ADDITIONAL RULES FOR THECERTIFICATION OF INFORMATION TECHNOLOGY - SERVICE MANAGEMENT SYSTEMS (SMS)

Original Copy

Revision Register:

Date	Edit.	Rev.	Edit for	Issued	Approved
01/09/2020	1	0	First emission	RSG	AMM
03/06/2024	1	1	Integration Requirements ISO 20000-1	RSG	AMM

Distribution	*Signature:* 
☑Verified copy	
☐Unverified copy	

1. GENERAL

The present Rules define the additional procedures, not as substitute, applied by QS for certification of information technology - service management systems in comparison to what is already defined in the QS General Rules for the certification of Management Systems, latest version in force.

QS issues the certification in accordance with requirements of standard ISO/IEC 17021-1:2015 and ISO/IEC 20000-6:2017 to Organizations whose Management System has been recognized in accordance with the requirementsISO/IEC 20000-1:2018.

In addition, upon request, QS can carry out conformity assessments of a company Management System according to other normative documents of reference and, if appropriate, issue the certifications (e.g. ISO/IEC 27001, ISO/IEC 27010, ISO 22301:2012).

In addition; ISO/IEC 20000-1:2018/Amd 1:2024, requires organisations to actively assess and address the implications of climate change in their operations and strategic planning.

For such cases should also be considered any specific rules of QS.

1.1 APPLICATION

A SMS supports the management of the service lifecycle, including the planning, design, transition, delivery and improvement of services, which meet agreed requirements and deliver value for customers, users and the organization delivering the services.

The standard ISO 20000-1 is intended to be applicable to all organizations, regardless of the organization's type or size, or the nature of the services delivered. Exclusion of any of the requirements (in Clauses4 to 10) is not acceptable when the organization claims conformity to this document, irrespective of the nature of the organization.

The organization in the scope of the SMS can be part of a larger organization, for example, a department of a large corporation. An organization or part of an organization that manages and delivers a service or services to internal or external customers can also be known as a service provider.

QS do not provide internal service management reviews of the client’s SMSsubject to certification. QS, according its own policy , is a third part body, independent of the body or bodies (including anyindividuals) which provide the internal SMS audit.

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.

1.2 TERMS AND DEFINITIONS

For all the terms and definitions please refer to reference applicable standards (point 2 of this document)

Asset:item, thing or entity that has potential or actual value to an organization.

Note 1: Value can be tangible or intangible, financial or non-financial, and includes consideration of risks and liabilities. It can be positive or negative at different stages of the asset life.

Note 2: Physical assets usually refer to equipment, inventory and properties owned by the organization. Physical assets are the opposite of intangible assets, which are non-physical assets such as leases, brands, digital assets, use rights, licenses, intellectual property rights, reputation or agreements.

Note 3: A grouping of assets referred to as an asset system could also be considered as an asset. Note 4 to entry: An asset can also be a configuration item. Some configuration items are not assets.

Configuration item(CI): element that needs to be controlled in order to deliver a service or services

Effectiveness: extent to which planned activities are realized and planned results achieved

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 or user

information security incident single or a series of unwanted or unexpected information security (3.2.6) events that have a significant probability of compromising business operations and threatening information security

Interested party: person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity related to the SMS or the services

Interested parties can include parts of the organization outside the scope of the SMS, customers (3.2.3), users (3.2.28), community, external suppliers (3.2.4), regulators, public sector bodies, nongovernment organizations, investors or employees

Organization: person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives (3.1.13)

Note 1: The concept of organization includes, but is not limited to sole-trader, company, corporation, firm. enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

Note 2: An organization or part of an organization that manages and delivers a service or services to internal or external customers can be known as a service provider.

Note 3: If the scope of the SMS covers only part of an organization, then organization, when used in this document, refers to the part of the organization that is within the scope of the SMS. Any use of the term organization with a different intent is distinguished clearly.

Service: means of delivering value for the customer by facilitating outcomes the customer wants to achieve

Note 1 to entry: Service is generally intangible.

Note 2 to entry: The term service as used in the ISO 20000-1 means the service or services in the scope of the SMS. Any use of the term service with a different intent is distinguished clearly.

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

Note 1 to entry: Service availability can be expressed as a ratio or percentage of the time that the service or service component is actually available for use compared to the agreed time.

Service catalogue documented information about services that an organization provides to its customers

service component part of a service) that when combined with other elements will deliver a complete service e.g Infrastructure, applications, documentation, licences, information, resources, supporting services.

Note 1 to entry: A service component can include configuration items , assets or other elements. service continuity capability to deliver a service without interruption, or with consistent availability as agreed

Note 1 to entry: Service continuity management can be a subset of business continuity management. ISO 22301 is a management system standard for business continuity management.

Service level agreement SLA documented agreement between the organization (3.1.14) and the customer (3.2.3) that identifies services (3.2.15) and their agreed performance Note 1 to entry: A service level agreement can also be established between the organization and an external supplier (3.2.4), an internal supplier (3.2.8) or a customer acting as a supplier.

