INTERNATIONAL STANDARD

ISO/IEC 20000-1

Second edition
2011-04-15

Information technology — Service management —

Part 1: Service management system requirements

Technologies de l'information — Gestion des services —

Partie 1: Exigences du système de gestion des services

Reference number
ISO/IEC 20000-1:2011(E)

COPYRIGHT PROTECTED DOCUMENT

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

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 20000-1 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 20000-1:2005), which has been technically revised. The main differences are as follows:

— closer alignment to ISO 9001;

— closer alignment to ISO/IEC 27001;

— change of terminology to reflect international usage;

— addition of many more definitions, updates to some definitions and removal of two definitions;

— introduction of the term “service management system”;

— combining Clauses 3 and 4 of ISO/IEC 20000-1:2005 to put all management system requirements into one clause;

— clarification of the requirements for the governance of processes operated by other parties;

— clarification of the requirements for defining the scope of the SMS;

— clarification that the PDCA methodology applies to the SMS, including the service management processes, and the services;

— introduction of new requirements for 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*[1)]

1) To be published. (Technical revision of ISO/IEC 20000-2:2005.)

— *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]

A process assessment model for service management will form the subject of a future Part 8.

Introduction

The requirements in this part of ISO/IEC 20000 include the design, transition, delivery and improvement of services that fulfil service requirements and provide value for both the customer and the service provider. This part of ISO/IEC 20000 requires an integrated process approach when the service provider plans, establishes, implements, operates, monitors, reviews, maintains and improves a service management system (SMS).

Co-ordinated integration and implementation of an SMS provides ongoing control and opportunities for continual improvement, greater effectiveness and efficiency. The operation of processes as specified in this part of ISO/IEC 20000 requires personnel to be well organized and co-ordinated. Appropriate tools can be used to enable the processes to be effective and efficient.

The most effective service providers consider the impact on the SMS through all stages of the service lifecycle, from strategy through design, transition and operation, including continual improvement.

This part of ISO/IEC 20000 requires the application of the methodology known as “Plan-Do-Check-Act” (PDCA) to all parts of the SMS and the services. The PDCA methodology, as applied in this part of ISO/IEC 20000, can be briefly described as follows.

Plan: establishing, documenting and agreeing the SMS. The SMS includes the policies, objectives, plans and processes to fulfil the service requirements.

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 policies, objectives, plans and service requirements and reporting the results.

Act: taking actions to continually improve performance of the SMS 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.

Figure 1 illustrates how the PDCA methodology can be applied to the SMS, including the service management processes specified in Clauses 5 to 9, and the services. Each element of the PDCA methodology is a vital part of a successful implementation of an SMS. The improvement process used in this part of ISO/IEC 20000 is based on the PDCA methodology.

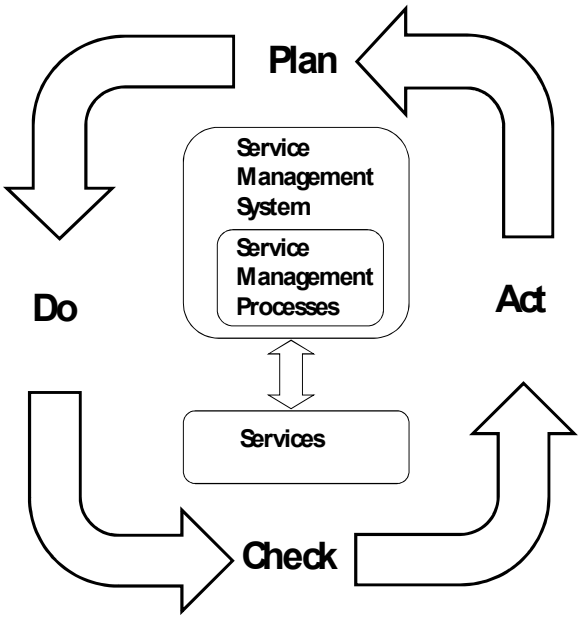

Figure 1 — PDCA methodology applied to service management

This part of ISO/IEC 20000 enables a service provider to integrate its SMS with other management systems in the service provider's organization. The adoption of an integrated process approach and the PDCA methodology enables the service provider to align or fully integrate multiple management system standards. For example, an SMS can be integrated with a quality management system based on ISO 9001 or an information security management system based on ISO/IEC 27001.

ISO/IEC 20000 is intentionally independent of specific guidance. The service provider can use a combination of generally accepted guidance and its own experience.

Users of an International Standard are responsible for its correct application. An International Standard does not purport to include all necessary statutory and regulatory requirements and contractual obligations of the service provider. Conformity to an International Standard does not of itself confer immunity from statutory and regulatory requirements.

For the purposes of research on service management standards, users are encouraged to share their views on ISO/IEC 20000-1 and their priorities for changes to the rest of the ISO/IEC 20000 series. Click on the link below to take part in the online survey.

ISO/IEC 20000-1 online survey

Information technology — Service management —

Part 1:
Service management system requirements

1 Scope

1.1 General

This part of ISO/IEC 20000 is a service management system (SMS) standard. It specifies requirements for the service provider to plan, establish, implement, operate, monitor, review, maintain and improve an SMS. The requirements include the design, transition, delivery and improvement of services to fulfil service requirements. This part of 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 its service providers, including those in a supply chain;

c) a 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 and delivery of services through effective implementation and operation of an SMS;

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

Figure 2 illustrates an SMS, including the service management processes. The service management processes and the relationships between the processes can be implemented in different ways by different service providers. The nature of the relationship between a service provider and the customer will influence how the service management processes are implemented.

