including:

a) the name and description of the service;

b) service targets, e.g. time to fulfil a service request, time to set up a service for a new user, time to reinstate a service after a major failure;

c) contact points;

d) service hours, support hours and exceptions;

e) security arrangements;

f) current services;

g) dependencies between the services and service components, e.g. a service supporting a user’s laptop includes support of applications, support for internet access and support of the hardware, each of which can be provided by different suppliers or internal groups.

NOTE The listed examples are not exhaustive.

The service provider should ensure that the catalogue of services is designed so that the information is easy to maintain. The logical and efficient grouping of information is particularly important for information that is subject to relatively rapid change. This minimizes the overhead of the change management process, as described in Clause 6.1.3.4 of this part of ISO/IEC 20000.

The catalogue of services should also show any dependencies between services and supporting services. For example when a business service is dependent on a number of underpinning services such as email, security or network services. Other examples include a service that is dependent on service components being provided by suppliers or internal groups outside the direct control of the service provider.

The catalogue of services is a key document for setting customer expectations and should be widely available to both the customer and the support personnel.

6.1.3.3 Service level agreements

The customer and the service provider should agree about the terms and targets for a service to be delivered, and document these in an SLA. An SLA is a document that describes the service and service targets. An SLA also specifies the responsibilities of the service provider and the customer. A single SLA may cover multiple services or multiple customers. SLAs should cover all components required to deliver the service.

The customer requirements, the business needs and the service provider's capabilities should be the defining force for the content, structure and targets of the SLA. The targets, against which the delivered service should be measured, should be defined from a customer perspective.

The service provider should be aware that too many targets in an SLA can create confusion and lead to excessive overheads without delivering benefits. The SLAs should include only an appropriate subset of the targets to focus attention on the most important aspects of the service for the business and the customer.

The minimum content that should be in an SLA or that may be directly referenced from an SLA in a catalogue of services is:

a) brief service description;

b) validity period and/or SLA change control mechanism;

c) change approval details;

d) brief description of communications, including reporting, review frequency and schedule;

e) service hours, e.g. 09:00 h to 17:00 h, date exceptions, e.g. weekends, public holidays, critical business periods and out-of-hours coverage;

f) scheduled and agreed interruptions to services, including notice to be given and number per period;

g) customer responsibilities, e.g. correct use of systems, adherence to the information security policy;

h) service provider liability and obligations, e.g. security;

i) impact and priority guidelines;

j) escalation and notification process;

k) complaints procedure;

l) service targets;

m) upper and lower workload limits, e.g. the ability of the service to support the agreed number of users/volume of work, system throughput;

n) high level financial management details, e.g. charge codes;

o) actions to be taken in the event of a service interruption, including both incidents and disasters, are normally referenced from the SLA;

p) glossary of terms;

q) supporting and related services;

r) any exceptions to the terms given in the SLA.

Information that changes frequently or information common to many SLAs may be provided via a reference in the SLA to documents such as telephone or email directories and organizational structure diagrams. This simplifies change management of the SLAs without impacting the quality of the SLM process. A glossary of terms, normally held in one place, should be common to all documents, including the catalogue of services. This is only viable if the referenced documents are also under the control of the change management process. Both the SLA and each service that the SLA describes should be subject to the change management process.

6.1.3.4 Managing the catalogue of services and service delivery

The service provider should have a procedure for making the catalogue of services readily available to those who need it to perform their roles effectively. The procedure should also ensure that the catalogue is kept current and is easy to keep up-to-date, without requiring specialist skills or knowledge outside the scope of personnel using the catalogue. Regular checks should be made on the accuracy of the information held in the catalogue.

Major business changes, e.g. due to growth, business reorganizations and mergers or changing customer requirements, can require service levels to be adjusted, redefined or even temporarily suspended.

Changes to the catalogue of services or to SLAs should be initiated and managed through the change management process, to ensure changes are not implemented without the overall impact being managed.

The SLM process should be sufficiently flexible to accommodate these changes. The SLM process should ensure that the service provider remains focused on the customer throughout the planning, implementation, and ongoing management of service delivery. The service provider should work with the BRM process and customer to gain an understanding of the customer's business drivers and requirements.

The SLM process should manage and coordinate contributors to the service levels, to identify:

a) agreement of the service requirements and expected service workload characteristics;

b) agreement on service targets;

c) measurement and reporting of the service levels achieved, workloads and an explanation if the agreed targets are not met, see Clause 6.2, of this part of ISO/IEC 20000;

d) review of service performance with the customer to confirm reported performance and customer satisfaction;

e) initiation of corrective or preventive action;

f) input to a plan for improving the service;

g) review appropriateness and alignment of service levels and service catalogue with business requirements in line with agreed planning activities, minimum annually.

The process should encourage both the service provider and the customer to develop a proactive attitude toward service improvement and should ensure that they have joint responsibility for the service.

Customer satisfaction is an important part of the SLM process but it should be recognized as being a subjective measurement, whereas service targets within an SLA should be objective measurements. The SLM process should work closely with the business relationship and supplier management processes to manage both customer satisfaction and to achieve service targets.

The catalogue of services and SLAs should be reviewed with the customer according to agreed planning activities.

6.1.3.5 Managing other parties

The service provider should recognise that a customer can act as both a supplier and a customer. For example, a specialist group in the customer's organization can provide a component of the service, but also receives a service in the scope on the service provider's SMS. If this is the case the service provider should use the SLM process to manage the customer acting as a supplier.

Similarly, an internal group that is not included in the SMS should be managed by the service provider using the SLM process.

NOTE Management of suppliers, by definition external to the service provider's organization, is under the supplier management process in Clause 7.2.

6.1.4 Documents and records

Documents to be produced and used by the customer, service provider and interested parties should include:

a) catalogue of services;

b) all SLAs and other relevant agreements;

c) processes and procedures for the SLM process, including the management of the catalogue of services and SLAs;

d) inputs to and output from reviews of the SLM process, the catalogue of services and the SLAs;

e) service reporting requirements;

f) service review planning activities;

g) monitoring and control report;

h) service review records and identified opportunities for improvement;

i) service improvement plans.

6.1.5 Authorities and responsibilities

In addition to the process owner, process manager and personnel performing the procedures of the process as described in Clause 4.4.2.1, authorities and responsibilities required within the SLM process should include the following.

a) The operation of the process and management of resources and communications should be the responsibility of a service level manager. This manager is also responsible for the service provider personnel that operate the procedures.

b) A customer representative and the service level manager are together responsible for the authorization of the catalogue of services and each SLA is the responsibility of the customer and service level manager. These two roles should have sufficient authority to agree the definitions of a service in the catalogue and the service targets.

6.2 Service reporting

6.2.1 Intent of the requirements

The service reporting process should ensure the production of agreed, timely, reliable, accurate reports to facilitate informed decision making and effective communication.

6.2.2 Concepts

The success of all service management processes is dependent on the use of the information provided in service reports. Monitoring and reporting should encompass all measurable aspects of the service, providing both current and historical analysis.

Service reports should be appropriate to the audience's needs and of sufficient accuracy to be used as a decision support tool. The language and presentation should aid the understanding of the reports so that they are easy to assimilate, e.g. the use of charts.

6.2.3 Explanation of requirements

The requirements for service reporting should be agreed and recorded for the customer and internal management. Several types of reports should be produced. These include reactive and proactive reports. Reactive reports show what has happened, after it has happened. Proactive reports give warning of significant events, thereby enabling preventive action to be taken beforehand, e.g. a report identifying the need for greater redundancy for a business critical service, to prevent customer impacting incidents from occurring. Other report types include schedules and forecasting reports. These show planned activities.

The service provider should produce reports for the customer and management including at least:

a) performance against service targets, e.g. exceptions or near-exceptions against targets, outage reports and achievements;

b) workload characteristics including volume information and periodic changes in workload, e.g. incidents, problems, changes and activities, classification, location, customer, seasonal trends, mix of priorities, number of requests for help, age profile of outstanding workload;

c) non-conformities with ISO/IEC 20000-1 identified during internal audits;

d) performance reporting of corrective and preventive actions, lessons learned following major events, e.g. major incidents, design, transition and release of new or changed services, and service continuity interruptions or tests and improvement activities;

e) projections of current trends to aid prediction of future performance;

f) tracking the resolution to the customer's satisfaction of corrective and preventive actions to address complaints, any negative feedback from customer satisfaction measurements, and their root causes;

g) forecasts and plans, e.g. financial projections, workload plans, schedule of planned changes.

Where there are multiple suppliers, lead suppliers and sub-contracted suppliers, the reports should reflect the relationships between suppliers, e.g. a lead supplier should report on the whole of the service they provide, including any services by sub-contracted suppliers that they manage as part of the customer's service.

Decisions relating to the service, including those made by top management, and the resulting actions of each, should be based on the findings contained in the service reports. The SMS should include a procedure that routinely verifies that such decisions have been validated by service report information, e.g. prior availability or performance reports used as a basis to invest in increased capacity. Not all decisions related to the service can be based on service reports. Examples of exceptions include legal and regulatory changes, external market studies, changing business structure, or technological advancement.

The service provider should ensure that reports and outcomes from each process are communicated to all interested parties, including top management, process owners, the customer, suppliers and lead suppliers, wherever relevant.

6.2.4 Authorities and responsibilities

In addition to the process owner, process manager and personnel performing the procedures described in Clause 4.4.2.1, authorities and responsibilities required within the service reporting process should include:

a) personnel responsible for the timely and accurate production and distribution of service reports to the relevant recipients;

b) personnel responsible for the definition of contents of each report, including its format, contents, style and frequency;

c) process owners of other service management processes, service owners, technical groups and other interested parties, who should analyze reports and identify, prioritize and action improvements.

6.3 Service continuity and availability management

6.3.1 Intent of the requirements

The service continuity and availability management process should ensure that agreed service continuity and availability commitments can be met, within agreed targets.

6.3.2 Concepts

The service continuity and availability management process includes both a focus on prevention of and recovery from service failures or disasters as well as ensuring the provision of sufficient service availability to meet service requirements.

Service providers may operate the service continuity and availability management process as two separate processes that are linked. Alternatively, the service provider may operate them as a single process. The decision should be based on the service provider's circumstances and should be documented as part of the SMS.

The service continuity and availability management process should allow for both reactive and proactive aspects of the process and prioritising of the business criticality of the agreed services. The service continuity and availability process should also capture data to allow services to be monitored, managed, reviewed and improved by the service provider and reported to the customer where relevant.

The service provider should develop effective plans to ensure that agreed requirements can be met. These requirements include requirements for availability and continuity under both normal circumstances and following a major loss of service. The plans should include solutions for increases or decreases in service levels, expected peaks in activity and an understanding of new or changed requirements to address future business need for service continuity and availability.

6.3.3 Explanation of requirements

6.3.3.1 Risk assessment and management

A key feature of the service continuity and availability management process should be risk assessment and risk management. The risk assessment should include business impact analysis of a major loss of service.

Service continuity and availability requirements should be identified and agreed based on the agreed service requirements, the results obtained from business impact analysis exercises, the customer's business priorities, policies and plans, SLAs and assessed risks. The service provider should maintain sufficient service capability, together with effective plans designed to ensure that agreed service levels are maintained in the event of a major loss of service.

Ensuring that service levels are maintained following a major loss of service should take into consideration those elements of the live operation of the service that are under the control of other parties such as the customer or suppliers.

Service continuity and availability requirements for normal service and after a major loss of service should include at least the following:

a) access rights, e.g. who can have access rights under normal conditions and who can have the highest priority for access to a limited service, following a major loss of service;

b) response times, e.g. response times under normal circumstances and also after a major loss of service. It should be defined and agreed with the customer as to what is the acceptable response time for different services and what actions should be taken to ensure that agreed response times are achieved;

c) end-to-end availability of services, e.g. for normal service what is the required availability of components required to deliver a complete service. After a major loss of service what priority should be given to returning each specific service to normal performance.

6.3.3.2 Service continuity policy

The service provider can find it useful to develop and maintain a policy that defines the general approach to meeting service continuity obligations. The scope of the service continuity policy should be consistent with the scope of the SMS.

The policy should define a consistent method for determining the required vs. actual resilience for each service and to effectively prioritize opportunities for improvement in alignment with the business criticality of services.

The service continuity policy should drive the service provider's continuity planning activities within the scope of the service continuity plan.

The policy should address the roles, activities and responsibilities required to meet the agreed service requirements.

The policy should define the interfaces between the service continuity and availability management process and other service management processes. Annex A of this part of ISO/IEC 20000 includes information about interfaces between the service continuity and availability management process and other components of the SMS.

The policy should take into account agreed service hours and critical business periods. The service provider should identify the requirements separately for each customer group and service, including:

a) the maximum acceptable continuous period of lost service;

b) the maximum acceptable periods of degraded service;

c) the acceptable degraded service levels during a period of service recovery.

The agreed service hours and critical business periods should be defined in relation to specific business cycles and their associated criticality, e.g. month end, end of year, holiday periods.

If the service provider relies on a service continuity policy to direct the process, the service continuity policy should be reviewed at agreed intervals, at least annually. Any changes to the policy should be formally agreed between the service provider and customer.

6.3.3.3 Service continuity and availability plans

If a service continuity policy is in place, the service provider can align the policy with a service continuity strategy. It should be appropriate to the criticality of the services based upon the business impact analysis of the services. The service provider should also gather relevant information from other service management processes as input into the service continuity strategy.

