TECHNICAL REPORT

ISO/IEC
TR
20000-3

First edition
2009-11-01

Information technology — Service management —

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

Technologies de l'information — Gestion des services —

Partie 3: Directives pour la définition du domaine d'application et l'applicabilité de l'ISO/CEI 20000-1

© ISO/IEC 2009

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC TR 20000-3:2009
https://standards.iteh.ai/catalog/standards/sist/3df35d18-d988-41fe-b835-
8602bdd0b85e/iso-iec-tr-20000-3-2009

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.

In exceptional circumstances, the joint technical committee may propose the publication of a Technical Report of one of the following types:

— type 1, when the required support cannot be obtained for the publication of an International Standard, despite repeated efforts;

— type 2, when the subject is still under technical development or where for any other reason there is the future but not immediate possibility of an agreement on an International Standard;

— type 3, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example).

Technical Reports of types 1 and 2 are subject to review within three years of publication, to decide whether they can be transformed into International Standards. Technical Reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.

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 TR 20000-3, which is a Technical Report of type 2, was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 7, *Software and systems engineering*.

ISO/IEC TR 20000-3 was developed for use with ISO/IEC 20000-1 and ISO/IEC 20000-2.

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

— *Part 1: Specification*

— *Part 2: Code of practice*

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

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

Introduction

This part of ISO/IEC 20000 provides guidance on scope definition, applicability and demonstration of conformity for the service provider aiming to fulfil the requirements specified in ISO/IEC 20000-1, or for the service provider intending to use ISO/IEC 20000-1 as a business objective. The intended user of this part of ISO/IEC 20000 is the service provider, but it could also be useful for consultants and assessors. It supplements the advice in the code of practice, ISO/IEC 20000-2, which provides generic guidelines for implementing a service management system (SMS) in accordance with ISO/IEC 20000-1. It is not intended as guidance on obtaining an ISO/IEC 20000-1 certificate.

This part of ISO/IEC 20000 takes the form of examples, guidance and recommendations. It should not be quoted as if it were a specification of requirements and particular care should be taken to ensure that declarations of conformity are not misleading.

ISO/IEC 20000-1 specifies requirements for an SMS to deliver information technology (IT) services. There are no requirements that relate to organization structure, size, names and type. ISO/IEC 20000-1 applies to service providers irrespective of size. The process requirements described in ISO/IEC 20000-1 do not change with organizational structure, technology or service. Operating the processes in a particular system or service environment will result in unique skill, tool and information requirements, even though the process attributes are unchanged.

The service provider who implements an SMS based on ISO/IEC 20000-1 is required to define the scope of the SMS as part of its planning. This part of ISO/IEC 20000 provides guidance on defining the scope of the SMS and on the applicability of ISO/IEC 20000-1. Guidance provided in this part of ISO/IEC 20000 will also be useful to the service provider who is making preparations for conformity assessment against ISO/IEC 20000-1, including how to state the scope of the SMS for the assessment.

Service management processes in the IT industry can cross many organizational, legal and national boundaries as well as different time zones. Many service providers depend on a complex supply chain for the delivery of services. Many service providers also provide a range of services to several different types of customer. This makes the scope of the SMS, and the agreement of the scope statement, a complex stage in the service provider's use of ISO/IEC 20000-1.

This part of ISO/IEC 20000 provides practical examples of scope statements for the service provider irrespective of whether they have experience of documenting a scope statement required by other management system standards.

ISO/IEC TR 20000-3:2009
https://standards.iteh.ai/catalog/standards/sist/3df35d18-d988-41fe-b835-
8602bdd0b85e/iso-iec-tr-20000-3-2009

Information technology — Service management —

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

1   Scope

ISO/IEC 20000-1 specifies a number of related management processes. This part of ISO/IEC 20000 provides guidance and commentary on scope definition and applicability of ISO/IEC 20000-1 to enable the service provider to fulfil the requirements specified in ISO/IEC 20000-1.