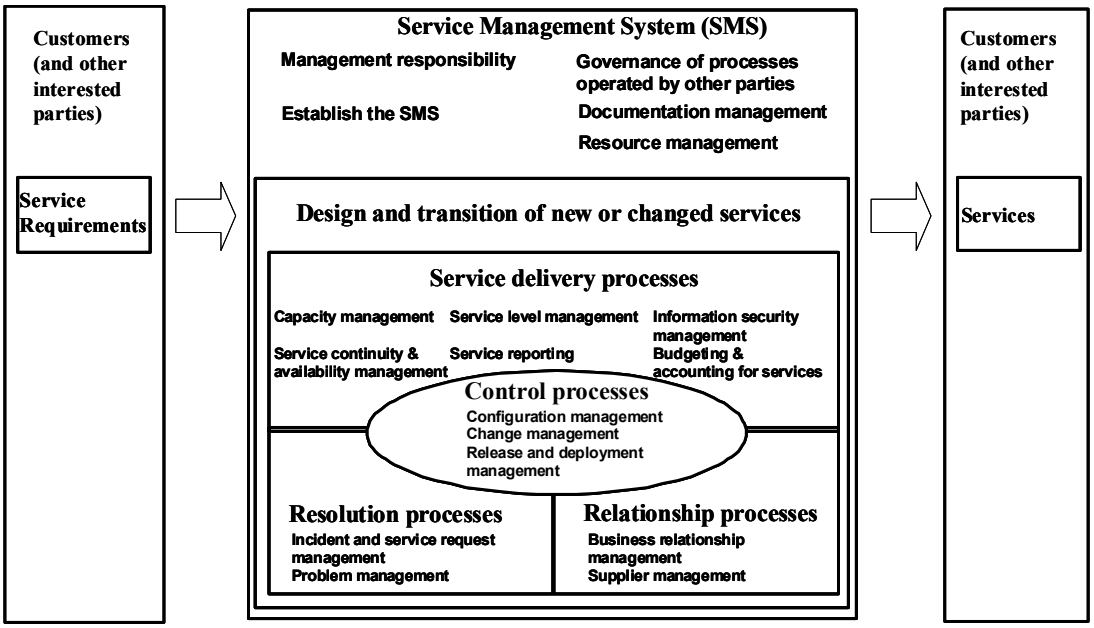

Figure 2 — Service management system

1.2 Application

All requirements in this part of ISO/IEC 20000 are generic and are intended to be applicable to all service providers, regardless of type, size and the nature of the services delivered. Exclusion of any of the requirements in Clauses 4 to 9 is not acceptable when a service provider claims conformity to this part of ISO/IEC 20000, irrespective of the nature of the service provider's organization.

Conformity to the requirements in Clause 4 can only be demonstrated by a service provider showing evidence of fulfilling all of the requirements in Clause 4. A service provider cannot rely on evidence of the governance of processes operated by other parties for the requirements in Clause 4.

Conformity to the requirements in Clauses 5 to 9 can be demonstrated by the service provider showing evidence of fulfilling all requirements. Alternatively, the service provider can show evidence of fulfilling the majority of the requirements themselves and evidence of the governance of processes operated by other parties for those processes, or parts of processes, that the service provider does not operate directly.

The scope of this part of ISO/IEC 20000 excludes the specification for a product or tool. However, organizations can use this part of ISO/IEC 20000 to help them develop products or tools that support the operation of an SMS.

NOTE ISO/IEC TR 20000-3 provides guidance on scope definition and applicability of this part of ISO/IEC 20000. This includes further explanation about the governance of processes operated by other parties.

2 Normative references

The following referenced 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.

No normative references are cited. This clause is included in order to ensure clause numbering is identical with ISO/IEC 20000-2:—, *Information technology — Service management — Part 2: Guidance on the application of service management systems*[2)].

2) To be published.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
availability
ability of a service or service component to perform its required function at an agreed instant or over an agreed period of time

NOTE Availability is normally expressed as a ratio or percentage of the time that the service or service component is actually available for use by the customer to the agreed time that the service should be available.

3.2
configuration baseline
configuration information formally designated at a specific time during a service or service component's life

NOTE 1 Configuration baselines, plus approved changes from those baselines, constitute the current configuration information.

NOTE 2 Adapted from ISO/IEC/IEEE 24765:2010.

3.3
configuration item
CI
element that needs to be controlled in order to deliver a service or services

3.4
configuration management database
CMDB
data store used to record attributes of configuration items, and the relationships between configuration items, throughout their lifecycle

3.5
continual improvement
recurring activity to increase the ability to fulfil service requirements

NOTE Adapted from ISO 9000:2005.

3.6
corrective action
action to eliminate the cause or reduce the likelihood of recurrence of a detected nonconformity or other undesirable situation

NOTE Adapted from ISO 9000:2005.

3.7
customer
organization or part of an organization that receives a service or services

NOTE 1 A customer can be internal or external to the service provider's organization.

NOTE 2 Adapted from ISO 9000:2005.

3.8
document
information and its supporting medium

[ISO 9000:2005]

EXAMPLES Policies, plans, process descriptions, procedures, service level agreements, contracts or records.

NOTE 1 The documentation can be in any form or type of medium.

NOTE 2 In ISO/IEC 20000, documents, except for records, state the intent to be achieved.

3.9
effectiveness
extent to which planned activities are realized and planned results achieved

[ISO 9000:2005]

3.10
incident
unplanned interruption to a service, a reduction in the quality of a service or an event that has not yet impacted the service to the customer

3.11
information security
preservation of confidentiality, integrity and accessibility of information

NOTE 1 In addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.

NOTE 2 The term “availability” has not been used in this definition because it is a defined term in this part of ISO/IEC 20000 which would not be appropriate for this definition.

NOTE 3 Adapted from ISO/IEC 27000:2009.

3.12
information security incident
single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

[ISO/IEC 27000:2009]

3.13
interested party
person or group having a specific interest in the performance or success of the service provider's activity or activities

EXAMPLES Customers, owners, management, people in the service provider's organization, suppliers, bankers, unions or partners.

NOTE 1 A group can comprise an organization, a part thereof, or more than one organization.

NOTE 2 Adapted from ISO 9000:2005.

3.14
internal group
part of the service provider's organization that enters into a documented agreement with the service provider to contribute to the design, transition, delivery and improvement of a service or services

NOTE The internal group is outside the scope of the service provider's SMS.

3.15
known error
problem that has an identified root cause or a method of reducing or eliminating its impact on a service by working around it

3.16
nonconformity
non-fulfilment of a requirement

[ISO 9000:2005]

3.17
organization
group of people and facilities with an arrangement of responsibilities, authorities and relationships

EXAMPLES Company, corporation, firm, enterprise, institution, charity, sole trader, association, or parts or combination thereof.

NOTE 1 The arrangement is generally orderly.

NOTE 2 An organization can be public or private.

