INTERNATIONAL STANDARD

ISO/IEC 20000-6

First edition
2017-06

Information technology — Service management —

Part 6: Requirements for bodies providing audit and certification of service management systems

Technologies de l'information — Gestion des services —

Partie 6: Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la gestion des services

Reference number
ISO/IEC 20000-6:2017(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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

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

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

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

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

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

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

Introduction

This document is for use by certification bodies for auditing and certifying a service management system (SMS) in accordance with ISO/IEC 20000-1. It can also be used by accreditation bodies when assessing certification bodies. It is intended to be used in conjunction with ISO/IEC 17021-1, which sets out criteria for certification bodies providing audit and certification of management systems. This document provides requirements additional to those in ISO/IEC 17021-1.

Correct application of this document will enable certification bodies to harmonize their application of ISO/IEC 17021-1 for assessments against ISO/IEC 20000-1. It will also enable accreditation bodies to harmonize their application of the standards they use to assess certification bodies.

This document follows the structure of ISO/IEC 17021-1, as far as possible. The requirements additional to those in ISO/IEC 17021-1 are shown as subclauses numbered "SMxxx".

ISO/IEC 17021-1 and this document use the term "client" for the organization seeking certification.

Information technology — Service management —

Part 6: Requirements for bodies providing audit and certification of service management systems

1 Scope

This document specifies requirements and provides guidance for certification bodies providing audit and certification of an SMS in accordance with ISO/IEC 20000-1. It does not change the requirements specified in ISO/IEC 20000-1. This document can also be used by accreditation bodies for accreditation of certification bodies.

A certification body providing SMS certification is expected to be able to demonstrate fulfilment of the requirements specified in this document, in addition to the requirements in ISO/IEC 17021-1.

2 Normative references

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

ISO/IEC 17021-1:2015, *Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements*

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

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 17021-1 and ISO/IEC TR 20000-10 apply.

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

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

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

4 Principles

For the purposes of this document, the principles in ISO/IEC 17021-1:2015, Clause 4 apply.

5 General requirements

5.1 Legal and contractual matters

The requirements in ISO/IEC 17021-1:2015, 5.1 apply.

5.2 Management of impartiality

The requirements in ISO/IEC 17021-1:2015, 5.2 apply. In addition, the following requirements and guidance apply.

5.2.1 SM5.2.1 Conflicts of interest

Certification bodies may carry out the following duties without them being considered as consultancy or having a potential conflict of interest:

a) arranging and participating as a lecturer in training courses. Where these courses relate to service management, related management systems or auditing, certification bodies shall confine themselves to the provision of generic information and advice which is publicly available, i.e. they shall not provide company-specific advice;

b) making available or publishing on request information describing the certification body's interpretation of the requirements of the certification audit standards;

c) activities prior to audit, solely aimed at determining readiness for certification audit. These activities shall not result in the provision of recommendations or advice that would contravene this subclause. The certification body shall be able to confirm that such activities do not contravene these requirements and that they are not used to justify a reduction in the eventual certification audit duration;

d) performing second and third-party audits according to standards or regulations other than those being part of the scope of accreditation;

e) adding value during certification audits and surveillance visits, e.g. by identifying opportunities for improvement, as they become evident during the audit, without recommending specific solutions.

The certification body shall not provide internal service management reviews of the client's SMS subject to certification. The certification body shall be independent of the body or bodies (including any individuals) which provide the internal SMS audit.

5.3 Liability and financing

The requirements in ISO/IEC 17021-1:2015, 5.3 apply.

6 Structural requirements

The requirements in ISO/IEC 17021-1:2015, Clause 6 apply.

7 Resource requirements

7.1 Competence of personnel

7.1.1 General considerations

The requirements in ISO/IEC 17021-1:2015, 7.1.1 apply.

7.1.2 Determination of competence criteria

The requirements in ISO/IEC 17021-1:2015, 7.1.2 apply. In addition, the following requirements and guidance apply.