This part of ISO/IEC 20000 assists the service provider who is planning service improvements or preparing for a conformity assessment against ISO/IEC 20000-1. It can also assist the service provider who is considering using ISO/IEC 20000-1 for establishing a service management system (SMS) and who needs specific advice on whether ISO/IEC 20000-1 is applicable to its circumstances. Finally, it shows how to define the scope of an SMS based on practical examples.

This part of ISO/IEC 20000 gives a list of main points on stating scope, on the applicability of ISO/IEC 20000-1 and on demonstrating conformity to ISO/IEC 20000-1. It also includes examples of scope statements, which vary according to the service provider's circumstances.

2   Normative references

The following referenced document is 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: Specification*

3   Terms and definitions

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

3.1
assessor
person, an internal or external auditor, who performs assessment activities necessary to establish whether the service provider's service management system fulfils the requirements specified in ISO/IEC 20000-1

4   Fulfilling the requirements specified in ISO/IEC 20000-1

Some service providers who have implemented a service management system (SMS) based on ISO/IEC 20000-1 wish to demonstrate conformity to the requirements specified in ISO/IEC 20000-1. The

service provider who wishes to demonstrate conformity should be able to demonstrate fulfilment of all requirements. The verbal form 'shall' is used for all requirements specified in ISO/IEC 20000-1.

The service provider should plan and record the improvements that are necessary to fulfil the requirements, so they are able to demonstrate that:

a) all processes required by ISO/IEC 20000-1 are documented and operated to achieve desired outcomes, including governance of those processes operated by other parties, within the scope of the SMS;

b) interfaces between processes are operated and documented within the service management plans and produce desired outcomes;

c) service management capability produces the agreed outcomes, according business needs and customer requirements;

d) the SMS is managed from an end-to-end perspective, working with suppliers and internal groups to meet the agreed outcomes.

There are three types of conformity assessments:

— first-party, done using the service provider's own resources, usually referred to as internal audit;

— second-party, done by a person or organization that has a user interest in the organization, such as customers, or by other persons on their behalf;

— third-party, done by a conformity assessment organization usually referred to as a certification body.

There are international standards on practices in conformity assessment. Some of them are designed for audits against management system standards. For example, ISO/IEC 17021 and ISO/IEC 19011 both include generic requirements for third-party assessments against management systems, including SMS. ISO/IEC 17021 is for third-party conformity assessment and ISO/IEC 19011 is for all types of conformity assessment.

ISO/IEC 17000 provides terms and definitions that are related to conformity assessment in general, including the terms first-party, second-party and third-party conformity assessment.

If the service provider intends to issue the declaration of conformity based on the successful results of a first-party conformity assessment that has proved the service provider fulfils the requirements specified in ISO/IEC 20000-1, the service provider should refer to ISO/IEC 17050-1 which specifies general requirements for such a declaration of conformity.

Certification bodies establish rules on the awarding of a certificate by the certification body following a successful third-party conformity assessment. For example, the certification body can require that an ISO/IEC 20000-1 certificate is only issued to a single legal entity, not a consortium.

5 Applicability of ISO/IEC 20000-1

5.1 Introduction

ISO/IEC 20000-1 is very widely applicable. A broad range of service providers can use an SMS based on ISO/IEC 20000-1. ISO/IEC 20000-1 applies to internal and external, large and small, and commercial and non-commercial service providers. The applicability of ISO/IEC 20000-1 is independent of the funding for the service so the costs may be in a single organizational budget covering both the internal customer and the internal service provider.

ISO/IEC 20000-1 can be applicable to the service provider even if its customers or suppliers have demonstrated conformity to ISO/IEC 20000-1. This is described in clause 5.2 and in Annex B.

Fulfilling all the requirements is not always possible for the service provider whose customers or suppliers have demonstrated conformity to ISO/IEC 20000-1. Typically, this arises when the service provider has governance of only some of the processes. Under these circumstances, the assessor's professional judgment can be that ISO/IEC 20000-1 is not appropriate and that another standard is more suitable, e.g. ISO 9001 or a more specialist standard covering only some aspects of service management, such as security or configuration management.