[ISO 9000:2005]

3.18
preventive action
action to avoid or eliminate the causes or reduce the likelihood of occurrence of a potential nonconformity or other potential undesirable situation

NOTE Adapted from ISO 9000:2005.

3.19
problem
root cause of one or more incidents

NOTE The root cause is not usually known at the time a problem record is created and the problem management process is responsible for further investigation.

3.20
procedure
specified way to carry out an activity or a process

[ISO 9000:2005]

NOTE Procedures can be documented or not.

3.21
process
set of interrelated or interacting activities which transforms inputs into outputs

[ISO 9000:2005]

3.22
record
document stating results achieved or providing evidence of activities performed

[ISO 9000:2005]

EXAMPLES Audit reports, incident reports, training records or minutes of meetings.

3.23
release
collection of one or more new or changed configuration items deployed into the live environment as a result of one or more changes

3.24
request for change
proposal for a change to be made to a service, service component or the service management system

NOTE A change to a service includes the provision of a new service or the removal of a service which is no longer required.

3.25
risk
effect of uncertainty on objectives

NOTE 1 An effect is a deviation from the expected — positive and/or negative.

NOTE 2 Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).

NOTE 3 Risk is often characterized by reference to potential events and consequences, or a combination of these.

NOTE 4 Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.

[ISO 31000:2009]

3.26
service
means of delivering value for the customer by facilitating results the customer wants to achieve

NOTE 1 Service is generally intangible.

NOTE 2 A service can also be delivered to the service provider by a supplier, an internal group or a customer acting as a supplier.

3.27
service component
single unit of a service that when combined with other units will deliver a complete service

EXAMPLES Hardware, software, tools, applications, documentation, information, processes or supporting services.

NOTE A service component can consist of one or more configuration items.

3.28
service continuity
capability to manage risks and events that could have serious impact on a service or services in order to continually deliver services at agreed levels

3.29
service level agreement
SLA
documented agreement between the service provider and customer that identifies services and service targets

NOTE 1 A service level agreement can also be established between the service provider and a supplier, an internal group or a customer acting as a supplier.

NOTE 2 A service level agreement can be included in a contract or another type of documented agreement.

3.30
service management
set of capabilities and processes to direct and control the service provider's activities and resources for the design, transition, delivery and improvement of services to fulfil the service requirements

3.31
service management system
SMS
management system to direct and control the service management activities of the service provider

NOTE 1 A management system is a set of interrelated or interacting elements to establish policy and objectives and to achieve those objectives.

NOTE 2 The SMS includes all service management policies, objectives, plans, processes, documentation and resources required for the design, transition, delivery and improvement of services and to fulfil the requirements in this part of ISO/IEC 20000.

NOTE 3 Adapted from the definition of “quality management system” in ISO 9000:2005.

3.32
service provider
organization or part of an organization that manages and delivers a service or services to the customer

NOTE A customer can be internal or external to the service provider's organization.

3.33
service request
request for information, advice, access to a service or a pre-approved change

3.34
service requirement
needs of the customer and the users of the service, including service level requirements, and the needs of the service provider

3.35
supplier
organization or part of an organization that is external to the service provider's organization and enters into a contract with the service provider to contribute to the design, transition, delivery and improvement of a service or services or processes

NOTE Suppliers include designated lead suppliers but not their sub-contracted suppliers.

3.36
top management
person or group of people who direct and control the service provider at the highest level

NOTE Adapted from ISO 9000:2005.

3.37
transition
activities involved in moving a new or changed service to or from the live environment

4 Service management system general requirements

4.1 Management responsibility

4.1.1 Management commitment

Top management shall provide evidence of its commitment to planning, establishing, implementing, operating, monitoring, reviewing, maintaining, and improving the SMS and the services by:

a) establishing and communicating the scope, policy and objectives for service management;

b) ensuring that the service management plan is created, implemented and maintained in order to adhere to the policy, achieve the objectives for service management and fulfil the service requirements;

c) communicating the importance of fulfilling service requirements;

d) communicating the importance of fulfilling statutory and regulatory requirements and contractual obligations;

e) ensuring the provision of resources;

f) conducting management reviews at planned intervals;

g) ensuring that risks to services are assessed and managed.

4.1.2 Service management policy

Top management shall ensure that the service management policy:

a) is appropriate to the purpose of the service provider;

b) includes a commitment to fulfil service requirements;

c) includes a commitment to continually improve the effectiveness of the SMS and the services through the policy on continual improvement in Clause 4.5.5.1;

d) provides a framework for establishing and reviewing service management objectives;

e) is communicated and understood by the service provider's personnel;

f) is reviewed for continuing suitability.

4.1.3 Authority, responsibility and communication

Top management shall ensure that:

a) service management authorities and responsibilities are defined and maintained;

b) documented procedures for communication are established and implemented.

4.1.4 Management representative

Top management shall appoint a member of the service provider's management who, irrespective of other responsibilities, has the authorities and responsibilities that include:

a) ensuring that activities are performed to identify, document and fulfil service requirements;

b) assigning authorities and responsibilities for ensuring that service management processes are designed, implemented and improved in accordance with the policy and objectives for service management;

c) ensuring that service management processes are integrated with the other components of the SMS;

d) ensuring that assets, including licences, used to deliver services are managed according to statutory and regulatory requirements and contractual obligations;

e) reporting to top management on the performance and opportunities for improvement to the SMS and the services.

4.2 Governance of processes operated by other parties

For the processes in Clauses 5 to 9, the service provider shall identify all processes, or parts of processes, which are operated by other parties. Other parties can be an internal group, a customer or a supplier. The service provider shall demonstrate governance of processes operated by other parties by:

a) demonstrating accountability for the processes and authority to require adherence to the processes;

b) controlling the definition of the processes, and interfaces to other processes;

c) determining process performance and compliance with process requirements;

d) controlling the planning and prioritizing of process improvements.

When a supplier is operating parts of the processes, the service provider shall manage the supplier through the supplier management process. When an internal group or a customer is operating parts of the processes, the service provider shall manage the internal group or the customer through the service level management process.

NOTE ISO/IEC TR 20000-3 provides guidance on scope definition and applicability of this part of ISO/IEC 20000. This includes further explanation about the governance of processes operated by other parties.