7.1.2.1 SM7.1.2.1 The term “technical area”

ISO/IEC 20000-1 states that all requirements are generic and are intended to be applicable to all clients, regardless of type, size and the nature of the services delivered. For ISO/IEC 20000-1 audits, the term “technical area” relates to the SMS, including service management processes and the services within the scope of the SMS. “Technical area” does not relate to any underlying technology used to enable service delivery.

7.1.3 Evaluation processes

The requirements in ISO/IEC 17021-1:2015, 7.1.3 apply.

7.1.4 Other considerations

The requirements in ISO/IEC 17021-1:2015, 7.1.4 apply.

7.2 Personnel involved in certification activities

The requirements in ISO/IEC 17021-1:2015, 7.2 apply. In addition, the following requirements and guidance apply.

7.2.1 SM7.2.1 Competence of personnel involved in certification activities

The certification body shall define criteria for the training and competence development of auditors and personnel involved in managing and supporting certification activities. The certification body shall ensure knowledge, as appropriate for each role, of:

a) the requirements specified in ISO/IEC 20000-1;

b) the relevant parts of ISO/IEC 20000, especially ISO/IEC 20000-2, ISO/IEC 20000-3 and ISO/IEC TR 20000-10.

The certification body shall ensure that auditors and personnel involved in managing and supporting certification activities have appropriate awareness of the impact of legal and regulatory requirements relevant to auditing an SMS, according to the jurisdictions in scope. Awareness of legal and regulatory requirements does not imply profound legal knowledge: a management system certification audit is not a legal compliance audit.

The certification body shall ensure auditors keep knowledge and skills in service management and auditing up to date through continual professional development.

7.3 Use of individual external auditors and external technical experts

The requirements in ISO/IEC 17021-1:2015, 7.3 apply.

7.4 Personnel records

The requirements in ISO/IEC 17021-1:2015, 7.4 apply.

7.5 Outsourcing

The requirements in ISO/IEC 17021-1:2015, 7.5 apply.

8 Information requirements

8.1 Public information

The requirements in ISO/IEC 17021-1:2015, 8.1 apply.

8.2 Certification documents

The requirements in ISO/IEC 17021-1:2015, 8.2 apply. In addition, the following requirements and guidance apply.

8.2.1 SM8.2.1 Scope definition

The guidance in ISO/IEC 20000-3 should be used when defining the scope.

8.3 Reference to certification and use of marks

The requirements in ISO/IEC 17021-1:2015, 8.3 apply.

8.4 Confidentiality

The requirements in ISO/IEC 17021-1:2015, 8.4 apply. In addition, the following requirements and guidance apply.

8.4.1 SM8.4.1 Access to the client's documents, including records

Before the certification audit is agreed, the certification body shall ask the client to report if any SMS documents or records cannot be made available for review by the audit team because they contain confidential or sensitive information. The certification body shall determine whether the SMS can be adequately audited in the absence of these documents or records. If any documents or records are essential for the audit and are not available, the certification body shall advise the client that an audit cannot take place until appropriate access arrangements are granted.

8.5 Information exchange between a certification body and its clients

The requirements in ISO/IEC 17021-1:2015, 8.5 apply.

9 Process requirements

9.1 Pre-certification activities

9.1.1 Application

The requirements in ISO/IEC 17021-1:2015, 9.1.1 apply.

9.1.2 Application review

The requirements in ISO/IEC 17021-1:2015, 9.1.2 apply. In addition, the following requirements and guidance apply.

9.1.2.1 SM9.1.2.1 Application review

The certification body shall review the application from the client to ensure a clear understanding of the areas of activity of the client and the likely risks to the SMS and the services.

9.1.3 Audit programme

The requirements in ISO/IEC 17021-1:2015, 9.1.3 apply.

9.1.4 Determining audit time

The requirements in ISO/IEC 17021-1:2015, 9.1.4 apply. In addition, the following requirements and guidance apply.

9.1.4.1 SM9.1.4.1 Determining audit time for initial audit

The certification body shall use the number of effective client personnel as the basis for determining audit time for an initial certification audit. The certification body shall use Table 1 when determining audit time. Table 1 is based on 8-hour days. The figures may be adjusted if the hours per day are higher or lower than 8 h.