Once the strategy is defined, a risk analysis should be conducted to identify continuity risks that conflict with the strategy and define controls to manage them or instigate mitigating actions where the level of risk is unacceptable.

The service provider should maintain sufficient service capability, together with workable plans designed to ensure agreed requirements can be met.

The service provider should develop service continuity and availability plans, recovery plans and procedures, and the service continuity testing policies. The service continuity plans and testing policies should be designed to reduce the impact of major disruptions on key business functions and processes.

The service continuity plan should be based on the requirements defined in the service continuity policy, a business impact analysis and risk assessments

Ongoing operation should define requirements for service continuity education, awareness and training, review and audit, service continuity testing and coordination with the change management process. Service continuity plans should be regularly tested and responsibilities for invoking should be clearly assigned. Service continuity testing should be undertaken at least annually or after every major business change. Regular training sessions should be provided to all relevant parties. A defined and managed distribution policy for the storage of service continuity and recovery plans should exist and all critical backup media, documentation and other resources necessary for recovery should be stored offsite.

The service provider should ensure that:

a) service continuity plans take into account dependencies between services and service components;

b) service continuity plans and other documents required to support service continuity are recorded and maintained;

c) responsibility for invoking service continuity plans is clearly assigned, and plans clearly allocate responsibility for taking action against each recovery requirement of the policy;

d) backups of data, documents and software, and any equipment and personnel necessary for service restoration are quickly available following a major service failure or disaster;

e) service continuity documents, for example, service continuity plans and schedules, contact lists and the CMDB, remain accessible during a disruption;

f) personnel understand their role in invoking and/or executing the plans;

g) standby arrangements exist with suppliers and recovery site providers, where appropriate.

Service continuity plans and related documents, e.g. contracts, should be assessed for impact prior to system or service changes being approved, and prior to significant new or amended customer requirements being agreed. Service continuity plans and related documents should also be reviewed and tested at least annually.

An availability plan should be developed and published. The availability plan should identify the business needs and customer requirements, design requirements, technical specifications and project planning activities required to meet the business availability requirements both currently and in the future. Predictions regarding future availability documented in the availability plan should include proposed preventive actions to mitigate the likelihood of unplanned non-availability. The availability plan should be reviewed and revised regularly, at least annually and after any major change.

Planning and design of the availability of new or changed services should be based on the criticality of the services to the business, and should balance cost against acceptable business risk.

All service and service component non-availability should be recorded, investigated and appropriate actions should be taken to reduce the impact and/or likelihood of any future occurrence.

6.3.4 Service continuity and availability monitoring and testing

6.3.4.1 Service continuity testing

Service continuity testing should be undertaken after every major business change and change to the service environment. The frequency should be based on the service provider's circumstances. The frequency should be sufficient to gain assurance that service continuity plans are effective, and remain so through the evolution of changing systems, processes, personnel and business needs. The scope of service continuity testing should include the return to normal service operation following a disruption.

Service continuity testing should involve the joint participation of the customer and the service provider, based upon an agreed set of objectives. Where applicable, it should also include other parties. Test failures should be documented and reviewed as input into a plan for improving the service.

Review after a service continuity test should be conducted to assess the achievement of the aims and objectives of the test and to identify any areas of weakness or opportunities for improvement.

6.3.4.2 Availability monitoring and testing

Service continuity and availability management should, according to the agreed availability plan:

a) monitor and record availability of the service;

b) maintain accurate historical data regarding availability of services;

c) make comparisons with requirements defined in SLAs to identify any nonconformity to the agreed availability targets;

d) document and review nonconformities;

e) predict future availability requirements.

A regular availability testing schedule should confirm that the availability solutions are achievable and appropriately resilient. Availability, reliability and resilience mechanisms should be reviewed and tested after any major change.

Where possible, potential issues should be predicted and preventive action taken. Service continuity and availability management should strive to achieve and improve defined levels of reliability for all the components of the service, with corrective and preventive actions identified, recorded and acted upon.

6.3.4.3 Management of risk to availability

Risk assessments should identify the vital business functions and availability requirements, and risks agreed with the business.

Risk management should produce solutions to enable the delivery of required levels of availability, and by implementing cost justifiable countermeasures to mitigate identified risks wherever possible. It is not advisable to exceed the requirements through major financial investments that cost far more than the benefits of improved availability.

Planning and design of the availability of new or changed services should be based on business criticality of the service, the importance to the business of different working periods and required service hours.

Regular monitoring, measurement, analysis reporting and reviews of service and component availability should be an essential aspect of the process. All relevant data pertaining to the availability and non-availability of services should be maintained. The reporting of achieved availability targets should use actual historical data and the focus of measurement and reporting should align with the agreed targets.

Assessment of requests for change for all new or changed services should take into consideration the potential impacts of risks to agreed availability targets. Availability, reliability and resilience mechanisms should be regularly reviewed and tested after any major change.

Availability design criteria should define base products, technology and components that deliver the required reliability.

6.3.4.4 Review after invocation of a service continuity plan

Review after invocation of a service continuity plan should be undertaken to:

a) identify the nature and cause of the service disruption that initiated the activation of the plan;

b) assess the adequacy of management's response;

c) assess the organization's effectiveness in meeting its recovery time objectives;

d) assess the adequacy of the service continuity plan and tests in preparing personnel for the activation of the plan;

e) identify improvements to be made to the service continuity plan and testing.

6.3.5 Documents and records

The documents and records that should be produced and retained by the service continuity and availability management process should include but not be limited to:

a) service continuity and availability management policies;

b) business impact analysis;

c) risk assessment reports;

d) service continuity and availability plans;

e) service continuity and availability customer requirements;

f) service component availability constraints and data;

g) service continuity and availability designs;

h) service continuity and availability test plans;

i) service continuity and availability test reports;

j) service continuity and availability management processes and procedures;

k) awareness training requirements and records;

l) availability management database;

m) availability monitoring reports;

n) maintenance and projected service outage schedules.

Personnel should understand their role in invoking and/or executing the plans and be able to rapidly access service continuity documents.

Service continuity plans and related documents, e.g. contracts, should be assessed for potential impact as part of the change management process, SLM process and the supplier management process. For example, before accepting new or changed services or agreeing service requirements.

6.3.6 Authorities and responsibilities

In addition to the process owner, process manager and personnel performing the procedures of the process as described in Clause 4.4.2.1, authorities and responsibilities required within the service continuity and availability management process should include:

a) availability administrator, responsible for ensuring that the infrastructure monitoring and collection of data relating to component and service availability is occurring correctly and as required;

b) a technical recovery team, responsible for disaster recovery planning, testing and restoration of services;

c) the customer, service provider personnel and interested parties who require access to service continuity and availability management information, participate in testing and agree service continuity requirements;

d) availability analyst, responsible for reviewing and analysing availability reports and data to identify actual and potential availability issues so that appropriate, solutions for improved availability can be identified;

e) service continuity personnel, responsible for maintaining monitoring capability and triggers.

6.4 Budgeting and accounting for services

6.4.1 Intent of the requirements

The budgeting and accounting process should support the service provider's understanding of and ability to manage the total cost of services. In order to achieve this objective, the process should ensure that:

a) the cost of individual services, overall service provision and the service provider’s budget are understood;

b) reliable forecasting of both costs and budget is achievable;

c) a budget is developed and used by service management processes;

d) unexpected variances of costs or budget are identified and managed;

e) the budget is adhered to so that service delivery is funded adequately throughout the budget period;

f) forecasts, budgets and costs are reviewed regularly to ensure the process and procedures remain effective.

6.4.2 Concepts

The budgeting and accounting process should control the financial aspects of services and service components. The budgeting and accounting for services process should provide information that supports both the live operation of services and the funding of service changes and improvements. Budgeting and accounting for service process should ensure that the costs of the service provision are tracked and the services themselves are affordable and in accordance with the budgets.

Responsibility for many of the financial decisions may lie outside the scope of the SMS. The requirements regarding the level of detail of financial information to be provided, in what form and at what frequencies may be dictated by parties external to the service provider. Other regulatory or organization specific requirements should also be taken into account as they will impact some of the defined policies and procedures. All accounting practices used should be aligned to the wider accountancy practices of the service provider's organization.

The budgeting and accounting for services process should be performed by the service provider, regardless of whether other aspects of financial management are performed elsewhere in the organization. The budgeting and accounting for services process should be aligned with and receive information from the financial processes of the service provider's organization.

6.4.3 Explanation of requirements

6.4.3.1 Policy

The service provider should have a documented policy and procedures for the financial management of services. The policy should define the objectives to be met by the budgeting and accounting for services process. The policy should also define the detail required to ensure that the objectives are met. To do this the policy should include the cost types used in the budget for cost allocation and an explanation of how overhead costs are apportioned.

Criteria should be defined to allow for a budget and accounting analysis for each service. When defined, these criteria can be applied to the budget items and accounting entries to guarantee that some periodic monitoring and visibility is available regarding the costs of services. This can be used to track the costs of a service and allow comparison with the costs of acquiring the same service elsewhere in the market.

The resources provided for the budgeting and accounting for services process should be based on the needs of the customer, service provider, suppliers and other interested parties for financial detail, as defined in the policy.

6.4.3.2 Cost types

The service provider should select categories for cost entries in the budget that are useful for service management. For example, service providers should define cost models in line with services and their components, as defined in the catalogue of services, Clause 6.1. A cost type should be assigned to each cost that forms part of a service. Cost models are useful as they enable the service provider to more accurately predict the cost/benefit of different levels of service quality, or of different service options. Cost models should be able to demonstrate the full cost of provision for each service.

The service provider should also consider cost types such as:

a) assets used to provide the services;

b) shared resources such as a service desk, also known as level 1 support;

c) overheads such as office space;

d) services delivered by suppliers;

e) the cost of employing the service management personnel.

When identifying suitable cost types there should be a balance between the benefits of detailed accounting information derived from cost types and the challenges of collecting and managing the large volumes of information required. Cost types should be based on categories that can be measured easily and reliably. Examples include hardware costs, software maintenance costs, and personnel costs.

6.4.3.3 Apportioning overheads and allocation of direct costs

Apportionment of overhead costs may be based on a variety of mechanisms, such as a flat rate cost, a fixed percentage, or based on the size of an agreed variable element of delivered services.

The service provider should use methods for apportioning overheads and allocating direct costs that are appropriate for their organization, balancing the cost of managing apportionment against the benefit of being able to apportion costs in detail. Other factors that can be considered include:

a) the nature, range and consumption or use of the services;

b) the granularity of the customer's organization, e.g. a business unit as one unit, subdivided into department, or by locations;

c) SLAs and the apportioning of costs for services and service levels;

d) services provided by suppliers.

6.4.3.4 Budgeting

Forecasting of costs and revenue for budgeting should take into account the planned changes to services during the budget period. Seasonal variations and short term planned changes to service costs and charges, where applicable, should be understood and included within forecast budgets. Budgeting and cost tracking should support planning to operate and improve the services so that service levels can be maintained throughout the year. There should be sufficient planned expenditure to cover the resources required to support the services to the agreed service levels for the agreed duration. A procedure for identifying and managing variances of actual against budgeted expenditure should also be established.

6.4.3.5 Accounting

Accounting activities should be used to track costs to an agreed level of detail over an agreed period of time. Decisions about service provision should be based on cost effectiveness comparisons. Cost models should be able to demonstrate the full costs of service provision.

Accounting reports should demonstrate over and under-spending. Ideally accounting reports should also provide sufficient information to calculate the costs of low service levels or costs resulting from a loss of service. To calculate the costs of low service levels or loss of service, the service provider should have a clear understanding of costs of resources required to deliver the service. This should include personnel, components, facilities, and any aspects of the service delivered by other parties. The service provider should also have a clear understanding of the business impact of loss of service, depending on duration, time of day/week/month or year and the service in question. This information can be provided by a business impact analysis.

Accounting reports may also utilize information from the CMDB regarding the status and lifecycle of CIs to calculate total cost of ownership and depreciation of CIs supporting a particular service. This information can in turn be used to understand and plan for costs in the next budget cycle.

6.4.3.6 Charging

Charging is not included in ISO/IEC 20000-1 but it is recommended that where charging is in use, the charging mechanism is defined and understood by all parties.

6.4.4 Documents and records

Documents and records to be produced and used by the customer, service provider and interested parties include:

a) policies, processes and procedures for budgeting and accounting;

b) historic budgets, draft budget for the next year, actual budget for the current year;

c) service management forecasts of workloads, capacity (including personnel), unit costs of revenue items; planned capital expenditure;

d) timetable for budget production;

e) financial reports showing costs and revenue for each time period in the budget year, with any variances;

f) reports on the causes of variances and how they will be managed;

g) financial input to continual service improvement projects;

h) cost models showing how cost elements are used to provide services and create value;

i) reports required for legal or regulatory purposes.

6.4.5 Authorities and responsibilities

In addition to the process owner, process manager and personnel performing the procedures of the process as described in Clause 4.4.2.1, authorities and responsibilities required within the budgeting and accounting management process should include:

a) a budgeting and accounting manager, responsible for the management of financial resources;

b) managers with accountability for a specific budget in the service provider's organization.

6.5 Capacity management

6.5.1 Intent of the requirements

The capacity management process should ensure that sufficient capacity is provided to meet the current agreed capacity and performance requirements. The service provider should create and implement a capacity plan to meet the agreed future service capacity and performance requirements.