4.3 Documentation management

4.3.1 Establish and maintain documents

The service provider shall establish and maintain documents, including records, to ensure effective planning, operation and control of the SMS. These documents shall include:

a) documented policy and objectives for service management;

b) documented service management plan;

c) documented policies and plans created for specific processes as required by this part of ISO/IEC 20000;

d) documented catalogue of services;

e) documented SLAs;

f) documented service management processes;

g) documented procedures and records required by this part of ISO/IEC 20000;

h) additional documents, including those of external origin, determined by the service provider as necessary to ensure effective operation of the SMS and delivery of the services.

4.3.2 Control of documents

Documents required by the SMS shall be controlled. Records are a special type of document and shall be controlled according to the requirements given in Clause 4.3.3.

A documented procedure, including the authorities and responsibilities, shall be established to define the controls needed to:

a) create and approve documents prior to issue;

b) communicate to interested parties about new or changed documents;

c) review and maintain documents as necessary;

d) ensure that changes and the current revision status of documents are identified;

e) ensure that relevant versions of applicable documents are available at points of use;

f) ensure that documents are readily identifiable and legible;

g) ensure that documents of external origin are identified and their distribution controlled;

h) prevent the unintended use of obsolete documents and apply suitable identification to them if they are retained.

4.3.3 Control of records

Records shall be kept to demonstrate conformity to requirements and the effective operation of the SMS.

A documented procedure shall be established to define the controls needed for the identification, storage, protection, retrieval, retention and disposal of records. Records shall be legible, readily identifiable and retrievable.

4.4 Resource management

4.4.1 Provision of resources

The service provider shall determine and provide the human, technical, information and financial resources needed to:

a) establish, implement and maintain the SMS and the services, and continually improve their effectiveness;

b) enhance customer satisfaction by delivering services that fulfil service requirements.

4.4.2 Human resources

The service provider's personnel performing work affecting conformity to service requirements shall be competent on the basis of appropriate education, training, skills and experience. The service provider shall:

a) determine the necessary competence for personnel;

b) where applicable, provide training or take other actions to achieve the necessary competence;

c) evaluate the effectiveness of actions taken;

d) ensure that its personnel are aware of how they contribute to the achievement of service management objectives and the fulfilment of service requirements;

e) maintain appropriate records of education, training, skills and experience.

4.5 Establish and improve the SMS

4.5.1 Define scope

The service provider shall define and include the scope of the SMS in the service management plan. The scope shall be defined by the name of the organizational unit providing the services, and the services to be delivered.

The service provider shall also take into consideration other factors affecting the services to be delivered including:

a) geographical location(s) from which the service provider delivers the services;

b) the customer and their location(s);

c) technology used to provide the services.

NOTE ISO/IEC TR 20000-3 provides guidance on scope definition and applicability of this part of ISO/IEC 20000.

4.5.2 Plan the SMS (Plan)

The service provider shall create, implement and maintain a service management plan. Planning shall take into consideration the service management policy, service requirements and requirements in this part of ISO/IEC 20000. The service management plan shall contain or include a reference to at least the following:

a) service management objectives that are to be achieved by the service provider;

b) service requirements;

c) known limitations which can impact the SMS;

d) policies, standards, statutory and regulatory requirements and contractual obligations;

e) framework of authorities, responsibilities and process roles;

f) authorities and responsibilities for plans, service management processes and services;

g) human, technical, information and financial resources necessary to achieve the service management objectives;

h) approach to be taken for working with other parties involved in the design and transition of new or changed services process;

i) approach to be taken for the interfaces between service management processes and their integration with the other components of the SMS;

j) approach to be taken for the management of risks and the criteria for accepting risks;

k) technology used to support the SMS;

l) how the effectiveness of the SMS and the services will be measured, audited, reported and improved.

Plans created for specific processes shall be aligned with the service management plan. The service management plan and plans created for specific processes shall be reviewed at planned intervals and, if applicable, updated.

4.5.3 Implement and operate the SMS (Do)

The service provider shall implement and operate the SMS for the design, transition, delivery and improvement of services according to the service management plan, through activities including at least:

a) allocation and management of funds and budgets;

b) assignment of authorities, responsibilities and process roles;

c) management of human, technical and information resources;

d) identification, assessment and management of risks to the services;

e) management of service management processes;

f) monitoring and reporting on performance of service management activities.

4.5.4 Monitor and review the SMS (Check)

4.5.4.1 General

The service provider shall use suitable methods for monitoring and measuring the SMS and the services. These methods shall include internal audits and management reviews.

The objectives of all internal audits and management reviews shall be documented. The internal audits and management reviews shall demonstrate the ability of the SMS and the services to achieve service management objectives and fulfil service requirements. Nonconformities shall be identified against the requirements in this part of ISO/IEC 20000, the SMS requirements identified by the service provider or the service requirements.

The results of internal audits and management reviews, including nonconformities, concerns and actions identified, shall be recorded. The results and actions shall be communicated to interested parties.

4.5.4.2 Internal audit

The service provider shall conduct internal audits, at planned intervals, to determine whether the SMS and the services:

a) fulfil the requirements in this part of ISO/IEC 20000;

b) fulfil the service requirements and the SMS requirements identified by the service provider;

c) are effectively implemented and maintained.

There shall be a documented procedure including the authorities and responsibilities for planning and conducting audits, reporting results and maintaining audit records.

An audit programme shall be planned. This shall take into consideration the status and importance of the processes and areas to be audited, as well as the results of previous audits. The audit criteria, scope, frequency and methods shall be documented.

The selection of auditors and conduct of audits shall ensure objectivity and impartiality of the audit. Auditors shall not audit their own work.

Nonconformities shall be communicated, prioritized and responsibility allocated for actions. The management responsible for the area being audited shall ensure that any corrections and corrective actions are taken without undue delay to eliminate nonconformities and their causes. Follow-up activities shall include the verification of the actions taken and the reporting of results.

NOTE See ISO 19011 for guidance on management systems auditing.

4.5.4.3 Management review

Top management shall review the SMS and the services at planned intervals to ensure their continued suitability and effectiveness. This review shall include assessing opportunities for improvement and the need for changes to the SMS, including the policy and objectives for service management.