The number of effective client personnel shall be calculated as full-time equivalents (FTE). The calculation of effective client personnel shall be based on those in the scope of the SMS. The certification body shall be able to justify the rationale used for the relationship between the number of effective client personnel supporting the SMS and the services and the audit time.

If the number of effective client personnel supporting the SMS and the services exceeds 1 175, the certification body's procedures shall provide for the calculation of audit time, following the progression in Table 1 in a consistent manner and define the days by extrapolation beyond the last band in Table 1.

The certification body shall base their plans for an initial audit on a minimum audit time of 2,5 d, after adjustments, irrespective of the number of client personnel.

The audit duration shall not be less than 80 % of the audit time. If additional time is needed for planning or report writing, this shall not reduce the audit duration.

Table 1 — Relationship between effective number of personnel and audit time before adjustments (initial audit)

Effective number of client personnel	Audit time: Stage 1 + Stage 2 (days)
1–15	3,5
16–25	4,5
26–45	5,5
46–65	6
66–85	7
86–125	8
126–175	9
176–275	10
276–425	11
426–625	12
626–875	13
876–1 175	15

NOTE Audit time is defined as the time needed to plan and accomplish a complete and effective audit of the client's management system. Audit time includes the total time on-site at a client's location (physical or virtual) and time spent off-site carrying out planning, document review, interacting with client personnel and report writing. Duration of management system certification audits is defined as that part of audit time spent conducting audit activities from the opening meeting to the closing meeting, inclusive.

The effective number of personnel consists of all personnel involved within the scope of certification including those working on each shift. When included within the scope of certification, it shall

also include non-permanent (e.g. contractors) and part-time personnel. Dependent upon the hours worked, part-time personnel numbers and employees partially in scope may be reduced or increased and converted to an equivalent number of full time personnel. When a high percentage of personnel perform activities or roles which are considered repetitive, a reduction to the number of personnel, which is coherent and applied consistently on a client to client basis within the scope of certification, is permitted.

9.1.4.2 SM9.1.4.2 Adjustments to audit time

All attributes of the client's SMS and the services shall be considered and adjustments made to the initial audit time for those factors that could justify more or less time. Regardless of the adjustment factors, the certification body shall ensure that sufficient audit time is allocated to accomplish a complete and effective audit of the client's SMS. The certification body shall document and be able to justify a decrease or increase in audit time.

Tables 2 and 3 show how relevant factors can affect the audit times in Table 1. A shift means handovers and interfaces across multiple locations and/or teams operating in consecutive work periods.

The maximum reduction shall be 30 % of the Table 1 audit time.

Table 2 — Factors which can decrease audit time

	Potential decrease factors
1	A low rate of change to the SMS and the services.
2	Previously demonstrated effective performance of the SMS, e.g. previously certified with another accredited certification body.
3	Combined audit of the SMS with one or more other relevant management systems.
4	Prior knowledge of the organization, e.g. already certified to another standard by the same certification body.
5	A single, simple service.
6	Identical activities performed on all shifts, with appropriate evidence of equivalent performance on all shifts, e.g. service desk.
7	A significant proportion of service management personnel carry out a similar simple function.
8	Single site with low number of personnel.
9	A low level of reliance on other parties, such as suppliers, internal groups or customers acting as suppliers, involved in the provision of services.

Table 3 — Factors which can increase audit time

Potential increase factors	
1	Complicated logistics involving multi-jurisdiction, multi-site working, in the same, or across a number of, time zone(s).
2	Complexity of language differences across different locations, e.g. personnel speaking in more than one language (requiring interpreter(s) or preventing individual auditors from working independently).
3	Large size or complexity of the SMS scope, e.g. high number of services, personnel or locations, specialized services which are difficult to understand and maintain.
4	High degree of legal and regulatory requirements affecting the client's SMS, e.g. intellectual property rights, privacy, food, drug, aerospace, nuclear.
5	Different activities done in different shifts.
6	Temporary sites within the scope of the SMS for a specific audit.
7	Complex business processes performed within the scope of the SMS.
8	A high level of reliance on other parties, such as suppliers, internal groups or customers acting as suppliers, involved in the provision of services.
9	Frequent addition of new services, removal of services, transfer of services or significant changes to services.