6.5.2 Concepts

Resources should be balanced to fulfil both current and agreed capacity and performance requirements, and to be prepared to fulfil future requirements.

The capacity management process should include both reactive and proactive activities. The reactive activities should focus on ongoing monitoring, tuning, analysis and improvement of operational capacity. The proactive aspect of the process should focus on planning to meet future agreed business demand.

The capacity management process should develop plans to ensure that capacity requirements can be agreed, forecast and met. These plans should transform business predictions and workload estimates into specific

capacity requirements. This should be facilitated by incorporating the following three areas of focus into the capacity management process:

a) business capacity management, which focuses on quantifying customer and service provider business plans and needs into future service requirements;

b) service capacity management, which focuses on planning and managing services and the supporting resources to ensure they meet all of their agreed service targets;

c) component capacity management, which focuses on planning and managing operational resources and components to ensure they effectively support the services and achieve agreed component targets.

6.5.3 Explanation of requirements

6.5.3.1 Capacity management activities

Capacity management activities encompass day to day operational tasks such as monitoring capacity usage and analysing capacity data, managing performance against service targets and planning for future capacity requirements.

Activities of the capacity management process include those listed below.

a) Assess, document and agree the capacity requirements, define workload, performance baselines, and set workload and performance thresholds and triggers.

b) Assess, document and agree the capacity requirements for new or changed services.

c) The capacity management process should be involved in the design of new or changing services and make recommendations for the procurement of components and resources, where performance and/or capacity are factors. In the interest of balancing cost and capacity, the capacity management process should obtain the costs of alternative proposed solutions and recommend the most appropriate cost-effective solution.

d) Activities for new capacity requirements should be based on input from planning, support teams and business groups. This should include planning the implementation of infrastructure from new projects and predicting the replacement of aging infrastructure components.

e) Set, monitor and use capacity thresholds, warnings and alarms to automatically manage and improve the utilization of components and the performance of services.

f) Maintain data and information used by the capacity management process in a repository, often referred to as the capacity database. This repository should be a key element of the capacity management process. The data and information contained within the capacity database is analysed by all capacity management activities and should include business, service, resource or utilization and financial data, from all areas of technology as shown below.

    1) Business data: reliable information on the current and future needs of the business.

    2) Service data including, but not limited to: transaction response times, transaction rates and workload volumes.

    3) Component utilization data: Limitations of components on the level to which they should be utilized should be documented. Beyond this level of utilization, the resource will be over-utilized and the performance of the services using the resource will be impaired.

    4) Other data to be utilized by the capacity management process includes bottlenecks and identified weaknesses; redundancy and spare capacity; resource, component and service thresholds and tolerances; current, past and forecast throughput and performance; comparisons of actual achievements against forecast achievements.

g) Producing capacity and performance reports, which provide valuable information to many service management processes. The capacity reports should be consolidated and stored within the capacity database so that interested parties can refer to them. These reports should include those listed below.

   1) Component-based reports and information to illustrate how components are performing and how much of their capacity is being used.
   2) Service-based reports and information to illustrate how the service and its constituent components are performing with respect to their overall service targets and constraints. These reports provide the basis of customer service reports and SLM reports on capacity and performance.
   3) Exception reports that show management and technical personnel when the capacity and performance of a particular component or service has become unacceptable should also be produced. In particular, exception reports should be of interest to the SLM process in determining whether the targets in SLAs have been achieved or breached. The incident and service request management process and the problem management process can then use the exception reports in the resolution of incidents and problems.

h) Forecasting of future component and service capacity and performance should be done in a variety of ways, depending on the techniques and the technology used. Examples include those listed below.

   1) Baseline modelling is the first stage in modelling. It is used to create a baseline model that reflects accurately the performance that is being achieved. When this baseline model has been created, predictive modelling can be developed.
   2) Trend analysis is completed using the resource utilisation and service performance information that has been collected.
   3) Analytical modelling uses mathematical techniques to analyze the performance of computer systems.
   4) Simulation modelling involves the modelling of discrete events, e.g. transaction arrival rates against a given system configuration.

6.5.3.2 Capacity plan

The capacity plan should document the actual performance, the expected business capacity needs and the service requirements. It should be produced at least annually or more frequently if rates of change to services and service volumes demand it. It should document the recommended solutions to achieve the agreed service targets and cost options for meeting the business requirements.

The capacity plan should include:

a) current and forecast service usage, ideally including recommendations regarding opportunities to influence the demand for capacity;

b) current and forecast resource usage and performance, including an understanding of which resources support which services;

c) the impact on capacity and performance of agreed requirements for availability, service continuity and service targets, e.g. workload estimates and capacity requirements in the event of a disaster;

d) time-scales, thresholds and costs for upgrades to service capacity, e.g. the required dates and costs for delivery of an increase in service capacity as the result of a business merger;

e) summaries of relevant business plans, scenarios and patterns of business activity;

f) summary of changes in business activity, including user profiles if available;

g) details of the methods, assumptions and information used in calculating the details in the capacity plan;

h) potential impact of new technologies on capacity and performance;

i) data and procedures to enable predictive analysis, e.g. modelling techniques;

j) potential impact on statutory, regulatory, contractual and organizational requirements, e.g. a plan to sustain sufficient storage and back up capacity for electronic medical records to satisfy regulations.

6.5.4 Documents and records

The documents and records produced and retained by the capacity management process should include:

a) capacity plan;

b) capacity management procedures;

c) baselines and profiles;

d) capacity management database;

e) service and resource threshold specifications and the thresholds for events and alarms;

f) service performance reports;

g) utilization levels and schedules;

h) effectiveness reviews;

i) workload analysis;

j) capacity management exception reports;

k) reviews of incidents records relating to capacity and performance.

The documents and records reviewed by the capacity management process should include customer and business current and future service capacity demands and requirements, including SLAs and required levels of service and audit reports. Changes to the capacity plan should be managed through the change management process.

6.5.5 Authorities and responsibilities

In addition to the process owner, process manager and personnel performing the procedures of the process as described in Clause 4.4.2.1, authorities and responsibilities required within the capacity management process should include the following.

a) Capacity analyst, responsible for analysing and reviewing capacity and performance data to identify actual and potential capacity issues so that solutions for removing those issues and maintaining service performance can be identified. The capacity analyst assists in the identification of options and analysis and recommendation of the preferred solution(s) to meet ongoing demand for capacity.

b) Customer and business representatives, responsible for the documentation and agreement of all capacity requirements.

6.6 Information security management

6.6.1 Intent of the requirements

The information security management (ISM) process should ensure that security controls are in place to protect information assets and that information security requirements are incorporated into the design and transition of new or changed services.

6.6.2 Concepts

Information security should be the result of a system of policies and procedures designed to identify, control and protect the organization's information and any resources used in connection with its storage, transmission and processing.

Management should ensure that clearly defined information security management objectives are in place and that they align to business needs.

The service provider and customer should categorize information assets according to value, confidentiality or business impact. For each category the service provider and customer should define and agree to an acceptable level of risk.

6.6.3 Explanation of requirements

6.6.3.1 Information security policy

Service requirements, statutory and regulatory requirements and contractual obligations should provide the basis of an information security policy. The policy should give direction on the use of physical, administrative and technical information security controls designed to preserve the security of information assets, e.g. confidentiality, integrity and accessibility. The policy should be approved by managers accountable for the SMS and the services.

The scope of the information security policy should include but not be limited to physical, administrative and technical controls required to ensure the confidentiality, integrity and accessibility of information assets within the scope of the SMS. The scope of the information security policy may exceed the scope of the SMS to accommodate the needs of the business.

Management should ensure that personnel, customers and suppliers and internal groups have both adequate understanding of the contents of the policy and an appreciation for the importance of adhering to it.

Management should also ensure that the information security policy is used as part of risk assessments and during information security audits.

The policy should provide guidance on the criteria for accepting risks and the approach for managing identified information security risks, e.g. password management.

The policy should ensure that internal information security audits are conducted at regular intervals, e.g. following an information security breach or following the deployment of a new or changed service.

The policy should ensure that information security audit results are reviewed at regular intervals and used to identify opportunities for improvement to information security. For example, correcting vulnerabilities identified during an information security audit.

NOTE Personnel with specialist information security roles can find it helpful to become familiar with ISO/IEC 27002, Information technology — Security techniques — Code of practice for information security management. This International Standard includes guidance on the content of a security policy.

6.6.3.2 Information security controls

Information security controls should guarantee that the information security management objectives are achieved and the information security risks are managed. Information security controls can be physical, administrative or technical.

The service provider should ensure that the controls are documented, describing their related risks and risk mitigation strategies. The service provider should also define the authorities and responsibilities for reviewing the controls and how often they should be reviewed.

The service provider should also define information security controls to manage external organizations and individuals that need to access, use or manage the organization's information or services.

6.6.3.3 Risk assessment

ISM process should conduct regular risk assessments to identify information security risks to the live environment, and then document and put in place specific controls to prevent or minimize the impact of identified risks. Additionally, the ISM process should perform or ensure appropriate risk assessments are performed as part of the design and transition of new or changed services.

The information security policy should ensure that Information security risk assessments:

a) are performed at agreed intervals, including for new or changed services;

b) are recorded and visible only to approved personnel;

c) are maintained during changes to business needs, processes and configurations;

d) aid in understanding what could impact a service;

e) define requirements for information security audits.

f) inform decisions regarding the types of controls to be operated.

Risks to information assets should be assessed according to the nature of the risk and the potential business impact.

NOTE Personnel with specialist information security responsibilities can find it helpful to become familiar with ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*.

6.6.3.4 Managing information security risks

The information security controls should ensure that the service provider is able to achieve the service management objectives and the requirements of the security policy. The controls should also enable the service provider to manage all identified information security risks.

The following are examples of information security controls:

a) the information security policy should be established, implemented and communicated to personnel, suppliers and the customer;

b) authorities and responsibilities for the information security management process should be defined and allocated;

c) the effectiveness of the information security policy should be monitored, measured and assessed;

d) personnel with significant information security roles should receive information security training;

e) expert help on risk assessment and control implementation should be available;

f) changes should not compromise the effective operation of controls;

g) information security incidents should be reported in line with incident and service request management process and allocated an appropriate priority;

h) an information security incident should be escalated to personnel with appropriate clearance to resolve it, depending on the priority and the level of authorization required to access the security incident record;

i) the details of information security incidents should only be visible to personnel with appropriate clearance;

j) regular risk assessments should be completed to identify changes to the readiness to tolerate risk of the organization;

k) regular audits should be conducted to assure compliance of the established information security policy and controls;

l) information security baselines should be defined and effectively applied;

m) findings of information security audits should be analysed, culminating in prioritized action plans;

n) information security training plans and training records should be created and kept up to date.

The service provider should work with the supplier management process to ensure information security controls are identified, documented and managed with any external organization that has access to or utilizes the service provider's information.

6.6.3.5 Information security changes and incidents

Information security changes and incidents should be processed in accordance with the change management process and the incident and service request management process.

Requests for change should be assessed to identify any new or changed information security risks as a result of the proposed change. The request for change should also be assessed against any potential impact on existing services, processes, policies or the existing information security controls.

The service provider should use the results of reviews of information security incident records as well as information security assessments and audits to identify potential deficiencies and opportunities for improvement.

6.6.4 Documents and records

The documents and records that should be produced and retained by the ISM process should include:

a) an information security strategy;

b) information security policy;

c) information security plan;

d) information security management procedures;

e) information security reports;

f) ISM process effectiveness and efficiency reports;

g) information security incident records;

h) information security risk assessments;

i) information asset inventories.

Documents and records should be analysed periodically to provide management with information on the effectiveness of the information security policy. Other features of interest includes trends in information security incidents, input to a plan for improving the service and control over access to information, assets, and systems.

6.6.5 Authorities and responsibilities

In addition to the process owner, process manager and personnel performing the procedures of the process as described in Clause 4.4.2.1, authorities and responsibilities required by the ISM process should include:

a) customer, service provider personnel and interested parties that require access to ISM CIs and data;

b) personnel that maintain the information security controls.

7 Relationship processes

7.1 Business relationship management

7.1.1 Intent of the requirements

The BRM process should ensure that mechanisms are established to manage the relationship between the service provider and the customer(s). An outcome from the process should be improved customer satisfaction and delivery of value through achievable business outcomes. The accountabilities and responsibilities of both the customer and the service provider for identifying and prioritizing service requirements should be clearly defined. Procedures to manage the ongoing relationship between the service provider and the customer should be defined and followed.

Mechanisms to manage the relationship between the service provider and the customer should include:

a) a designated individual who is responsible for managing the customer relationship and customer satisfaction;

b) regular communications with the customer to enable the service provider to understand the business environment, business needs and priorities, and requirements for new or changed services;

c) regular performance reviews with the customer of services in the live environment.

7.1.2 Concepts

The BRM process should be a key enabler toward developing the strategic alignment between the service provider and the customer. It should be through the alignment of the customer's business needs and the objectives of the service provider that increased business value is achieved. The BRM process should contribute to the reduction of any perceived or actual barriers between the service provider and its customer.

There should be a strong link between the BRM process and the SLM process. The SLM process should define and use measures to evaluate service level performance. The SLM process should manage currently delivered services and service levels at an operational level.