The input to management reviews shall include at least information on:

a) customer feedback;

b) service and process performance and conformity;

c) current and forecast human, technical, information and financial resource levels;

d) current and forecast human and technical capabilities;

e) risks;

f) results and follow-up actions from audits;

g) results and follow-up actions from previous management reviews;

h) status of preventive and corrective actions;

i) changes that could affect the SMS and the services;

j) opportunities for improvement.

Records of management reviews shall be maintained.

The records from the management review shall include at least decisions and actions related to resources, improvement of the effectiveness of the SMS and improvement of the services.

4.5.5 Maintain and improve the SMS (Act)

4.5.5.1 General

There shall be a policy on continual improvement of the SMS and the services. The policy shall include evaluation criteria for the opportunities for improvement.

There shall be a documented procedure including the authorities and responsibilities for identifying, documenting, evaluating, approving, prioritizing, managing, measuring and reporting of improvements. Opportunities for improvement, including corrective and preventive actions, shall be documented.

The cause of identified nonconformities shall be corrected. Corrective actions shall be taken to eliminate the cause of identified nonconformities in order to prevent recurrence. Preventive actions shall be taken in order to eliminate the cause of potential nonconformities in order to prevent occurrence.

NOTE For more information on corrective and preventive action, see ISO 9001:2008, Clause 8.5.

4.5.5.2 Management of improvements

Opportunities for improvement shall be prioritized. The service provider shall use the evaluation criteria in the policy on continual improvement, when making decisions on opportunities for improvement.

Approved improvements shall be planned.

The service provider shall manage improvement activities that include at least:

a) setting targets for improvements in one or more of quality, value, capability, cost, productivity, resource utilization and risk reduction;

b) ensuring that approved improvements are implemented;

c) revising the service management policies, plans, processes and procedures, where necessary;

d) measuring implemented improvements against the targets set and where targets are not achieved, taking necessary actions;

e) reporting on implemented improvements.

5 Design and transition of new or changed services

5.1 General

The service provider shall use this process for all new services and changes to services with the potential to have a major impact on services or the customer. The changes that are in the scope of Clause 5 shall be determined by the change management policy agreed as part of the change management process.

Assessment, approval, scheduling and reviewing of new or changed services in the scope of Clause 5 shall be controlled by the change management process. The CIs affected by new or changed services in the scope of Clause 5 shall be controlled by the configuration management process.

The service provider shall review outputs from the planning and design activities for new or changed services against the agreed service requirements and the relevant requirements given in Clauses 5.2 and 5.3. Based on the review, the service provider shall accept or reject the outputs. The service provider shall take necessary actions to ensure that the development and transition of the new or changed services can be performed effectively, using the accepted outputs.

NOTE The need for a new service or a change to a service can originate from the customer, the service provider, an internal group or a supplier in order to satisfy business needs or to improve the effectiveness of the services.

5.2 Plan new or changed services

The service provider shall identify the service requirements for the new or changed services. New or changed services shall be planned to fulfil the service requirements. Planning for the new or changed services shall be agreed with the customer and interested parties.

As input to planning, the service provider shall take into consideration the potential financial, organizational, and technical impact of delivering the new or changed services. The service provider shall also take into consideration the potential impact of the new or changed services on the SMS.

Planning for the new or changed services shall contain or include a reference to at least the following:

a) authorities and responsibilities for design, development and transition activities;

b) activities to be performed by the service provider and other parties including activities across interfaces from the service provider to other parties;

c) communication to interested parties;

d) human, technical, information and financial resources;

e) timescales for planned activities;

f) identification, assessment and management of risks;

g) dependencies on other services;

h) testing required for the new or changed services;

i) service acceptance criteria;

j) expected outcomes from delivering the new or changed services, expressed in measurable terms.

For services that are to be removed, the service provider shall plan for the removal of the service(s). Planning shall include the date(s) for the removal, archiving, disposal or transfer of data, documentation and service components. The service components can include infrastructure and applications with associated licences.

The service provider shall identify other parties who will contribute to the provision of service components for the new or changed services. The service provider shall evaluate their ability to fulfil the service requirements. The results of the evaluation shall be recorded and necessary actions taken.

5.3 Design and development of new or changed services

The new or changed services shall be designed and documented to include at least:

a) authorities and responsibilities for delivery of the new or changed services;

b) activities to be performed by the service provider, customer and other parties for delivery of the new or changed services;

c) new or changed human resource requirements, including requirements for appropriate education, training, skills and experience;

d) financial resource requirements for delivery of the new or changed services;

e) new or changed technology to support the delivery of the new or changed services;

f) new or changed plans and policies as required by this part of ISO/IEC 20000;

g) new or changed contracts and other documented agreements to align with changes in service requirements;

h) changes to the SMS;

i) new or changed SLAs;

j) updates to the catalogue of services;

k) procedures, measures and information to be used for the delivery of the new or changed services.

The service provider shall ensure that the design enables the new or changed services to fulfil the service requirements.

The new or changed services shall be developed in accordance with the documented design.

NOTE For further information about design, see the design and development process in ISO 9001:2008, Clause 7.3 or the architectural design process in ISO/IEC 15288:2008, Clause 6.4.3.

5.4 Transition of new or changed services

The new or changed services shall be tested to verify that they fulfil the service requirements and documented design. The new or changed services shall be verified against service acceptance criteria agreed in advance by the service provider and interested parties. If the service acceptance criteria are not met, the service provider and interested parties shall make a decision on necessary actions and deployment.

The release and deployment management process shall be used to deploy approved new or changed services into the live environment.

Following the completion of the transition activities, the service provider shall report to interested parties on the outcomes achieved against the expected outcomes.

6 Service delivery processes

6.1 Service level management

The service provider shall agree the services to be delivered with the customer.

The service provider shall agree a catalogue of services with the customer. The catalogue of services shall include the dependencies between services and service components.

For each service delivered, one or more SLAs shall be agreed with the customer. When creating SLAs, the service provider shall take into consideration the service requirements. SLAs shall include agreed service targets, workload characteristics and exceptions.

The service provider shall review services and SLAs with the customer at planned intervals.

Changes to the documented service requirements, catalogue of services, SLAs and other documented agreements shall be controlled by the change management process. The catalogue of services shall be maintained following changes to services and SLAs to ensure that they are aligned.