ISO/IEC 20000-1 is only applicable if the service provider remains accountable for the delivery of the service, as shown in the scenarios in Annex B.

5.2   Governance of processes operated by other parties

The service provider who wishes to conform to the standard is required to have governance of all processes in ISO/IEC 20000-1.

It is particularly important to demonstrate process governance if other parties operate some parts of the processes within the scope of the SMS.

Other parties may be internal groups in the same organization as the service provider, but who are not part of the service provider's own organizational unit. An internal group has a formal agreement with the service provider, specifying its contribution to the services delivered by the service provider.

Other parties may also be customers or suppliers. A customer is an organization or part of an organization that receives a service and may be internal or external to the service provider. A supplier is an external organization or part of an external organization and has a formal agreement with the service provider specifying its contribution to the services delivered by the service provider. Unlike internal groups, the supplier's formal agreement may be a legally-binding contract.

The service provider is required to demonstrate process governance by:

a) demonstrating accountability for the processes and the authority to require adherence to the processes. For example, establishing the information security policy, using controls, detecting breaches and initiating corrective actions;

b) controlling the definition of the processes and interfaces to other processes. For example, documenting, agreeing and operating the interfaces and dependencies of the change management process with the configuration management process;

c) determining process performance and compliance through access to and analysis of measurements and other records. For example, accessing a set of incident records and incident management process performance measurements, analysing them and initiating improvements;

d) controlling the planning and the prioritizing of process improvements. For example, assessing a set of improvements in the capacity management process, prioritizing them and scheduling their implementation.

The service provider can request other parties to use specific processes or can work with other parties to document and approve the processes that the other parties operate.

The service provider is not required to implement the process itself, in order to establish process governance.

Where suppliers are operating a process, the service provider is also required to manage the supplier through the supplier management process.

If the service provider relies on other parties for operation of the majority of the processes, 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 could fulfil the requirements specified in ISO/IEC 20000-1. Wherever other parties are involved, the service provider should be able to demonstrate process governance of all processes within the scope of the SMS.

In outsourced situations, the service provider should ensure that service contracts with suppliers do not prevent the service provider from having governance of all management processes within the scope of the SMS. Process governance has to be demonstrated only for processes included in the service provider's scope. Processes under the control of other parties cannot be included in the service provider's scope statement.

5.3 The extent of technology used to deliver services

The applicability of ISO/IEC 20000-1 is unaffected by the technologies used for the delivery of services, including the technologies used to automate service management processes. This is the case even if the technology is not included in the list of examples given below.

The technologies used by a service do not change the management processes, but will have a direct impact on the skill, tool and data requirements of the process activities.

The extent of technology includes but is not limited to the following:

a) servers and mainframes;

b) desktops;

c) networks;

d) telecommunications;

e) storage systems;

f) environmental equipment;

g) applications;

h) multi-media systems;

i) mobile and smart devices;

j) management tools and systems.

6 General principles for an SMS scope

6.1 Introduction

The service provider is required to define the scope of the SMS and include a scope statement in the service management plan, before establishing the SMS. Top management of the service provider are responsible for the service management plan. After the SMS has been established top management are responsible for reviewing the scope of the SMS for continuing effectiveness and validity.

The scope of the SMS is required to take into account that demonstrating conformity requires fulfilment of all requirements specified in ISO/IEC 20000-1. The service provider needs to have governance of all processes within the scope of the SMS, including processes crossing organizational boundaries between the service provider and other parties.

The scope statement should:

a) be as simple as possible;

b) be understandable without detailed knowledge of the service provider's organization;

c) include enough information for use in conformity assessment;

d) be worded so it does not intentionally or unintentionally imply that something is included if it is excluded.

6.2 Integrating or aligning with other management systems

The service provider should be aware that ISO/IEC 20000-1 enables alignment or integration of an SMS with other related management systems. The inclusion of the Plan-Do-Check-Act model in ISO/IEC 20000-1 enhances compatibility with other management system standards.