In contrast, the BRM process should seek to work closely with the customer to understand future business objectives and direction. By doing this, the BRM process should ensure that changes to services can be planned for in advance of their need by the customer. A good understanding of the customer's business objectives should also allow the service provider to offer closely aligned solutions that meet the customer's business needs.

Where large commercial services are delivered to many customers it can be difficult to have an individual relationship with each customer. For example, internet services used by individual households. In this case consideration should be given to how the service provider interacts with multiple customers. Measurement of customer satisfaction can be used to ensure that planned services and actual services are aligned to customer requirements.

7.1.3 Explanation of the requirements

7.1.3.1 General

The service provider should identify and document its customers, other interested parties, suppliers and dependent sub-contracted suppliers, in order to fully understand the dependencies between services. For

example, an internet based service being dependent on a service providing secure web portal and encryption capability. The interested parties can include user groups and business units.

The service provider should classify their customers according to the type of services delivered. Customers with similar characteristics may be grouped in similar ways to improve efficiency and effectiveness. The processes defined by the service provider may be different for each type of customer at a detailed level.

The service provider should identify a named individual(s) to be a clear single point of contact, who is responsible for managing the relationship and customer satisfaction for each customer. This individual may be chosen to manage the customer relationship on a fulltime basis, or may have the role combined with another role, if appropriate.

It is possible for the roles of business relationship manager and service level manager to be performed by the same person, due to the close relationship between the BRM and SLM processes. If the same person has both roles, the role descriptions should distinguish the different nature of the roles: the BRM process is strategic while the SLM process is operational or tactical. The risks of having one person performing these two roles with such different perspectives should also be managed.

The communication mechanisms established with the customer should include ad-hoc meetings and informal meetings, in addition to formalized and documented meetings. These communications should build a relationship with the customer, identify changes in business priorities and objectives and then trigger communication back to the service provider for action.

The communication mechanisms should aid understanding of the business environment in which the service operates including business needs, customer requirements and major changes. The service provider should use this information to respond to the identified needs.

Service providers can use a tool to track and manage information about the customer.

7.1.3.2 Customer service management reviews

The service provider should hold formal meetings with the customer to review customer satisfaction, strategic direction and major exceptions to the performance of the services. These meetings should include reviews of SLAs and performance, changes within the service provider's organization and changes within the customer's organization.

The meetings should be attended by representatives from all parties. The meetings should be scheduled in advance and held regularly, at least annually. The actual frequency should be influenced by the rate of change in service requirements, major projects such as new services and the quality of the service delivered. Meetings should be more frequent than the annual minimum when the service provider and customer are managing a high rate of change or when there are concerns about the quality of services. For example, a rapid rate of change in service requirements, major projects such as new or changed services. Holding customer review meetings more than four times a year can be counter-productive when there is insufficient content for the meeting for the management representatives involved.

The outcomes of customer reviews can result in the identification of new services or changes required to existing services or service levels. The service provider should ensure that changes to SLA(s) and contracts are managed through the change management process and follow the established SLM process.

Traceability from the customer requirements to the service change should be established.

7.1.3.3 Customer satisfaction

The service provider should establish a formal mechanism for recording customer satisfaction. The frequency and scale of any measurement should be agreed with the customer in advance, and this should include the sample of users to be surveyed. Such activities may often be driven by the service desk, also known as level 1 support, following incident/problem resolution. However, for true measurement of customer satisfaction, a broader measure should be undertaken that includes, for example, number and type of service requests,

actual cost, perceived cost and business value of the delivered services. The results should be identified, analysed and reviewed to identify opportunities for improvement.

Satisfaction survey results should be measured over time, so that trends in satisfaction can be tracked and any necessary issues or improvements identified.

The documented service complaints procedure should include recording, investigating, acting upon, reporting and closing any service complaints received. It should include an escalation procedure to be used if the customer does not agree to or accept the proposed actions or resolution. The complaint should remain open until the customer provides formal agreement that it can be closed.

The service provider should understand, define and agree with the customer what constitutes a formal service complaint. A formal service complaint is normally very serious and submitted in written rather than verbal form. The formal service complaint should be sent by a manager of the customer to a manager of the service provider. An incident or problem may be the cause of complaints but they are not themselves complaints.

The outcome of the review of the complaint should be summarized and reported back to the customer so that they can see that their opinions have been taken seriously and acted upon.

7.1.4 Documents and records

Documentation for the BRM process should include:

a) a description of the customer/interested parties, including basic contact information, key roles, services consumed;

b) a role specification for the designated individual to be shared with the customer;

c) agenda and minutes from any formal meetings between the customer and service provider;

d) notes from any informal meetings between the customer and the service provider;

e) summary of service metrics showing overall performance of the service provider;

f) service complaints procedure;

g) records of complaints and actions taken;

h) customer satisfaction survey/measurement;

i) records of satisfaction review, analysis and action;

j) summary of outcomes from customer satisfaction for feedback to customer.

7.1.5 Authorities and responsibilities

In addition to the process owner, process manager and personnel performing the procedures of the process as described in Clause 4.4.2.1, authorities and responsibilities required within the BRM process should include:

a) a business analyst role, responsible for performing overall customer satisfaction activities, including collecting and analysing complaints, customer satisfaction data;

b) a business relationship manager role, responsible for:

   1) improving customer satisfaction for each customer;
   2) acting on behalf of the customer within the service provider's organization;

3) establishing efficient and effective communication mechanisms between the service provider and customer(s);

4) conducting service reviews with the customer and ensuring improvements or actions are implemented;

5) ensuring that any changes to the customer's requirements are reflected in the SLAs and other documents, by the SLM process;

6) liaising with the SLM process;

7) management of formal service complaints to ensure they are resolved to the satisfaction of the customer;

8) ensuring that measurement of customer satisfaction is undertaken routinely and the results analysed, reviewed and acted upon;

9) communicating the results of customer satisfaction and resulting actions back to the customer in a timely manner;

10) ensuring any escalations from the customer are dealt with in a timely and effective manner;

11) understanding and planning for future business requirements.

The name of this role can vary, although business relationship manager is common. Other possible titles are customer relationship manager or account manager. The service provider should be aware that this role can be merged with another, or be performed by a whole team, depending on the circumstances.

In order to perform this role effectively the service provider should recognise the need for expertise in the service provider's own business, the technology and the customer's business requirements and priorities. This expertise should also be used to communicate customer requirements to the service provider's technology specialists. The complexity of this role means that attention to detail and the ability to liaise with multiple parties should be recognised as an important aspect of the role. The service provider should also recognise that these responsibilities are beyond the capabilities of a junior entry-level position.

7.2 Supplier management

7.2.1 Intent of the requirements

The purpose of the supplier management process should be to manage suppliers to ensure the provision of seamless, quality services. Service providers can use suppliers to operate some parts of the processes or services, or to supply components such as hardware and software. The supplier management process should be used for all suppliers. This includes suppliers operating processes or parts of processes for the service provider. The supplier management process can be a useful supplement for the SLM process for the management of internal groups and customers acting as suppliers.

7.2.2 Concepts

Supplier management procedures should ensure that:

a) the suppliers understand their obligations to the service provider;

b) agreed requirements are met within agreed service levels and scope;

c) changes to requirements and obligations are managed;

d) business transactions between all parties are recorded;

e) information on performance of all suppliers can be observed and acted upon;

f) the service provider’s SLAs with the customer are aligned with the supplier contracts.

7.2.3 Explanation of requirements

7.2.3.1 Managing contracts

The service provider should designate a contact person responsible for the relationship with each supplier. There should also be designated contacts between suppliers where services or components of services have dependencies.

The contract should include the requirements and service levels required of the supplier. The service targets agreed in the supplier's contract should be articulated to ensure that the service provider's SLAs with the customer can be met. If supplier service levels are not aligned with SLAs, this should be managed as a risk with plans developed to resolve the risk in a timely manner.

All supplier contracts should contain a review schedule. At least an annual review should be scheduled. The review should assess whether the business objectives for sourcing a service or a service component remain valid and the supplier is achieving agreed performance against the service targets in the contract.

There should be a clearly defined process for managing each contract. The process for contract amendment should also be clearly defined. Any changes to this procedure should be formally notified to all affected suppliers.

If a contract includes penalties or bonuses, their basis should be clearly stated and compliance to the requirements and service targets measured and reported upon.

When a supplier is to provide part of a service, the service provider should ensure that the contract with the supplier includes everything necessary to enable the achievement of the relevant customer requirements. This should be assured and documented prior to making a commitment to the customer. The supplier should also accept the service provider will have governance of the service management processes operated by the supplier, as described in Clause 4.2.

The service provider should, at planned intervals, obtain evidence that the supplier is meeting all requirements of the contract, and has quality processes that effectively ensure these requirements will be met consistently. This may be achieved by means of the service provider auditing the supplier.

All outcomes of meetings, reviews and audits concerning the subcontracted service should be reviewed to identify opportunities for improvement. Where changes are required, they should be controlled using the change management process.

7.2.3.2 Supplier details

The service provider should maintain the following for each service and supplier, even if this information is not included in the contract:

a) a definition of services, roles and responsibilities;

b) scope and capability of the service;

c) requirements to be fulfilled by the supplier;

d) defined and agreed service targets, penalties or consequences for service targets not met;

e) workload characteristics such as number of transactions, number of servers or database size;

f) agreed exceptions criteria for SLA;

g) contract management process, the authorization levels and a contract exit plan;

h) payment terms if relevant;

i) agreed reporting parameters and records of achieved performance.

7.2.3.3 Managing sub-contracted suppliers

It should be clear whether the service provider is dealing with all suppliers directly or with lead suppliers, each taking responsibility for sub-contracted suppliers.

The service provider should obtain evidence, from lead suppliers, that lead suppliers are formally managing sub-contracted suppliers. This evidence should be guided by the requirements of ISO/IEC 20000-1. The lead supplier should be required to record the names of all sub-contracted suppliers and their responsibilities and relationships. This information should be made available to the service provider if required. An example of suppliers and sub-contracted suppliers providing part of a service is shown in Figure 3, taken from ISO/IEC TR 20000-3.

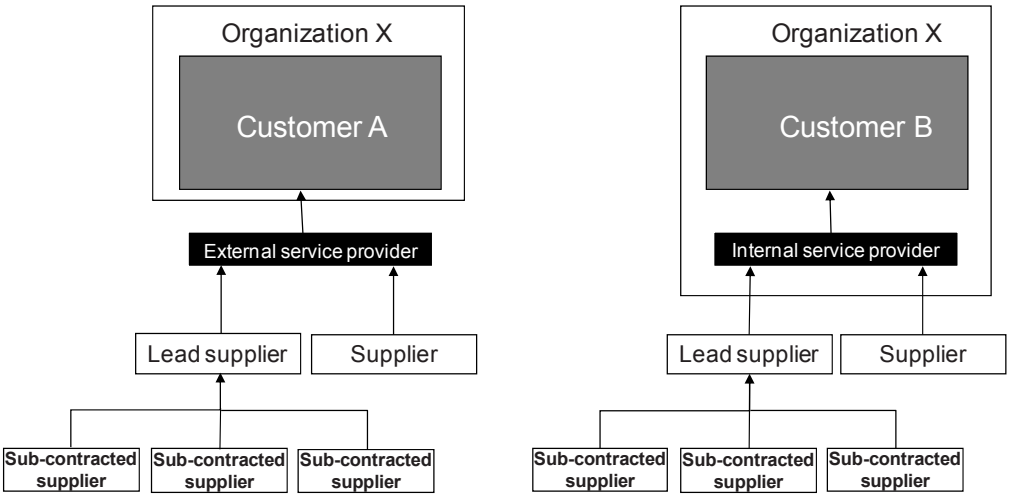

Figure 3 — Example of relationship with lead suppliers and sub-contracted suppliers

7.2.3.4 Contractual disputes management

Both the service provider and the supplier should agree a process for managing disputes. This should be defined or referred to within the contract and implemented if necessary. An escalation path should be available for disputes that cannot be resolved through the normal means of communication. The process should ensure that disputes are recorded, investigated, acted upon and formally closed.

7.2.3.5 Contract termination

The contract management process should include provision for contract termination, either at the expected end or prematurely. It should also provide for the transfer of the service to another organization at the end of the contract. The contract termination clauses should clarify the responsibilities for closing or transferring the service, costs, ownership of intellectual property, hardware, software licences and data.

7.2.4 Documents and records

An approved copy of all supplier contracts should be held by the service provider and the supplier. The contracts should include or reference a service definition and identify the service management processes that cover all services delivered by the supplier. The interface between processes operated by multiple parties should be documented.

The service provider should also hold:

a) the names, responsibilities and relationships within the organizations of all interested parties, including the customer, service provider, lead supplier and any subcontracted suppliers;

b) evidence that the service provider is formally managing the supplier, including records and actions from periodic contract review meetings, and reports from any subcontract audits;

c) evidence, similar to the above, that lead suppliers are formally managing subcontracted suppliers.

7.2.5 Authorities and responsibilities

In addition to the process owner, process manager and personnel performing the procedures of the process as described in Clause 4.4.2.1, authorities and responsibilities required within the supplier management process should include the following.

a) Supplier relationship manager, a designated individual responsible for managing the service provider's relationship with a specific supplier. This includes management of the contract and performance. Where several personnel are engaged in these activities, there should be a procedure to ensure that information on supplier performance is consistent, comparable, observed and acted on.

b) Defined contact person within each supplier.