The service provider shall monitor trends and performance against service targets at planned intervals. Results shall be recorded and reviewed to identify the causes of nonconformities and opportunities for improvement.

For service components provided by an internal group or the customer, the service provider shall develop, agree, review and maintain a documented agreement to define the activities and interfaces between the two parties. The service provider shall monitor performance of the internal group or the customer against agreed service targets and other agreed commitments, at planned intervals. Results shall be recorded and reviewed to identify the causes of nonconformities and opportunities for improvement.

6.2 Service reporting

The description of each service report, including its identity, purpose, audience, frequency and details of the data source(s), shall be documented and agreed by the service provider and interested parties.

Service reports shall be produced for services using information from the delivery of services and the SMS activities, including the service management processes. Service reporting shall include at least:

a) performance against service targets;

b) relevant information about significant events including at least major incidents, deployment of new or changed services and the service continuity plan being invoked;

c) workload characteristics including volumes and periodic changes in workload;

d) detected nonconformities against the requirements in this part of ISO/IEC 20000, the SMS requirements or the service requirements and their identified causes;

e) trend information;

f) customer satisfaction measurements, service complaints and results of the analysis of satisfaction measurements and complaints.

The service provider shall make decisions and take actions based on the findings in service reports. The agreed actions shall be communicated to interested parties.

6.3 Service continuity and availability management

6.3.1 Service continuity and availability requirements

The service provider shall assess and document the risks to service continuity and availability of services. The service provider shall identify and agree with the customer and interested parties service continuity and availability requirements. The agreed requirements shall take into consideration applicable business plans, service requirements, SLAs and risks.

The agreed service continuity and availability requirements shall include at least:

a) access rights to the services;

b) service response times;

c) end to end availability of services.

6.3.2 Service continuity and availability plans

The service provider shall create, implement and maintain a service continuity plan(s) and an availability plan(s). Changes to these plans shall be controlled by the change management process.

The service continuity plan(s) shall include at least:

a) procedures to be implemented in the event of a major loss of service, or reference to them;

b) availability targets when the plan is invoked;

c) recovery requirements;

d) approach for the return to normal working conditions.

The service continuity plan(s), contact lists and the CMDB shall be accessible when access to normal service locations is prevented.

The availability plan(s) shall include at least availability requirements and targets.

The service provider shall assess the impact of requests for change on the service continuity plan(s) and the availability plan(s).

NOTE The service continuity plan(s) and availability plan(s) can be combined into one document.

6.3.3 Service continuity and availability monitoring and testing

Availability of services shall be monitored, the results recorded and compared with agreed targets. Unplanned non-availability shall be investigated and necessary actions taken.

Service continuity plans shall be tested against the service continuity requirements. Availability plans shall be tested against the availability requirements. Service continuity and availability plans shall be re-tested after major changes to the service environment in which the service provider operates.

The results of the tests shall be recorded. Reviews shall be conducted after each test and after the service continuity plan has been invoked. Where deficiencies are found, the service provider shall take necessary actions and report on the actions taken.

6.4 Budgeting and accounting for services

There shall be a defined interface between the budgeting and accounting for services process and other financial management processes.

There shall be policies and documented procedures for:

a) budgeting and accounting for service components including at least

   1) assets — including licences — used to provide the services,

   2) shared resources,

   3) overheads,

   4) capital and operating expenses,

   5) externally supplied services,

   6) personnel,

   7) facilities;

b) apportioning indirect costs and allocating direct costs to services, to provide an overall cost for each service;

c) effective financial control and approval.

Costs shall be budgeted to enable effective financial control and decision-making for services delivered.

The service provider shall monitor and report costs against the budget, review the financial forecasts and manage costs.

Information shall be provided to the change management process to support the costing of requests for change.

NOTE Many service providers charge for their services. The scope of the budgeting and accounting for services process excludes charging.

6.5 Capacity management

The service provider shall identify and agree capacity and performance requirements with the customer and interested parties.

The service provider shall create, implement and maintain a capacity plan taking into consideration human, technical, information and financial resources. Changes to the capacity plan shall be controlled by the change management process.

The capacity plan shall include at least:

a) current and forecast demand for services;

b) expected impact of agreed requirements for availability, service continuity and service levels;

c) time-scales, thresholds and costs for upgrades to service capacity;

d) potential impact of statutory, regulatory, contractual or organizational changes;

e) potential impact of new technologies and new techniques;

f) procedures to enable predictive analysis, or reference to them.

The service provider shall monitor capacity usage, analyse capacity data and tune performance. The service provider shall provide sufficient capacity to fulfil agreed capacity and performance requirements.

6.6 Information security management

6.6.1 Information security policy

Management with appropriate authority shall approve an information security policy taking into consideration the service requirements, statutory and regulatory requirements and contractual obligations. Management shall:

a) communicate the information security policy and the importance of conforming to the policy to appropriate personnel within the service provider, customer and suppliers;

b) ensure that information security management objectives are established;

c) define the approach to be taken for the management of information security risks and the criteria for accepting risks;

d) ensure that information security risk assessments are conducted at planned intervals;

e) ensure that internal information security audits are conducted;

f) ensure that audit results are reviewed to identify opportunities for improvement.

6.6.2 Information security controls

The service provider shall implement and operate physical, administrative and technical information security controls in order to:

a) preserve confidentiality, integrity and accessibility of information assets;

b) fulfil the requirements of the information security policy;

c) achieve information security management objectives;

d) manage risks related to information security.

These information security controls shall be documented and shall describe the risks to which the controls relate, their operation and maintenance.

The service provider shall review the effectiveness of information security controls. The service provider shall take necessary actions and report on the actions taken.

The service provider shall identify external organizations that have a need to access, use or manage the service provider's information or services. The service provider shall document, agree and implement information security controls with these external organizations.

6.6.3 Information security changes and incidents

Requests for change shall be assessed to identify:

a) new or changed information security risks;

b) potential impact on the existing information security policy and controls.

Information security incidents shall be managed using the incident management procedures, with a priority appropriate to the information security risks. The service provider shall analyse the types, volumes and impacts of information security incidents. Information security incidents shall be reported and reviewed to identify opportunities for improvement.

NOTE The ISO/IEC 27000 family of standards specifies requirements and provides guidance to support the implementation and operation of an information security management system.