Service management: set of capabilities and processes to direct and control the organization's activities and resources for the planning, design, transition, delivery and improvement of services to deliver value

1.2.1 ACRONYMS:

- CI: Configuration Item

-**SLA:** Service level agreement

- SMS : Service Management System

2. REFERENCE STANDARD/REQUIREMENTS FOR CERTIFICATION

To get certification by QS, a ISMS meet initially and over time the requirements of ISO 20000-1 last version in force and the additional ones required by Accreditation Bodies.

The applicable regulations as reference for SMS certification, in addition to the basic standards already defined in the QS general rules and QS Manual, are:

- ISO/IEC 20000-1:2018Information technology — Service management — Part 1: Service management system requirements
- ISO/IEC 20000-6:2017Information technology — Service management — Part 6: Requirements for bodies providing audit and certification of service management systems
- ISO/IEC 20000-2:2019/Amd 1:2020Information technology — Service management — Part 2: Guidance on the application of service management systems
- ISO/IEC 20000-10:2018Information technology — Service management — Part 10: Concepts and vocabulary
- ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary
- ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements
- ISO/IEC 19770-1:2017Information technology — IT asset management — Part 1: IT asset management systems — Requirements
- ISO/IEC 19770-5:2015Information technology — IT asset management — Part 5: Overview and vocabulary
- ISO 31000:2018 Risk management — Guidelines

3. CERTIFICATION PROCEDURE

To start the certification procedure, the company shall:

- have an operating management system in accordance with ISO/IEC 20000-1:2018 at any particular requirements established for types of process/service;
- describe this system in specific documented information
- have made at least one cycle of internal audits and one management review that covers the purpose of SMS Certification

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.

In addition to what is established by point 10 of the QS General Rules, together with the certification application form, or immediately later, the Organization shall provide the following documentation to QS:

- Locations, sites size
- Type of services
- Customers

- Other parties involved in the provision of services (internal groups, suppliers, customers acting as a supplier)
- If the audit shall be provided in several language
- Shifts of personnel
- legal and regulatory requirements

QS will 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.

During of the certification process, the organization shall keep in consideration the following particular provisions and requirements:

The standard lists in sections from 4 to 10 (included) a series of mandatory requirements for SMS, which cannot be subject to exclusion therefore.

In addition to what is established in the QS General Rules, the company shall communicate to QS:

- any confidential or particular information that may not be available during the audit being not authorized to communicate them to third parties (es. mandatory law). (QS reserves the right to assess whether the system can be verified properly even without the availability of such data. If QS will consider that this situation may affect the efficiency of the audit, QS will try to reach an agreement with the Organization; If the agreement will be not reached, the certification process cannot be started. Such an agreement may consist in the fact that the Organization authorize the audit team to access information, confidential or sensitive data, only for the time of the audit and in accordance with specified arrangements)
- any need based on the context and company operating procedures, which some processes/requirements shall be examined through network-assisted auditing techniques (eg. remote access to documented information, web-based interactive communications, teleconferencing, etc.). Using these techniques must be agreed during the audit planning. QS reserves the right not to use such audit techniques in the case that found that may put at risk the efficiency and effectiveness of the audit as well as the integrity of the audit process.
- Before the certification audit is agreed, the client shall report if any SMS documents or records cannot be made available for review by the audit team because they contain confidential or sensitive information. QS will 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, QS will advise the client that an audit cannot take place until appropriate access arrangements are granted

The cost of certification activity is proportional to the number of man-days (m/d) necessary to the evaluation of the SMS and the level of complexity/criticality/risks, sites etc, with reference to ISO/IEC 20000-6 document latestversion in force.

The total number of persons doing work under the organization’s control for all shifts within the scope of the certification is starting point for determination of audit time.

The planning of audits will be decided in consultation with the organization taking into consideration the most appropriate time to assess better the certification scope with an adequate level of sampling (according sites, seasons, local variations, languages, days shifts etc)

4. INTEGRATED AUDITS

QS admits carrying out audits about SMS integrated with other management systems.
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. 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.

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.

5. CERTIFICATION OF "MULTI-SITE" ORGANIZATION

The multi-site sampling approach is considered possible, where organizations that require it operates in different sites but with similar processes and activities under the supervision and coordination of a central entity.

In addition to that specified in the QS General Rules, QS specifies that the multisite sampling is applicable only under the following conditions:
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.

Sampling shall always provide for the assessment of the effectiveness of service controls and responsibilities of leadership the main operative headquarter, plus a sample of sites allowing, in a reasonable period and in any case before recertification, coverage of the entire organization.

The non-conformities found in various sites during the audits, will be subject to a process of improvement applied to all sites of the organization.
The possible persistence of noncompliance, involves the withdrawal of certification to the entire organization, not only at the individual site audited.

6. CERTIFICATION DOCUMENT

The certification documents is issued according requirements of ISO/IEC 17021-1:2015 and guidance ISO/IEC 20000-3 (guidance when defining the scope).
An ISO/IEC 20000-1 certificate would normally be issued to a single entity, rather than a group pf different unrelated legal entity.