8 Resolution processes

8.1 Incident and service request management

8.1.1 Intent of the requirements

The incident and service request process should manage incidents and service requests consistently to ensure that incident resolution or request fulfilment is achieved within agreed service targets and time frames.

8.1.2 Concepts

The incident and service request management process should enable the effective and efficient management of all incidents and service requests, in alignment with business and customer priorities. Data collected as part of the incident and service request process should be used to monitor performance against relevant service targets. This data can be included in service reports to the customer.

An incident is considered to be an unplanned interruption to a service, a reduction in the quality of a service or a failure of a configuration item that has not yet impacted a service. Examples of service requests may include standard changes, e.g. low risk, well defined and pre-approved changes, requests for information, requests for guidance or requests for access to standard services.

The incident and service request management process should be supported by two separate documented procedures. The first is for the management of incidents, the second for the management of service requests. The two procedures should define the following:

a) the consistent recording of incidents and service requests;

b) the prioritization and classification of incidents and service requests based on agreed and documented service targets;

c) activities necessary to resolve incidents and fulfil service requests, as detailed in the paragraphs below;

d) the actions needed to update and close incident and service request records on confirmation from the user that the incident has been resolved or the service request fulfilled;

e) escalation as appropriate to ensure resolution or fulfilment of each incident or service request in accordance with the agreed service levels.

The incident and service request procedures should include the comparison of incidents against known errors and problems and service requests against the catalogue of services.

8.1.3 Explanation of requirements

8.1.3.1 Receiving and recording incidents and service requests

Procedures for the incident and service request management process should define the mechanisms for receiving and recording incidents and service requests. This should ensure:

a) a consistent approach to handling;

b) the storage and retrieval of data as required by an organization;

c) appropriate communication channels/methods are used and are available, both within agreed service hours, and outside those hours.

All incidents and service requests should be classified so they can be acted upon in line with their priority and service target commitment. Classification by incident or service request type should include determining which CIs are impacted, which in turn should help to identify the personnel who may need to be involved in resolution or fulfilment.

The priority should be agreed with the customer upon receipt of the incident or service request, or as soon as possible afterwards. The determination of the priority should be based on an assessment of the impact and urgency of the incident or service request in question.

Incidents and service requests should be evaluated for possible security implications and determination whether security incident response procedures should be implemented in addition to normal operational response. For example, operational personnel should have procedures established to determine whether information security personnel or law enforcement personnel should be contacted.

A matrix of priorities based on impact and urgency should be developed for both incidents and service requests as part of discussing and agreeing the service targets. An example of target resolution times for incidents based on priority is shown in Table 1. The general principles of targets based each of several categories should be adopted for both incidents and service requests.

Table 1 — Example matrix of incident resolution target times based on priorities

	Impact			
Urgency	Major	High	Medium	Low
High	P1: Resolution in 2 hours	P2: Resolution in 4 hours	P3: resolution in 1 day	P4: Resolution in 2 days
Medium	P2: Resolution in 4 hours	P3: Resolution in 1 day	P4: Resolution in 2 days	P5: Resolution in 3 days
Low	P3: Resolution in 1 day	P4: Resolution in 2 days	P5: Resolution in 3 days	P6: Resolution in 5 days

Table 1 is for incidents, but service requests can have different target times and require a separate table.

8.1.3.2 Incident and service request lifecycle and use of data

The following should be defined as part of the incident and service request management process.

a) identification of input sources for incidents and service requests;

b) responsibilities for the creation and update of incident and service request records;

c) use of appropriate information sources, e.g. CMDB, known error database, the catalogue of services, other relevant document and records;

d) relationship with/interface to the problem management process;

e) rules for escalations, including triggers, functional or hierarchical types and authority to invoke;

f) interface to the change management process when a request for change is used to enable resolution of incidents or to fulfil service requests;

g) responsibility for verification of resolution of the incident or fulfilment of the service request;

h) the policy and approach for closure of the incident or service request, e.g. the process should seek a confirmation of effective recovery from the user or customer, then update the record, and finally set the record to a status of closed.

Without confirmation of effective recovery from the user or customer, the service provider may make an inaccurate assumption that the incident has been resolved or the service request has been fulfilled.

8.1.4 Major incident procedure

The incident and service request management process should include a documented procedure specifically for the handling of major incidents. A major incident generally imposes higher impact and special attention is required to resolve it.

The major incident procedure should define:

a) what constitutes a major incident;

b) who has the authority to declare a major incident and how it will be declared;

c) who should coordinate and control activities and who should be involved;

d) how resolution efforts will be conducted;

e) what communications should be provided during and following major incidents;

f) the format, timing and participants required for a major incident review following resolution;

g) the interfaces with the service continuity and availability management process, in the event that service continuity invocation is required.

8.1.5 Documents and records

The documents and records that should be produced and retained by the incident and service request management process should include:

a) incident and service request management procedures;

b) incident records;

c) service request records;

d) major incident records, including major incident reviews and action plans;

e) reports on incident and service requests over a given time period;

f) incident resolution and service request fulfilment performance reports, including instances where service targets were exceeded or not met;

g) statistical reports on call types, call closure types, call classifications, volume breakdowns;

h) exception reports for incidents and service requests mishandled, where quality factors may include categories such as misclassifications, priority adjustments, escalations, re-opened incidents and service request records with incorrect data;

i) incidents passed to the problem management process for problem investigation;

j) any potential improvements that have been identified or where action has been taken.

8.1.6 Authorities and responsibilities

In addition to the process owner, process manager and personnel performing the procedures of the process as described in Clause 4.4.2.1, authorities and responsibilities required within the incident and service request management process should include those listed below.

a) Major incident manager, responsible for invocation of the major incident management process, the response team and identifying the roles and personnel required for each major incident.

b) Level 1 support, which provides a communications role for gathering the initial symptom data and ongoing communications with end users.

c) Resolution groups that can be designated as level 2 and level 3 support. These groups would be assigned escalated incidents for diagnosis and resolution, and typically would have technical skills and experience exceeding those of level 1 support personnel.

d) Service delivery groups that can be assigned tasks to assist in the completion of each service request.

e) External suppliers and vendors that can provide support services as defined within underpinning contracts and agreements.

8.2 Problem management

8.2.1 Intent of the requirements

The problem management process identifies the unknown, underlying root causes of incidents and proposes permanent resolutions through the change management process. The problem management process also proactively prevents incidents from occurring through trend analysis and recommendations of preventative action.

8.2.2 Concepts

The problem management process should investigate the root causes of incidents. The problem management process should then minimize or avoid the impact of incidents and problems through proposing permanent solutions via the change management process.

The problem management process should also produce and manage the known error records including temporary fixes once the underlying root cause has been identified. The known error records can be used to ensure efficient incident resolution and organizational learning.

The problem management process should have a defined scope and should determine the problem management methods used. It can be useful to have a problem management policy that can define the criteria for both prioritization and investigation of problems.

The primary focus of the problem management process for many organizations is based upon incidents that have already occurred. There can be tremendous benefit to the organization in finding permanent resolutions for the highest impact and highest risk problems, which in turn can enable the services to become more reliable, cost-effective and efficient.

Once the environment has become more reliable as a result of these problem management activities, it may be possible for personnel to spend more time on proactive problem management. Proactive problem management activities should be aimed at preventing incidents from occurring in the first place. For example, identifying a potential single point of failure for a business critical service and proposing redundancy to prevent any future incident impacting the customer.

8.2.3 Explanation of requirements

The problem management process should include the procedures listed below.

a) Problem identification, including:
   1) detection of an unknown root cause of one or more incidents;
   2) the analysis of one or more incidents revealing an underlying problem;
   3) a notification from a supplier or an internal group of a problem with a component of the service.

b) Problem recording, to ensure that each problem is recorded. The records should include relevant details of the problem, including the date and time, and a cross-reference to the incident(s) that initiated the problem record.

c) Problem classification and prioritization, which should ensure that:
   1) each problem is categorized to help determine its nature and to provide meaningful information, making use of the same classification criteria that are used in the incident and service request management process;
   2) each problem is given a priority for resolution according to its urgency and the impact of related incidents;
   3) time and resources for investigating the problem and identifying the best options for resolution are allocated according to the priority of the problem;
   4) the resolution of the problem is allocated time and resources according to the priority of the problem and the benefit of making the change in order to fulfil service requirements.

d) Problem investigation and diagnosis, which should ensure that:
   1) each problem is investigated to diagnose the root cause;
   2) a method of resolution can be identified, which depends on the impact of related incident(s) and potential incidents, whether or not a temporary fix exists and the estimated cost of resolution;
   3) a decision to resolve the problem depends on the impact of related incidents, whether a temporary fix exists and the cost of resolution;
   4) a decision not to resolve the problem is managed according to the problem management policy;
   5) the problem management process is able to support the incident and service request management process even before the known error is found, through identifying a temporary fix;
   6) problem diagnosis is complete when the root cause is identified and a method of resolving the problem is identified.

f) Problem tracking should ensure that the progress of all problems is recorded to:
   1) track the progress through the problem management process, including details of the person currently responsible for progressing the problem;
   2) record all resources used and actions taken.

g) Problem escalation should ensure all issues are escalated to appropriate parties including:
   1) identification of related incident(s) breaching service targets;

2) cascading information to the customer so they can take appropriate actions to minimize the impact of the unresolved problem;

3) enable the service desk or level 1 support to provide regular updates to affected users or customers;

4) defining the escalation points.

h) Documenting known errors, which should ensure that:

1) when the root cause and a proposed method of resolving the problem is identified, a known error is recorded in the known error database, together with details of any temporary fix;

2) a known error record is not closed until after the permanent solution has been successfully implemented via the change management process;

3) known error records are made available to all relevant personnel and they are regularly made aware of any new or updated known error records;

4) if a known error record stays open for a defined duration of time, it is reviewed and kept up to date so that no obsolete information is held in the known error database;

5) all known errors are recorded against the current and potentially affected services and the configuration item suspected of being at fault.

i) Problem record closure, when the known error has been identified and recorded, should ensure that:

1) details of resolution have been accurately recorded;

2) the problem record has been matched to any related incidents to facilitate analysis;

3) the root cause is categorized to facilitate analysis.

j) Major problem reviews held to investigate unresolved, unusual or high impact problems, should ensure:

1) risks to the business, the customer or service provider are identified and managed;

2) there is management visibility into the reasons for unresolved problems, as well as their ongoing business impact.

k) Problem reviews should be recorded and should include appropriate recommendations for improvements to the service. They should examine:

1) opportunities to improve the problem management process;

2) opportunities to improve other processes, services or the SMS;

3) how to prevent recurrence or a particular type of problem;

4) whether training or awareness should be provided to correct or prevent incidents caused by human error;

5) whether there has been any responsibility on the part of suppliers, customers or internal groups for problems that have occurred and whether any follow-up actions are required.

l) Proactive problem management should ensure that:

1) incident and problem data, the CMDB and other relevant information sources are analysed to identify trends;

2) incident and problem data, the CMDB and other relevant information sources can be used to improve decision making and assist with pre-empting possible degradations of service;

3) the knowledge gained from a problem review is communicated to the customer to ensure that the customer is aware of the actions taken and the service improvement recommendations identified;

4) key measurements that demonstrate the business value of proactive problem management are defined;

5) potential single points of failure, emerging trends and risks to services are identified and options are proposed through the change management process.

8.2.4 Documents and records

The documents and records, that should be produced and retained by the problem management process should include:

a) problem management procedures;

b) problem records;

c) known error records;

d) details of temporary fixes;

e) links to changes resulting in permanent fixes;

f) problem review records including minutes of problem review meetings;

g) management reports including incident and problem trend information;

h) recommendations for service improvements.

A problem management policy can be useful to facilitate and support the problem management process.

8.2.5 Authorities and responsibilities

In addition to the process owner, process manager and personnel performing the procedures of the process as described in Clause 4.4.2.1, authorities and responsibilities required within the problem management process should include:

a) personnel who carry out the root cause analysis of problems, determine the resolution and/or temporary fix and create the associated known error data record;

b) suppliers, customers or internal groups involved in providing resolutions, temporary fixes, known error information, advice and reviews.

9 Control processes

9.1 Configuration management

9.1.1 Intent of the requirements

The configuration management process should include the identification, control, recording, tracking, reporting and verification of configuration items and the management of CI information in the CMDB. It should establish and maintain the integrity of information about identified services, service components and CIs across the service lifecycle. The configuration management process should also identify, manage and verify the information about relationships between CIs, as well as the relationships between CIs and the services they support.

The scope of the configuration management process should exclude financial asset management but include an interface to the financial asset management process.

9.1.2 Concepts

The configuration management process should provide a focal point for the management and control of the evolving service assets and configurations, as well as their relationships. It should include activities to plan and perform the configuration management process.

Configuration management should document the definition of each type of CI and identify each CI according to the configuration management policy and procedures. The information recorded for each CI should ensure effective control of each CI and its associated configuration information.

Configuration information is recorded in a CMDB that includes data on configuration items, versions, relationships, baselines and releases. The information for each CI should include an identifier, description, status, location, its relationships and associated records such as requests for change, incident, problem and known error records. Configuration information should be maintained by approved individuals and made available only to approved interested parties.