7 Relationship processes

7.1 Business relationship management

The service provider shall identify and document the customers, users and interested parties of the services.

For each customer, the service provider shall have a designated individual who is responsible for managing the customer relationship and customer satisfaction.

The service provider shall establish a communication mechanism with the customer. The communication mechanism shall promote understanding of the business environment in which the services operate and requirements for new or changed services. This information shall enable the service provider to respond to these requirements.

The service provider shall review the performance of the services at planned intervals, with the customer.

Changes to the documented service requirements shall be controlled by the change management process. Changes to the SLAs shall be co-ordinated with the service level management process.

The definition of a service complaint shall be agreed with the customer. There shall be a documented procedure to manage service complaints from the customer. The service provider shall record, investigate, act upon, report and close service complaints. Where a service complaint is not resolved through the normal channels, escalation shall be provided to the customer.

The service provider shall measure customer satisfaction at planned intervals based on a representative sample of the customers and users of the services. The results shall be analysed and reviewed to identify opportunities for improvement.

7.2 Supplier management

The service provider may use suppliers to implement and operate some parts of the service management processes. An example of supply chain relationships is illustrated in Figure 3.

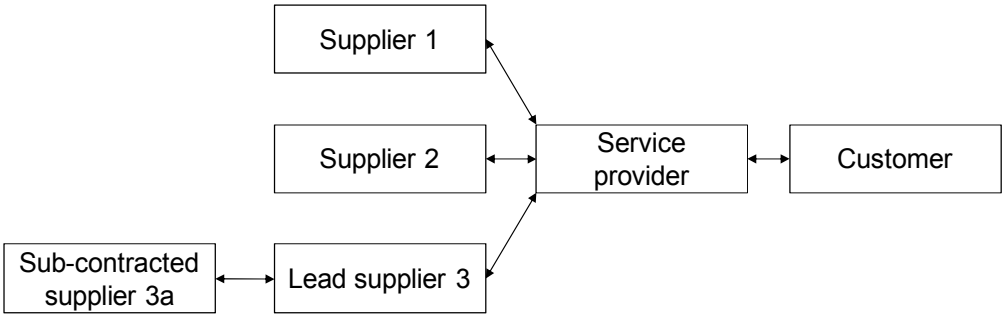

Figure 3 — Example of supply chain relationships

For each supplier, the service provider shall have a designated individual who is responsible for managing the relationship, the contract and performance of the supplier.

The service provider and the supplier shall agree a documented contract. The contract shall contain or include a reference to:

a) scope of the services to be delivered by the supplier;

b) dependencies between services, processes and the parties;

c) requirements to be fulfilled by the supplier;

d) service targets;

e) interfaces between service management processes operated by the supplier and other parties;

f) integration of the supplier's activities within the SMS;

g) workload characteristics;

h) contract exceptions and how these will be handled;

i) authorities and responsibilities of the service provider and the supplier;

j) reporting and communication to be provided by the supplier;

k) basis for charging;

l) activities and responsibilities for the expected or early termination of the contract and the transfer of services to a different party.

The service provider shall agree with the supplier service levels to support and align with the SLAs between the service provider and the customer.

The service provider shall ensure that roles of, and relationships between, lead and sub-contracted suppliers are documented. The service provider shall verify that lead suppliers are managing their sub-contracted suppliers to fulfil contractual obligations.

The service provider shall monitor the performance of the supplier at planned intervals. The performance shall be measured against service targets and other contractual obligations. Results shall be recorded and reviewed to identify the causes of nonconformities and opportunities for improvement. The review shall also ensure that the contract reflects current requirements.

Changes to the contract shall be controlled by the change management process.

There shall be a documented procedure to manage contractual disputes between the service provider and the supplier.

NOTE 1 The scope of the supplier management process excludes the selection of suppliers and the procurement of services.

NOTE 2 Further examples of supply chain relationships are shown in ISO/IEC TR 20000-3.

8 Resolution processes

8.1 Incident and service request management

There shall be a documented procedure for all incidents to define:

a) recording;

b) allocation of priority;

c) classification;

d) updating of records;

e) escalation;

f) resolution;

g) closure.

There shall be a documented procedure for managing the fulfilment of service requests from recording to closure. Incidents and service requests shall be managed according to the procedures.

When prioritizing incidents and service requests, the service provider shall take into consideration the impact and urgency of the incident or service request.

The service provider shall ensure that personnel involved in the incident and service request management process can access and use relevant information. The relevant information shall include service request management procedures, known errors, problem resolutions and the CMDB. Information about the success or failure of releases and future release dates, from the release and deployment management process, shall be used by the incident and service request management process.

The service provider shall keep the customer informed of the progress of their reported incident or service request. If service targets cannot be met, the service provider shall inform the customer and interested parties and escalate according to the procedure.

The service provider shall document and agree with the customer the definition of a major incident. Major incidents shall be classified and managed according to a documented procedure. Top management shall be informed of major incidents. Top management shall ensure that a designated individual responsible for managing the major incident is appointed. After the agreed service has been restored, major incidents shall be reviewed to identify opportunities for improvement.

8.2 Problem management

There shall be a documented procedure to identify problems and minimize or avoid the impact of incidents and problems. The procedure for problems shall define:

a) identification;

b) recording;

c) allocation of priority;

d) classification;

e) updating of records;

f) escalation;

g) resolution;

h) closure.

Problems shall be managed according to the procedure.

The service provider shall analyse data and trends on incidents and problems to identify root causes and their potential preventive action.

Problems requiring changes to a CI shall be resolved by raising a request for change.

Where the root cause has been identified, but the problem has not been permanently resolved, the service provider shall identify actions to reduce or eliminate the impact of the problem on the services. Known errors shall be recorded.

The effectiveness of problem resolution shall be monitored, reviewed and reported.

Up-to-date information on known errors and problem resolutions shall be provided to the incident and service request management process.

9 Control processes

9.1 Configuration management

There shall be a documented definition of each type of CI. The information recorded for each CI shall ensure effective control and include at least:

a) description of the CI;

b) relationship(s) between the CI and other CIs;

c) relationship(s) between the CI and service components;

d) status;

e) version;

f) location;

g) associated requests for change;

h) associated problems and known errors.