The service provider may define the scope of its SMS as geographically or organizationally identical to the scope of other management systems, such as an Information Security Management System (ISMS) based on ISO/IEC 27001 or a Quality Management System (QMS) based on ISO 9001.

However, the service provider should be aware that there could be a need for differences within the scope in order to fulfil specific requirements in each management system standard. There are differences in requirements because each type of management system has a different purpose. The SMS, ISMS and QMS each cover topics that the others do not.

6.3 The scope of the SMS

6.3.1 Defining the scope

The service provider should discuss the scope statement with its assessor. Reassurance that the proposed scope is valid, before establishing the SMS, will avoid setting false expectations.

The service provider should demonstrate that the scope is valid at the beginning of an assessment because it is fundamental to the assessor's planning of the assessment.

Processes and services to customers outside the scope of the SMS do not have to fulfil the requirements specified in ISO/IEC 20000-1 and will not influence or affect an assessment. Exclusions do not have to be referred to in the scope statement but can help to make the scope statement unambiguous.

6.3.2 Limits to the scope

Where the service provider intends to include an entire business area in the SMS, defining the scope of an SMS is relatively simple. This is because the scope is everything the service provider does. If the service provider includes only some of its services in the SMS it can be difficult to define the scope in simple terms or to avoid ambiguity.

A demonstration of conformity may be the fulfilment of all requirements for one small service to one customer, which represents a small proportion of the service provider's total services. This needs to be explicitly stated in the scope statement, to avoid any risk of the scope statement being misunderstood.

The external service provider can have many customers and deliver many services, so the scope of the SMS may include services for several customers. When this is the case, the processes should be used to deliver services to each customer. The processes for each customer may vary in detail, but each process is required to fulfil the requirements for that process.

An internal service provider supplies services to customers within the same organization as the service provider. In the situation where an internal service provider supplies many services to many customers within its own organization, the scope statement should be based on the services offered, within the scope of the SMS.

Despite the difficulty of including only some services in the SMS, many service providers prefer to demonstrate conformity initially for only some of the services. The service provider may then extend the scope of the SMS, up to the whole extent of the service provider's services, as described in clause 6.6.

6.4   Service contracts between customers and the service provider

The service provider delivering services under the terms of a legally binding contract should be aware that it is not possible for the contract to reduce the service provider's obligation to fulfil all the requirements specified in ISO/IEC 20000-1. Nor is it possible for the terms of a contract to remove the assessor's obligations to obtain sufficient evidence of conformity to all the requirements. This is the case even if a contract limits the services and processes.

6.5   Scope definition parameters

6.5.1   Permitted types of scope definition parameters

The service provider should use parameters to define the scope of the SMS to ensure that there is no ambiguity about what is included and excluded. The parameters include but are not limited to:

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

b)   services offered, e.g. a single service, group of services 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 customers or internal customers;

e)   technology used to provide the services (see 5.3).

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

If the scope statement includes many customers, services or locations, then an assessor may base the assessment on a sample, using his/her professional judgement for selection of the sample and what will be assessed. The scope statement may include the full range of customers, services and locations within the scope of the SMS, not just those sampled.

EXAMPLE:

The structure of a scope statement may be:

"The service management system of *<name of service provider organizational unit>* that delivers *<service(s)>* to *<customer organizational name and/or name of organizational unit>* from *<geographical location>*"

A scope statement using the names of customers may include only those customers where all requirements are fulfilled, even if the service provider has many other customers. Alternatively, instead of using customer names, other parameters, such as service, location, or technology, may be used. For example, "*all services from the data centre at location A*" or "*all mainframe-based services*" could include several customers, without listing individual customers.

Examples based on commonly used scope definition parameters are given in Annex B.

6.5.2   Currency of parameters

The parameters used in scope statements can become out of date. The service provider should review the scope of the SMS and scope statements on a regular basis, to check that they are still valid.

The service provider should ensure that the scope statement is, as far as possible, able to accommodate changes without introducing ambiguity. Although any parameters can become out of date, an explicit list of organizational units (departments), geographic locations (specific addresses) or services is normally useful.