9.1.3 Explanation of requirements

9.1.3.1 Configuration Management activities

Planning for the configuration management process should enable a service provider to achieve a degree of control that is sufficient to:

a) fulfil the agreed requirements of the customer, user, service provider and other interested parties;

b) ensure that assets, including licences, used to deliver services are managed according to statutory and regulatory requirements and contractual obligations;

c) ensure that the integrity of information about services and service components is maintained;

d) maintain the recorded configuration information to ensure its reliability and accuracy.

9.1.3.2 Resources and capability

The configuration management process should be planned to ensure that there are sufficient resources and capabilities for both the implementation and maintenance of the evolving CI records. The scope of the configuration management process and policy should include:

a) planning the scope of the configuration management process aligned with the SMS and the scope of the change management process;

b) the definition of each type of CI and its relationships to other CIs and service components;

c) authorization to access and control changes to CIs;

d) documented procedures for identifying, recording, controlling and tracking versions and the status of CIs;

e) the locations and conditions of storage for physical CIs and in the case of information, storage media, in accordance with designated levels of integrity, security and safety;

f) the criteria or events for commencing configuration control and maintaining baselines of evolving configurations;

g) a documented procedure including the authorities and responsibilities for planning and conducting audits, reporting results and maintaining audit records;

h) planning for the removal, archiving, disposal or transfer of data regarding CIs in accordance with statutory and regulatory requirements and contractual obligations;

i) sufficient automation to ensure effective control , e.g. to reduce opportunities for human error.

9.1.3.3 Identification and definition of CIs

Planning should include the identification and definition of CI types that are subject to the control of the configuration management process. CIs should be chosen using established selection criteria, grouped, classified and identified in such a way that they are manageable and traceable throughout their lifecycle.

Each service should be classified or segregated into logically related and subordinate groups of the constituent service components that enable:

a) interested parties to find and use the configuration information that they are allowed to use;

b) a shared understanding between the interested parties on how information about CIs and their relationships are managed;

c) personnel involved in all service management processes to have access to the CMDB, the configuration management policy and procedures that are required or useful to help them fulfil their role;

d) the service provider to implement editable access to the CMDB solely to personnel having the correct levels of authority and provide read access to all other personnel.

CIs should be clearly identified by unique, durable identifiers or markings, where appropriate. The identifiers should be in accordance with relevant standards and conventions, so that all CIs under the control of the configuration management process are unambiguously traceable to their specifications or equivalent, documented descriptions. There should be a list of CIs and a definition of the information to be recorded for each CI. Appropriate relationships and dependencies between CIs should be identified to provide the necessary degree of visibility and control.

9.1.3.4 Types of CIs

CI types should include:

a) services as listed in the catalogue of services and their related information and documents, e.g. SLA, agreement, contract, service requirements, specification of service design;

b) service components including hardware, software and licences, tools, applications, documentation, supporting services;

c) all issues and releases of services, systems and software configuration baselines or build statements for each applicable environment and standard hardware build, e.g. image of a hardware configuration;

d) master copies of CIs stored in physical and/or electronic libraries, the CMDB and tools used;

e) information security assets;

f) assets that need to be tracked for financial asset management or business reasons, e.g. secure magnetic media, equipment;

g) SMS documentation, e.g. policies, process documentation, procedures, plans.

Each CI type should have associated information in the CMDB or in integrated documents or records.

9.1.3.5 Maintenance of CIs

Performing configuration management should include activities to maintain information on CIs and their relationships with an appropriate level of integrity and security.

The configuration control procedures should ensure that only agreed and identifiable CI types and records are accepted and held in a suitable and secure environment. No CI should be added, modified, replaced or removed/withdrawn without appropriate controlling documentation, e.g. an approved request for change. The

evolving status of CIs through their lifecycle should be documented as a baseline triggered at designated times or under defined circumstances. The rationale for the baseline should be recorded. Configuration records should be maintained throughout the lifecycle of a CI and archived or removed according to the configuration management policy.

To protect the integrity of systems, services and the infrastructure, records of CIs and the CMDB should be held in a suitable and secure environment. This environment should protect them from unapproved access, changes or CMDB corruption. There should also be a means for disaster recovery of the CMDB and a method that permits the controlled retrieval of a copy of the controlled master, e.g. software, electronic media.

Configuration audit activities should be performed both at planned intervals and in response to specific events. Adequate procedures and resources should be in place to:

a) verify that the service provider is in control of the information about all CIs and their relationships within the scope of the process;

b) verify that the service provider is in control of information about the location and quantity of software licences;

c) provide confidence that configuration information is accurate, controlled and visible to approved personnel;

d) identify the cause of any discrepancies between the actual and expected configuration information and resolve in coordination with the change management process;

e) ensure that a configuration baseline is done at regular intervals and at least prior to the deployment of a release into the live environment;

f) ensure confidentiality and accessibility of the information in the CMDB.

9.1.4 Documents and records

The documents and records that should be produced and retained by the configuration management process should include:

a) a configuration management policy;

b) procedures for the configuration management process;

c) up to date and accurate information about CIs and their relationships to other CIs, service components and services;

d) CI type definitions;

e) configuration baselines;

f) configuration management reports;

g) configuration audit reports;

h) a documented procedure specifying frequency and testing of backups of the CMDB.

9.1.5 Authorities and responsibilities

In addition to the process owner, process manager and personnel performing the procedures of the process as described in Clause 4.4.2.1, authorities and responsibilities required within the configuration management process should include:

a) the customer, users, service provider personnel and interested parties with authorized access to configuration information;

b) personnel who maintain the CMDB;

c) responsible asset or CI owner who ensures that updates regarding the status of CIs is provided;

d) internal and external suppliers of assets and CIs.

9.2 Change management

9.2.1 Intent of the requirements

The change management process should manage changes through their lifecycle, ensuring all changes are assessed, approved, implemented and reviewed in a controlled manner.

9.2.2 Concepts

The change management process provides a structured approach for the effective implementation of changes that minimizes risk and ideally the prevention of incidents caused by unmanaged or poorly managed changes.

To enable the required visibility and control, all requests for change should be recorded and classified. A schedule of change containing details of the changes approved for development and their proposed implementation dates should be established and communicated to interested parties and updated as necessary.

Typical examples of types of request for change are given below.

a) Emergency change: a change that should be implemented as soon as possible. For example, to resolve a major incident or implement an information security patch.

b) Normal change: any planned service change that is not a standard change or an emergency change.

c) Standard change: a pre-authorized change that is low risk, relatively common and follows a procedure or work instruction.

Normal changes can be categorized as major, significant and minor, depending on the level of cost and risk involved. This categorization can be linked to and used to identify an appropriate change authority, a person with authority for that category of change.

Procedures should be documented and used to control the recording, classification, assessment, approval, planning, development, testing and deployment of all changes.

Following the successful implementation of changes, the change management process should inform the configuration management process that the CMDB should be updated to reflect the changed environment.

9.2.3 Explanation of requirements

9.2.3.1 Change management policy

A change management policy should be established and documented that defines the CIs under the control of the change management process. All requests for change to CIs defined in the change management policy as within the scope of the change management process should be managed by the process.

Changes with the potential to have a major impact on services or the customer should be classified according to defined criteria in a change management policy. These changes should be managed using the design and transition of new or changed service process and coordinated with the change management process.

The change management policy should define criteria for determining which changes should be managed through the change management process and which changes should be managed through the design and transition of new or changed services process.

The criteria used to determine changes to be managed through the design and transition of new or changed services process should include changes for the removal of a service and changes for the transfer of a service from the service provider to another party. The other party can be the customer or a supplier.

9.2.3.2 Planning and implementation

Requests for change should have a documented scope and they should be classified according to defined and agreed criteria. Requests for change should be assessed and approved before development or build, taking into account the risks, impacts to services and the customer, financial ramifications, business benefits and technical feasibility.

The management of the build, test and implementation of changes should be coordinated with the configuration management process and the release and deployment management process.

The activities required to reverse or remedy an unsuccessful change should be planned and tested. The change should be reversed or remedied if unsuccessful. Unsuccessful changes should be investigated and appropriate actions taken.

A schedule of change containing details of the changes approved for development and their proposed implementation dates should be established and communicated to interested parties, e.g. level 1 support; BRM, supplier management.

The change management process and procedures should ensure that:

a) changes have a clearly defined and documented scope that identifies the impacted configuration items;

b) decision making on the acceptance and approval of requests for change takes into consideration the risks, priorities, potential impacts to services or the customer, the service requirements, business benefits, technical feasibility and financial impact;

c) a schedule of change is established that contains details of the approved changes and their proposed deployment dates;

d) the schedule of change is communicated to interested parties;

e) the schedule of change is used for planning the deployment of releases;

f) approved changes to the identified services and configuration items are developed and tested according to the schedule of change;

g) changes are deployed according to the schedule of change;

h) activities to reverse or remedy an unsuccessful change are planned and tested;

i) unsuccessful changes are reversed or remedied and the reasons for the unsuccessful change are documented and investigated;

j) the CMDB is updated following the deployment, regardless of the success or failure of that change.

9.2.3.3 Reviewing the request for change

Recorded requests for change should be analysed at planned intervals to identify increasing levels of changes, frequently recurring types, emerging trends and other relevant information. The results and conclusions drawn from the analysis of changes should be recorded and used to identify opportunities for improvement. Any nonconformity should be recorded and action taken.

Any weaknesses or deficiencies identified in the change management process as a result of a review of an individual request for change should be incorporated into plans for improvement.

Once the change has been deployed and accepted the request for change should be closed. The request for change can also be closed when a decision has been made to not carry through the change. When the request for change has been closed the result of the change should be reported to the initiator of the request for change and other interested parties.

9.2.3.4 Emergency changes

Emergency changes should be differentiated from other changes, due to the increased risk and often increased cost of approving and implementing them.

For emergency changes there should be a defined process that includes arrangements for approval and post-implementation documentation and review. Emergency changes should be approved by an appropriate change authority and if possible, communicated to interested parties.

Emergency changes may be used to resolve emergency situations where there is insufficient time to adhere to normal change process procedures, time lines and approval authorities. Where possible, the complete change process should be followed. However, due to the urgency of implementing an emergency change, some details may be documented retrospectively and some testing may not be possible. Even if some of these steps are bypassed to accommodate the urgency of the emergency, there should be a plan to reverse or remedy the emergency change if it is unsuccessful. Where the emergency procedure bypasses other change management requirements, e.g. incomplete testing prior to implementation, the change should conform to these requirements as soon as practicable. Emergency changes should be justified by the implementer and reviewed after the change to verify that it was a true emergency.

9.2.4 Documents and records

The documents, including records, that should be produced and retained:

a) change management policy;

b) change management process documentation and procedures, including an emergency change procedure and a standard change procedure;

c) a list of approved standard changes;

d) a schedule of changes;

e) recorded requests for change and any related information e.g. risk assessment, remediation plan, deployment plan;

f) change management process effectiveness and efficiency reports;

g) change management reports, including post implementation reviews.

The change records associated with each request for change should be recorded in a suitable change log. If the organization has a CMDB, the change record should be associated to the relevant CI via a link to the CI record. Ideally this link between the change record and the relevant CI or CIs should be visible from the time the request for change is recorded, through approval and implementation.

9.2.5 Authorities and responsibilities

In addition to the process owner, process manager and personnel performing the procedures of the process as described in Clause 4.4.2.1, authorities and responsibilities required within the change management process should include those listed below.

a) The roles and individuals that can record and classify a request for change.

b) An owner that is responsible for managing the lifecycle of each request for change, e.g. service owner, process owner.

c) Nominated representatives to provide advice on the impact of changes. This may be a change advisory board that typically includes representatives of the service provider, customer and interested parties depending on the scope and impact of the change on the service and business environment.

d) A change authority to make decisions on the acceptance and approval of change. A change authority should be relevant to the change type and may be a nominated role, an individual or a change advisory board and emergency change advisory board.

9.3 Release and deployment management

9.3.1 Intent of the requirements

The release and deployment management process should ensure that all releases are effectively deployed into the live environment so that the integrity of hardware, software and service components is maintained. The release and deployment management process should coordinate all aspects of a release. This should include technical functionality, integration with the environment, allocation of resources to develop, test and deploy the release, training, support, release documentation. All aspects should be considered together to ensure that the release is successful.

The integrity of the live environment should be protected and disruption should be minimized through proper planning, testing and coordination with the change management process.

9.3.2 Concepts

The release and deployment management process is responsible for coordinating both large or complex releases and minor releases. The release and deployment management process should therefore be designed to enable effective management and coordination of releases with different scope, complexity and degrees of risk.

A release may be one or more changes to a service that are built, tested and deployed together. Multiple changes may be packaged together into one or more release to help to manage dependencies and for efficiency. A release package should include a set of CIs that will be deployed together as a single release.

The release and deployment management process should ensure that the changes within each release are compatible with each other.

Deployment should be responsible for distributing and delivering the service and service components at the correct location and time in the target environment.

The service provider should co-ordinate release and deployment activities with the customers, users and interested parties. In many cases releases should be coordinated with business change projects and with business change management to ensure alignment with relevant awareness, communication and training programmes.

The release and deployment management process should plan and manage individual releases for new or changed services in coordination with both the design and transition of new or changed services process and the change management process.

Where possible, releases should use standardized or consistent methods to ensure the integrity of CIs. Releases can be achieved more cost effectively by seeking efficiencies of scale through the use of standard methods and where feasible, using automation.