9.1.4.3 SM9.1.4.3 Adjustments for other management system standard certifications

If the client is certified under other relevant management system standard(s), e.g. ISO 9001 and/or ISO/IEC 27001, the certification body may decrease the initial audit time.

A decrease in audit time, due to certification against other relevant management system standards, shall only be permitted under the following conditions:

a) the other management system standard is relevant to the SMS to be audited;

b) any existing certificate is current and has been audited by an accredited certification body at least once in the last 12 months;

c) the scope of the other certification(s), is the same as, or greater than, that defined for the ISO/IEC 20000-1 certification.

The amount of reduction of the audit time shall be dependent on the extent to which the client's management system is integrated with the other management system(s).

Regardless of other relevant management systems standards, the certification body shall ensure that sufficient time is allocated to accomplish a complete and effective audit of the client's SMS.

NOTE When two or more management systems of different disciplines are audited together, this is termed a "combined audit". Where these systems are integrated into a single management system, the principles and procedures for auditing are the same as for a combined audit.

9.1.4.4 SM9.1.4.4 Determining audit time for surveillance and recertification audits

The time needed to conduct surveillance and recertification audits shall be calculated using the following factors:

a) the audit duration shall not be less than 80 % of the total audit time;

b) surveillance audits shall be a minimum of one third of the audit time for the initial audit annually, whether performed in a single audit or more;

c) recertification audits shall be a minimum of two thirds of the audit time for the initial audit;

d) the minimum audit time for surveillance audits, after adjustment, shall be 1 d;

e) the minimum audit time for recertification audits, after adjustment, shall be 2 d.

9.1.4.5 SM9.1.4.5 Remote auditing

Audits which are not performed face-to-face in the same location but are executed from another location are called remote audits. The audit plan shall identify the remote auditing techniques that will be utilized during the audit.

The acceptable and unacceptable use of remote audits is specified in Table 4. The certification body shall not use the unacceptable practices in Table 4 and may use the acceptable practices.

Remote audits shall not reduce the audit time below that which is calculated from Table 1, with appropriate adjustments.

If the certification body develops an audit plan for which the remote auditing activities represent more than 30 % of the planned on-site audit time, the certification body shall document the justification.

Table 4 — Acceptable and unacceptable remote audit practices

Acceptable	
1	Teleconferencing: video and audio, web meeting, interactive web-based communications.
2	Remote access to tools used to support the SMS.
3	Remote access to the library of SMS documents and records.
Unacceptable	
4	Reliance on documentation only.
5	Assumption that all locations function identically without supporting evidence for the assumption.
6	Audits conducted without interviewing personnel.

NOTE On-site audit time refers to the on-site audit time allocated for individual sites. Electronic audits of remote sites are considered to be remote audits, even if the electronic audits are physically carried out on one of the client's premises.

9.1.5 Multi-site sampling

The requirements in ISO/IEC 17021-1:2015, 9.1.5 apply. In addition, the following requirements and guidance apply.

9.1.5.1 SM9.1.5.1 Criteria for multi-site sampling

If a client has a number of locations, certification bodies may use a sample-based approach to multi-site certification audits if all locations are:

a) operating under the same SMS, which is centrally administered;

b) included within the client's internal audit programme;

c) included within the client's management review programme.

9.1.6 Multiple management systems standards

The requirements in ISO/IEC 17021-1:2015, 9.1.6 apply. In addition, the following requirements and guidance apply.

9.1.6.1 SM9.1.6.1 Combining management system audits

An SMS audit can be combined with audits of other management systems. A combined or integrated audit shall ensure that the audit evidence fulfils the requirements specified in ISO/IEC 20000-1 within

the scope of the audit. All findings relating to ISO/IEC 20000-1 shall be easily identifiable in audit reports.