CIs shall be uniquely identified and recorded in a CMDB. The CMDB shall be managed to ensure its reliability and accuracy, including control of update access.

There shall be a documented procedure for recording, controlling and tracking versions of CIs. The degree of control shall maintain the integrity of services and service components taking into consideration the service requirements and the risks associated with the CIs.

The service provider shall audit the records stored in the CMDB, at planned intervals. Where deficiencies are found, the service provider shall take necessary actions and report on the actions taken.

Information from the CMDB shall be provided to the change management process, to support the assessment of requests for change.

Changes to CIs shall be traceable and auditable to ensure integrity of the CIs and the data in the CMDB.

A configuration baseline of the affected CIs shall be taken before deployment of a release into the live environment.

Master copies of CIs recorded in the CMDB shall be stored in secure physical or electronic libraries referenced by the configuration records. This shall include at least documentation, licence information, software and, where available, images of the hardware configuration.

There shall be a defined interface between the configuration management process and financial asset management process.

NOTE The scope of the configuration management process excludes financial asset management.

9.2 Change management

A change management policy shall be established that defines:

a) CIs which are under the control of change management;

b) criteria to determine changes with potential to have a major impact on services or the customer.

Removal of a service shall be classified as a change to a service with the potential to have a major impact. Transfer of a service from the service provider to the customer or a different party shall be classified as a change with potential to have a major impact.

There shall be a documented procedure to record, classify, assess and approve requests for change.

The service provider shall document and agree with the customer the definition of an emergency change. There shall be a documented procedure for managing emergency changes.

All changes to a service or service component shall be raised using a request for change. Requests for change shall have a defined scope.

All requests for change shall be recorded and classified. Requests for change classified as having the potential to have a major impact on the services or the customer shall be managed using the design and transition of new or changed services process. All other requests for change to CIs defined in the change management policy shall be managed using the change management process.

Requests for change shall be assessed using information from the change management process and other processes.

The service provider and interested parties shall make decisions on the acceptance of requests for change. Decision-making shall take into consideration the risks, the potential impacts to services and the customer, service requirements, business benefits, technical feasibility and financial impact.

Approved changes shall be developed and tested.

A schedule of change containing details of the approved changes and their proposed deployment dates shall be established and communicated to interested parties. The schedule of change shall be used as the basis for planning the deployment of releases.

The activities required to reverse or remedy an unsuccessful change shall be planned and, where possible, tested. The change shall be reversed or remedied if unsuccessful. Unsuccessful changes shall be investigated and agreed actions taken.

The CMDB records shall be updated following the successful deployment of changes.

The service provider shall review changes for effectiveness and take actions agreed with interested parties.

Requests for change shall be analysed at planned intervals to detect trends. The results and conclusions drawn from the analysis shall be recorded and reviewed to identify opportunities for improvement.

9.3 Release and deployment management

The service provider shall establish and agree with the customer a release policy stating the frequency and type of releases.

The service provider shall plan with the customer and interested parties the deployment of new or changed services and service components into the live environment. Planning shall be coordinated with the change management process and include references to the related requests for change, known errors and problems which are being closed through the release. Planning shall include the dates for deployment of each release, deliverables and methods of deployment.

The service provider shall document and agree with the customer the definition of an emergency release. Emergency releases shall be managed according to a documented procedure that interfaces to the emergency change procedure.

Releases shall be built and tested prior to deployment. A controlled acceptance test environment shall be used for the building and testing of releases.

Acceptance criteria for the release shall be agreed with the customer and interested parties. The release shall be verified against the agreed acceptance criteria and approved before deployment. If the acceptance criteria are not met, the service provider shall make a decision on necessary actions and deployment with interested parties.

The release shall be deployed into the live environment so that the integrity of hardware, software and other service components is maintained during deployment of the release.

The activities required to reverse or remedy an unsuccessful deployment of a release shall be planned and, where possible, tested. The deployment of the release shall be reversed or remedied if unsuccessful. Unsuccessful releases shall be investigated and agreed actions taken.

The success or failure of releases shall be monitored and analysed. Measurements shall include incidents related to a release in the period following deployment of a release. Analysis shall include assessment of the impact of the release on the customer. The results and conclusions drawn from the analysis shall be recorded and reviewed to identify opportunities for improvement.

Information about the success or failure of releases and future release dates shall be provided to the change management process, and incident and service request management process.

Information shall be provided to the change management process to support the assessment of the impact of requests for change on releases and plans for deployment.

Bibliography

[1] ISO/IEC 20000-2:2005, *Information technology — Service management — Part 2: Code of practice*

[2] ISO/IEC TR 20000-3, *Information technology — Service management — Part 3: Guidance on scope definition and applicability for ISO/IEC 20000-1*

[3] ISO/IEC TR 20000-4, *Information technology — Service management — Part 4: Process reference model*

[4] ISO/IEC TR 20000-5, *Information technology — Service management — Part 5: Exemplar implementation plan for ISO/IEC 20000-1*

[5] ISO 9000:2005, *Quality management systems — Fundamentals and vocabulary*

[6] ISO 9001, *Quality management systems — Requirements*

[7] ISO 9004:2000, *Quality management systems — Guidelines for performance improvements*

[8] ISO 10002, *Quality management — Customer satisfaction — Guidelines for complaints handling in organizations*

[9] ISO 10007, *Quality management systems — Guidelines for configuration management*

[10] ISO/IEC 15288, *Systems and software engineering — System life cycle processes*

[11] ISO/IEC 15504-1, *Information technology — Process assessment — Part 1: Concepts and vocabulary*

[12] ISO/IEC 15504-2, *Information technology — Process assessment — Part 2: Performing an assessment*

[13] ISO/IEC 15504-3, *Information technology — Process assessment — Part 3: Guidance on performing an assessment*

[14] ISO 19011, *Guidelines for quality and/or environmental management systems auditing*

[15] ISO/IEC 19770-1, *Information technology — Software asset management — Part 1: Processes*

[16] ISO/IEC/IEEE 24765:2010, *Systems and software engineering — Vocabulary*

[17] ISO/IEC 27000:2009, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

[18] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[19] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

[20] ISO 31000, *Risk management — Principles and guidelines*

ICS 03.080.99; 35.020

Price based on 26 pages