9.3.3 Explanation of requirements

9.3.3.1 Release policy

The service provider, in conjunction with the customer and interested parties, should develop and agree on a release policy to help to specify the frequency of releases and approach for each type of release. A release policy can typically include:

a) definition of each type of release including an emergency release, other examples are major, significant, minor;

b) the frequency of each type of release;

c) definition of key roles and responsibilities for all release and deployment management process activities;

d) authority levels for release acceptance and deployment approvals;

e) rules on verification and acceptance of releases;

f) identification schemes for releases;

g) rules for versioning of releases;

h) build and packaging of releases;

i) release and deployment approach for each type of release including automated deployment methods and tools where applicable;

j) a predefined and consistent testing approach.

9.3.3.2 Release and deployment planning

The release and deployment management process should plan the release and deployment of a new or changed service into the live environment with the customer and interested parties. Project management methods and techniques should be used to support release and deployment planning. The minimum information for release and deployment plans should be defined by the service provider and may differ according to the type of release.

The release and deployment plans should always ensure that all changes are coordinated with the change management process. Release and deployment planning should include an assessment of the impact of the release, associated risks and the identification of any mitigation measures that would be employed to minimize any unacceptable risks.

Typical factors that should be considered when planning a release and its deployment are the volume of business, technical and other changes necessary to deploy a release. For example, new skills, new or changed processes and new tools. Other factors include dependencies and the time and resources needed to build, test and deploy a release.

Release and deployment plans should include the following components:

a) scope and content of the release including the deliverables;

b) services and service components to transfer, decommission or retire including licences;

c) timetable for the packaging and deployment of the release with dates determined in consultation with the customer for each nominated site;

d) roles and responsibilities for planning, coordinating, building, testing, deploying and reviewing the release;

e) the release and deployment procedures and methods that ensure the integrity of software, hardware and other service components during deployment;

f) plans for communication activities that provide the required information to users within the customer organization, the personnel within the service provider and any relevant suppliers;

g) the approach for identifying, tracking and managing any issues detected during the release;

h) test plans including items such as acceptance criteria, test method, scripts and result recording sheets;

i) approach to managing controlled test environments where appropriate, to ensure releases can be sufficiently tested prior to pilot, trial and or deployment;

j) approach to managing assets and CIs according to applicable policies and procedures e.g. asset management, configuration management, health and safety, environmental, information security management;

k) the criteria that the release and deployment should be verified against, along with any appropriate criteria and the approved approach to be used for reversing or remediation of failed releases;

l) references to or requirements defined in the plans for:

   1) release and deployment work instructions, regardless of the use of internal or external resources;
   2) tools that are required to effect the release, including the use of tools and techniques for remote or unattended installation of software;
   3) the implementation of standard changes that are approved for releases via the change management process;
   4) updating the configuration details of any service, service components and CIs affected by the release.

9.3.3.3 Release and deployment practices

Each release should contain a set of CIs. The release and deployment management process should work closely with the configuration management process to ensure that the CIs are correctly defined according to:

a) agreed CI types, e.g. a configuration management policy;

b) relationships with other CIs;

c) naming and versioning conventions;

d) technical hardware and environment builds;

e) software images;

f) work instructions.

This should ensure the integrity of the information about services and service components during deployment.

The contents of a release should ensure the suitability of the release for deployment. The contents of a release should define the assets and CIs to be procured and assembled as the release components. This may include master software licences that require procurement and subsequent storage in the software library. It may also include the procurement of hardware items that should be held in an identified hardware store.

Consistent work practices and defined procedures that have been proven through testing, pilots and trials should be used. Examples of such work practices and procedures include; release building, testing, release distribution, release installation, verification, and if necessary the reversal or remediation of the release.

The release and deployment management process should define the methods and practices to be employed for emergency releases in coordination with the interface to the emergency change management procedure.

9.3.3.4 Testing of releases

Testing activities should include:

a) creating a test plan;

b) creating test routines and preparing the test environment for the release;

c) test activities to be conducted in the test environment;

d) user acceptance testing;

e) recording of test results, including version, issues and time and date the issue is found;

f) production of a test report;

g) sign off for the release, providing it meets acceptance criteria and is fit for purpose.

9.3.3.5 Deployment activities and procedures

Deployment activities and procedures should include the following:

a) distributing and delivering the CIs supporting the service and service components at the correct location and time;

b) building, installing and configuring CIs with any converted or new data and information;

c) verifying that the services and service components have been tested according to the acceptance tests and producing the installation and test reports;

d) updating records for the new release and any CIs or services removed during the changeover;

e) recording any incidents, problems, known errors, unexpected events or deviations from the plans;

f) implementing corrective actions during the deployment;

g) reversing or taking remedial action to correct an unsuccessful release.

9.3.4 Documents and records

The documents and records that should be produced and retained by the release and deployment management process include:

a) release policy;

b) release plan;

c) contents of each release including related changes approved by the change management process;

d) contents of each release including new components, altered components resulting from the release and deployment activities, retired components being recovered or made obsolete during deployment;

e) release design, release notes, and installation guides for the release;

f) deployment plan, which may be in the form of a project plan;

g) a schedule of releases and deployments that indicates any periods when releases cannot be scheduled due to elevated risk to the customer in that period, e.g. end of financial year;

h) user impact assessment and business change impact assessment;

i) communications plan;

j) training plan covering users, service provider personnel and interested parties;

k) release and deployment test plans and test results;

l) release acceptance and customer sign off;

m) records of success and failure along with follow-up action lists or incident logs;

n) incident, problem and known error records for any release failures, reversals or remediation work;

o) CI information for each release:
   1) release identifier and version;
   2) description of the release;
   3) relationship between the release and its constituent CIs;
   4) location of the release package and installation;
   5) associated requests for change;
   6) associated incidents, problems and known errors, including those that were corrected by the release.

9.3.5 Authorities and responsibilities

In addition to the process owner, process manager and personnel performing the procedures of the process as described in Clause 4.4.2.1, authorities and responsibilities required within the release and deployment management process should include:

a) the customer or customer's representative, responsible for planning and coordinating releases and deployment with business change activities;

b) the user, responsible for operating the new or changed service or service component and performing user testing where applicable;

c) service provider personnel, responsible for testing the operating activities for the new or changed service or service component.

Annex A
(informative)

Interfaces between processes and integration of processes with SMS

The listed examples in all tables in this Annex are not exhaustive.

Table A.1 — Interfaces and integration for design and transition of new or changed services

Example interfaces between design and transition of new or changed services and the rest of the SMS include:
SLM process should provide service level requirements of the new or changes service.
BRM process should provide all customer and business requirements of the new or changed service, to ensure that they are identified, documented, agreed and delivered.
Incident and service request management process should provide details of the impact of the introduction of the new or changed services after the transition into the live environment.
Release and deployment management process should provide advice on the timing and method of deployment.
Budgeting and accounting for service process should receive a change of services provision cost estimates report.
Change management process should receive requests for change being introduced by the introduction of the new or changed service.
Examples of integration between design and transition of new or changed services and the rest of the SMS include:
Design and transition of new or changed services should receive the audit nonconformity record as an input to identify potential requirements for new or changed services.
Design and transition of new or changed services should receive the customer satisfaction analysis report as an input to identify potential requirements for new or changed services to address customer satisfaction.

Table A.2 — Interfaces and integration for SLM

Example interfaces between SLM and the rest of the SMS include:
Service continuity and availability management process should provide continuity or availability requirements, as input to the SLA, and reduce SLA breaches due to discontinuity or unavailability.
Capacity management process should provide performance requirements as input to the SLA to reduce SLA breaches due to poor performance.
Supplier management process should provide details of contracts with suppliers, so that supplier's contractual targets align with SLAs.
ISM process should provide the information security policy so that SLAs are developed to align with the security policy.
Incident and service request management process should provide relevant data about incidents.
Incident and service request management process should receive SLA, so that incidents and requests are prioritized and resolved or fulfilled in line with agreed timeframes for response and resolution.
Change management process should receive requests for change to SLAs, and identify projected service outages detailing planned variations from SLAs.
Examples of integration between SLM and the rest of the SMS include:
SLM process should maintain the agreed definition of service between top management, the customer , users and the service level manager.
SLM process should define the service provider's skills and resources required to deliver the service.
SLM process should interact with suppliers of services which underpin the service resolver groups such as level 2 and level 3 support, and fulfilment for service request provisioning.

Table A.3 — Interfaces and integration for service reporting

Example interfaces between service reporting and the rest of the SMS include:
SLM process should provide information corresponding to SLAs to define the appropriate policies and rules regarding service reporting.
Incident and service request management process should provide relevant data about incidents to service reporting, so that all interested parties can understand the impact and take agreed actions.
Service continuity and availability management process should provide service and component availability information.
Capacity management process should provide workload reporting information, including against pre-defined thresholds.
BRM process should receive the right level of information, to enable the delivery of optimum levels of service and improved customer satisfaction.
Examples of integration between service reporting and the rest of the SMS include:
Service reporting process should provide reports to interested parties regarding the quality, costs and risks of services, to enable the making of decisions and taking actions related to the service.
Service reporting process should receive data from every service management process to enable the communication and visibility required to manage and improve the SMS.

Table A.4 — Interfaces and integration for service continuity and availability management

Example interfaces between service continuity and availability management and the rest of the SMS include:
SLM process should provide: - service continuity and availability obligations in SLAs; - service levels that would be acceptable to the business in the event of a disaster; - assistance to determine availability targets and the investigation and resolution of service and component breaches.
Capacity management process should provide: - capacity plan, to enable alignment with the availability plan; - modelling information, so that there can be sufficient resources, e.g. data storage to enable recovery following a disaster and with the provision of resilience and spare capacity.
ISM process should provide definition of when an information security incident could be considered a disaster.
Configuration management process should provide information about the components that make up the infrastructure, to enable all of the service continuity and availability management process activities, as well as the maintenance of plans and recovery facilities.
Change management process should provide: information about all changes with potential impact on service continuity and availability plans.
SLM process should receive recovery requirements and options, so that they can be agreed and documented in the SLAs.
Incident and service request management and problem management processes should receive clear agreed and documented criteria for the invocation of the service continuity and availability plans.
Examples of integration between service continuity and availability management and the rest of the SMS
Service continuity and availability management process should receive information about business plans from the customer and interested parties, to identify new or changed requirements for service continuity or availability.
Service continuity and availability management process should provide business impact analysis, to top management and all interested parties to ensure that service management decisions are based upon a clear understanding of impact to the business due to a lack of availability.

Table A.5 — Interfaces and integration for budgeting and accounting for services

Example interfaces between budgeting and accounting for services and the rest of the SMS include:
Design and transition of new or changed services process should provide new or changed services plans including budgets and time scales.
SLM process should provide the catalogue of services as the basis for building cost models for services provided by the service provider.
Capacity management process should provide capacity plan, including costed options for meeting business requirements.
Supplier management process should provide details of changes to costs, both short term and over the life of a contract.
Configuration management process should provide details of all configuration items.
Capacity management process should receive budget for service and infrastructure upgrades or the purchase of new components.
Change management process should receive financial approval, where required.
Examples of integration between budgeting and accounting for services and the rest of the SMS include:
Budgeting and accounting for services process should receive sufficient information from the service provider's financial management organization, to enable reliable forecasting and apportionment of costs.
Budgeting and accounting for services process should provide the budgeting and accounting for services policy to the organization, to enable alignment with the financial management policy, as well as to regulatory requirements.
Financial resources should be budgeted at a level of detail suitable to manage the implementation, operation and improvements to the SMS, which will require the coordination of the budgeting and accounting for services process and financial management.

Table A.6 — Interfaces and integration for capacity management

Example interfaces between capacity management and the rest of the SMS include:
SLM process should provide SLA's and the required service levels, in addition to the capacity management targets.
Budgeting and accounting services should provide information about efficiency gains in the provision of services resulting in lower capacity costs or better utilization of capacity resources.
Incident and service request management process should provide information about incidents related to capacity and performance.
Configuration management process should provide technical, service, utilisation, financial and business data regarding CIs maintained in the CMDB.
SLM process should receive regular reports, to ensure that performance and capacity targets for new or changed requirements can be achieved. Performance is dependent on a given workload; therefore both are required in an SLA with specific performance targets. Similarly there can be a requirement for the capacity management process to assist the SLM process in drafting and reviewing operational level agreements and external contracts where capacity or performance issues are involved.
Service continuity and availability management process should receive modelling data, to determine the capacity required for all recovery options used. The minimum hardware and software configurations required are defined to provide the required performance and throughput levels following an invocation.
Problem management process should receive specialist expertise, to aid in identifying, diagnosing and resolving capacity related problems.
Change management process should receive information from the capacity management process regarding the cumulative effect of changes upon capacity. Capacity management process is also represented on the change advisory board, to assess the impact of changes on existing capacity and to identify changes in capacity requirements.
Release and deployment management process should receive information to aid in determining the distribution policy for releases, particularly where the network is used for distribution. Factors such as network bandwidth, host and target capacity, distribution window and number of targets should be considered as part of the distribution policy for the release.
Examples of integration between capacity management and the rest of the SMS include:
Capacity management process should receive the results of audits identifying non-conformities and opportunities for improvement.
Capacity management process should provide requirements for competence, awareness and training to ensure that the service provider has sufficient skills and skills levels to support the capacity management process.