The integrity of the ISO/IEC 20000-1 audit shall not be adversely affected by the combination of audits.

9.1.6.2 SM9.1.6.2 Combining management system audits for ISO/IEC 20000-1 and ISO/IEC **27001**

Where an audit is combined for ISO/IEC 27001 and ISO/IEC 20000-1, the information security management process in ISO/IEC 20000-1 shall be audited to ensure that:

a) the information security policy is relevant to the SMS and the services;

b) relevant information security risks are identified and information security controls are implemented to support the SMS and the services.

The auditor may find some supporting evidence from the information security management system (ISMS).

If the scope of the ISMS is outside of the scope of the SMS, then the information security management process in ISO/IEC 20000-1 shall be audited as a standalone process without the support of the ISMS.

The information security policy, risks and controls shall be audited to ensure that they are appropriate for the services within the scope of the client's SMS.

9.2 Planning audits

9.2.1 Determining audit objectives, scope and criteria

The requirements in ISO/IEC 17021-1:2015, 9.2.1 apply. In addition, the following requirements and guidance apply.

9.2.1.1 SM9.2.1.1 Determining audit objectives

The audit objectives shall include checking that interfaces at the boundaries of the SMS with other parties participating in the activities of the SMS, are identified and controlled. The certification body shall also ensure that the client is aware of and managing any risks to the SMS and the services arising from the interfaces.

9.2.2 Audit team selection and assignments

The requirements in ISO/IEC 17021-1:2015, 9.2.2 apply.

9.2.3 Audit plan

The requirements in ISO/IEC 17021-1:2015, 9.2.3 apply. In addition the following requirements and guidance apply.

9.2.3.1 SM9.2.3.1 Sampling accuracy

The certification body shall have procedures in place to ensure the following:

a) an adequate level of sampling shall be determined at initial contract review, and subsequent audit activities, identifying differences between the following:

   1) locations, e.g. site sizes or use of temporary sites which are covered by the SMS but are not in the scope of certification;

   2) services;

   3) customers;

4) other parties (internal groups, suppliers, customers acting as a supplier) involved in the provision of services;

5) languages;

6) consistency of approach across all shifts. A client with a high proportion of personnel working in shifts can be audited in less time if each shift operates in the same way. This involves a review of records to confirm the consistency of approach across all shifts. If shifts are consistent, all shifts can be treated as one set of activities and one shift can be used as the sample for audit;

7) local variations of the SMS;

8) legal and regulatory requirements;

b) a representative sample shall be selected from the scope of the client's SMS. The selection shall be based upon the judgement of the certification body, reflecting the factors presented in a), as well as a random element;

c) the design of the audit plan shall take into consideration the requirements in a) and b). The plan shall cover representative samples of the full scope of the SMS within the three-year period between certification audits.

9.3 Initial certification

The requirements in ISO/IEC 17021-1:2015, 9.3 apply. In addition, the following requirements and guidance apply.

9.3.1 SM9.3.1 Identification of other parties

The certification body shall have access to evidence of the identification of other parties involved in the provision of services for the client and how they are controlled as specified in ISO/IEC 20000-1.

9.3.2 SM9.3.2 Integration of SMS documentation with that for other management systems

The certification body shall take into account that the client can integrate the documentation for the SMS with that for other management systems, e.g. a quality management system or information security management system.

If the documentation for multiple management systems is combined, the client's SMS shall be clearly identified.

9.4 Conducting audits

9.4.1 General

The requirements in ISO/IEC 17021-1:2015, 9.4.1 apply.

9.4.2 Conducting the opening meeting

The requirements in ISO/IEC 17021-1:2015, 9.4.2 apply.

9.4.3 Communication during the audit

The requirements in ISO/IEC 17021-1:2015, 9.4.3 apply.

9.4.4 Obtaining and verifying information

The requirements in ISO/IEC 17021-1:2015, 9.4.4 apply.