Table A.7 — Interfaces and integration for ISM

Example interfaces between ISM and the rest of the SMS include:
Budgeting and accounting services process should provide information about the costs associated with security controls.
Capacity management process should provide the capacity impact of security controls (security controls often impact the performance of services).
Supplier management process should provide reports measuring whether suppliers are adhering to and maintaining the information security policy.
Incident and service request management process should provide details of all information security incidents, to meet the requirements of the information security policy and prevent repetition.
Problem management process should provide the root cause of identified information security incidents to ISM.
Configuration management process should provide details of configuration items held in the CMDB associated with high security risk and provide information in the CMDB which can determine the impact of information security problems and resolutions.
Change management process should provide details of information security resolutions and temporary fixes.
SLM process should receive information security requirements to be included in SLAs.
Service continuity and availability management process should receive details of information security incidents, problems and resolutions to ensure the continuity and availability of services.
BRM process should receive alerts about information security threats.
Incident and service request management process should receive guidance on how to deal with information security incidents.
Examples of integration between ISM and the rest of the SMS include:
ISM process should provide the information security policy to documentation management to ensure that all information is protected and controlled in alignment with the business value, regulatory requirements and required levels of confidentiality, integrity and availability.
ISM process should provide the information security policy to risk management to ensure that security risks to services are assessed and managed.

Table A.8 — Interfaces and integration for BRM

Example interfaces between BRM and the rest of the SMS include:
SLM process should provide SLAs or contracts, including service scope.
Service reporting process should provide service reports including identified needs and customer requirements.
Service continuity and availability management process should provide details of the service continuity plans.
ISM process should provide alerts of threats which may affect the customer relationship.
Incident and service request management process should provide details of formal complaints and compliments from the customer.
Change management process should receive any remediation and improvement actions arising out of customer complaints and customer satisfaction surveys.
Examples of integration between BRM and the rest of the SMS include:
BRM process should provide these results to the customer, leading to improved communication and customer satisfaction.
Customer complaints and customer satisfaction surveys should provide an input into reviews of the SMS.

Table A.9 — Interfaces and integration for supplier management

Example interfaces between supplier management and the rest of the SMS include:
SLM process should provide targets, requirements and responsibilities, ensuring their inclusion in underpinning agreements and contracts, so that these targets support service requirements, including those specified in SLAs.
Service continuity and availability management process should provide continuity and availability requirements for services being supplied by other parties.
Budgeting and accounting services should provide adequate funds to finance supplier management requirements and contracts and to provide advice and guidance on purchase and procurement matters.
ISM process should provide the policies and procedures regarding suppliers' access to services and systems, and their responsibilities with regard to conformance to ISM policies and requirements.
Examples of integration between supplier management and the rest of the SMS include:
Supplier management process should receive supplier performance data and measure this against available alternatives to negotiate the best value for money to support customer requirements and the business plan.
Supplier management process should provide requirements for supplier competence, awareness and training and supplier training evaluation results to ensure that the supplier is continually aligned with the business capability requirements.
Changes to the contract, documented agreement or other documents agreed by the interested parties, including changes to service commitments, should be managed by the change management process.
The change management process should ensure as required that suppliers comply with the change management practices of the organization and that suppliers are included during review, assessment and authorization of proposed changes which will impact supplier provided services.

Table A.10 — Interfaces and integration for incident and service request management

Example interfaces between incident and service request management and the rest of the SMS include:
SLM process should provide agreed incident and service request targets.
Problem management process should provide known error records and details of temporary fixes to minimize impact of incidents.
Configuration management process should provide information regarding CIs impacted by incidents or service requests to the incident and service request management process, to enable more accurate impact assessments.
Service continuity and availability management process should receive details of incidents and major incidents which are having a high impact on availability or continuity of service.
Capacity management process should receive details of incidents and major incidents which are related to capacity shortages.
Problem management process should receive details of incident and service request records, for trend analysis.
Change management process should receive reporting on the impact of unsuccessful changes which have resulted in new incidents.
Examples of integration between incident and service request management and the rest of the SMS include:
Incident and service request management process requires specialized personnel competencies for different roles. These service management competency requirements should be clearly defined. Where there is a shortfall or other deficiency in the individual being considered for or already in the role, the service provider should ensure that this shortfall is corrected.
Incident records and service requests should be reviewed to identify opportunities for process improvement and cost savings.

Table A.11 — Interfaces and integration for problem management

Example interfaces between problem management and the rest of the SMS include:
SLM process should provide SLAs and agreements including agreed problem management targets.
Service continuity and availability management process should provide details of problems which are having high impact on availability or continuity of service.
Capacity management process should provide any trends in capacity.
Incident and service request management process should provide: - details on incidents for which there is an unknown root cause to problem management; - incident data for proactive problem management such as trend analysis.
Configuration management process should provide information regarding the relationships between CIs which can aid in determining the impact of problems and resolutions.
Incident and service request management process should receive: - details of known errors for new or changed services being introduced into the live environment; - known error records and details of temporary fixes in order to minimize impact of incidents.
Change management process should receive requests for change to implement permanent solutions to known errors.
Examples of integration between problem management and the rest of the SMS include:
Problem management process should receive information related to problems with the SMS.
Problem management process should identify the root cause of the problems with the SMS and resolve them through the change management process.
The known error database should adhere to the documentation management policies and procedures.

Table A.12 — Interfaces and integration for configuration management

Example interfaces between configuration management and the rest of the SMS include:
Configuration management process should provide information regarding the relationships between CIs that can aid in analyzing the impact and root cause of problems.
Configuration management should provide information regarding which CIs will be impacted by proposed changes.
Configuration management should provide information about CIs that support services listed in the service catalogue.
Design and transition of new or changed services process should provide details of all plans and designs for new or changed services so that impact on existing CIs and services can be assessed by interested parties.
Incident and service request management process should provide details of all incidents and service requests related to CIs.
Problem management process should provide link between known errors and temporary fixes and the affected configuration items.
Change management process should provide details of changes to the CIs, and the authorization to reflect those changes in the CMDB.
Release and deployment management process should provide configuration baselines of release items and the target environment before and after releases.
All processes should receive up-to-date and accurate information about all CIs within the scope of the process.
Budgeting and accounting for services process should receive details of any asset, including licences, used to provide the services.
Examples of integration between configuration management and the rest of the SMS include:
Top management is responsible for ensuring that all assets, including licences, used to deliver services are managed according to statutory and regulatory requirements, and contractual obligations. Configuration management is a primary means by which this requirement is achieved.
The configuration management process does not include financial asset accounting but should include the interface to the financial asset accounting process.

Table A.13 — Interfaces and integration for change management

Example interfaces between change management and the rest of the SMS include:
Service continuity and availability management process should provide: - requests for change, to update service continuity procedures and plans, this will ensure that service continuity procedures and plans remain accurate, up-to-date and that interested parties are kept aware of changes; - potential impact of a proposed change on the availability of a service or component to change management.
Capacity management process should provide assessment of proposed changes, including not only the individual change impact but also total impact of changes on service capacity and resource or component capacity.
ISM process should provide assessment of potential impact of proposed changes on the information security policy and controls.
Incident and service request management process should provide information on incidents associated with implemented changes.
Problem management process should provide information on problems associated with implemented changes.
Configuration management process should provide reliable, quick and easy access to accurate configuration information, to enable interested parties and personnel to assess the impact of proposed changes.
Release and deployment management process should receive information about approved changes which will be implemented through release management.
Examples of integration between change management and the rest of the SMS include :
All changes to the SMS should go through the change management process.
Change management process should provide details of all changes to the SMS, catalogue of services, services, policies, objectives and plans, business requirements, service requirements and supplier requirements.
The scope of the SMS has implications for the time and cost of improvements and other changes, which has implications for the change management process.

Table A.14 — Interfaces and integration for release and deployment management

Example interfaces between release and deployment management and the rest of the SMS include:
Service continuity and availability management process should provide the assessment of any technical designs to ensure that services continue to meet availability targets particularly when overall capacity can increase. Early review and update of the continuity management plan should include any significant new release. Scheduling of suitable continuity reviews and tests should be carried out prior to release deployment.
Capacity management process should provide information and support regarding the purchase and installation of incremental capacity to support the release. This may include the reservation of capacity for development and test environments.
ISM process should provide an updated security plan in line with the adoption of new policies, practices and tools that result from the release.
Supplier management process should provide the required contracts and agreements that are in place or are updated prior to procurement and support of the technical components within a release. This caters for the release being in production.
Change management process should provide the approved request for change to release and deployment management.
SLM process should receive updates regarding any changes to service or service level documentation and key contacts.
Problem management process should receive notice and records of any defects and corresponding temporary fixes that will be promoted to the live environment with the release.
Configuration management process should receive information reflecting changes to the live environment following the release. This information will ensure the accuracy of the CMDB. Additional release information relevant to the CMDB will include updates to modified or decommissioned CIs and new services that supersede legacy services.
Examples of integration between release and deployment management and the rest of the SMS include:
Release and deployment management process should take into account any training, recruitment or early life support required as part of the release.
Top management should ensure the quantity and skills of personnel resources acquired or used by the service provider are sufficient to build, test and deploy the release, as well as to support and operate the new release once in production.

Bibliography

[1] ISO/IEC TR 20000-3, *Information technology — Service management — Part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1*

[2] ISO/IEC TR 20000-4, *Information technology — Service management — Part 4: Process reference model*

[3] ISO/IEC TR 20000-5, *Information technology — Service management — Part 5: Exemplar implementation plan for ISO/IEC 20000-1*

[4] ISO 9000, *Quality management systems — Fundamentals and vocabulary*

[5] ISO 9001, *Quality management systems — Requirements*

[6] ISO 9004, *Managing for the sustained success of an organization — A quality management approach*

[7] ISO/IEC TR 9126-2, *Software engineering — Product quality — Part 2: External metrics*

[8] ISO/IEC TR 9126-3, *Software engineering — Product quality — Part 3: Internal metrics*

[9] ISO 10002, *Quality management — Customer satisfaction — Guidelines for complaints handling in organizations*

[10] ISO 10007, *Quality management systems — Guidelines for configuration management*

[11] ISO/IEC 12207, *Systems and software engineering — Software life cycle processes*

[12] ISO/IEC 14598 (all parts), *Software engineering — Product evaluation*

[13] ISO/IEC 15288, *Systems and software engineering — System life cycle processes*

[14] ISO/IEC 15504-1, *Information technology — Process assessment — Part 1: Concepts and vocabulary*

[15] ISO/IEC 15504-2, *Information technology — Process assessment — Part 2: Performing an assessment*

[16] ISO/IEC 15504-3, *Information technology — Process assessment — Part 3: Guidance on performing an assessment*

[17] ISO/IEC 15504-4, *Information technology — Process assessment — Part 4: Guidance on use for process improvement and process capability determination*

[18] ISO/IEC 15504-5, *Information technology — Process assessment — Part 5: An exemplar Process Assessment Model*

[19] ISO/IEC 15939, *Systems and software engineering — Measurement process*

[20] ISO 19011, *Guidelines for quality and/or environmental management systems auditing*

[21] ISO/IEC 19770-1, *Information technology — Software asset management — Processes*

[22] ISO/IEC TR 24748-2, *Systems and software engineering — Life cycle management — Part 2: Guide to the application of ISO/IEC 15288 (System life cycle processes)*

[23] ISO/IEC TR 24748-3, *Systems and software engineering — Life cycle management — Part 3: Guide to the application of ISO/IEC 12207 (Software life cycle processes)*

[24] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[25] ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security management*

[26] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

[27] ISO 31000, *Risk management — Principles and guidelines*

[28] ISO/IEC 38500, *Corporate governance of information technology*

[29] ISO/IEC 90003, *Software engineering — Guidelines for the application of ISO 9001:2000 to computer software*

ICS 03.080.99; 35.020

Price based on 85 pages

This page deliberately left blank

British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards and other standards-related publications, information and services. It presents the UK view on standards in Europe and at the international level.

BSI is incorporated by Royal Charter. British Standards and other standardisation products are published by BSI Standards Limited.

Revisions

British Standards and PASs are periodically updated by amendment or revision. Users of British Standards and PASs should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using British Standards would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover. Similary for PASs, please notify BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001

BSI offers BSI Subscribing Members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of British Standards and PASs.

Tel: +44 (0)20 8996 7669 Fax: +44 (0)20 8996 7001
Email: plus@bsigroup.com

Buying standards

You may buy PDF and hard copy versions of standards directly using a credit card from the BSI Shop on the website **www.bsigroup.com/shop.** In addition all orders for BSI, international and foreign standards publications can be addressed to BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001
Email: orders@bsigroup.com

In response to orders for international standards, BSI will supply the British Standard implementation of the relevant international standard, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Knowledge Centre.

Tel: +44 (0)20 8996 7004 Fax: +44 (0)20 8996 7005
Email: knowledgecentre@bsigroup.com

BSI Subscribing Members are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

Tel: +44 (0)20 8996 7002 Fax: +44 (0)20 8996 7001
Email: membership@bsigroup.com

Information regarding online access to British Standards and PASs via British Standards Online can be found at **www.bsigroup.com/BSOL**

Further information about British Standards is available on the BSI website at **www.bsi-group.com/standards**

Copyright

BSI

389 Chiswick High Road London W4 4AL UK

Tel +44 (0)20 8996 9001
Fax +44 (0)20 8996 7001
www.bsigroup.com/standards

raising standards worldwide™