

JAPANESE
INDUSTRIAL
STANDARD

Translated and Published by
Japanese Standards Association

JIS Q 20000-1 : 2012

(ISO/IEC 20000-1 : 2011)

(JIPDEC/JSA)

Information technology—Service management—Part 1: Service management system requirements

ICS 03.080.99;35.020

Reference number : JIS Q 20000-1 : 2012 (E)

PROTECTED BY COPYRIGHT

Date of Establishment: 2007-04-20

Date of Revision: 2012-09-20

Date of Public Notice in Official Gazette: 2012-09-20

Investigated by: Japanese Industrial Standards Committee
Standards Board
Committee on Management System Standards

JIS Q 20000-1:2012, First English edition published in 2013-01

Translated and published by: Japanese Standards Association
4-1-24, Akasaka, Minato-ku, Tokyo, 107-8440 JAPAN

In the event of any doubts arising as to the contents,
the original JIS is to be the final authority.

© JSA 2013

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

Printed in Japan

PROTECTED FY COPYRIGHT

Contents

	Page
0.1 Introduction	1
0.2 Service management system requirements	1
1 Scope	2
1.1 General	2
1.2 Application	4
2 Normative references	4
3 Terms and definitions	4
4 Service management system general requirements	10
4.1 Management responsibility	10
4.2 Governance of processes operated by other parties	11
4.3 Documentation management	11
4.4 Resource management	12
4.5 Establish and improve the SMS	13
5 Design and transition of new or changed services	16
5.1 General	16
5.2 Plan new or changed services	17
5.3 Design and development of new or changed services	18
5.4 Transition of new or changed services	18
6 Service delivery processes	19
6.1 Service level management	19
6.2 Service reporting	19
6.3 Service continuity and availability management	20
6.4 Budgeting and accounting for services	21
6.5 Capacity management	21
6.6 Information security management	22
7 Relationship processes	23
7.1 Business relationship management	23
7.2 Supplier management	24
8 Resolution processes	25
8.1 Incident and service request management	25
8.2 Problem management	26
9 Control processes	26
9.1 Configuration management	26
9.2 Change management	27
9.3 Release and deployment management	28

Bibliography	30
--------------------	----

Foreword

This translation has been made based on the original Japanese Industrial Standard revised by the Minister of Economy, Trade and Industry, through deliberations at the Japanese Industrial Standards Committee as the result of proposal for revision of Japanese Industrial Standard submitted by the Japan Institute for Promotion of Digital Economy and Community (JIPDEC)/Japanese Standards Association (JSA) with the draft being attached, based on the provision of Article 12 Clause 1 of the Industrial Standardization Law applicable to the case of revision by the provision of Article 14.

Consequently **JIS Q 20000-1:2007** is replaced with this Standard.

This **JIS** document is protected by the Copyright Law.

Attention is drawn to the possibility that some parts of this Standard may conflict with a patent right, application for a patent after opening to the public or utility model right. The relevant Minister and the Japanese Industrial Standards Committee are not responsible for identifying the patent right, application for a patent after opening to the public or the utility model right.

JIS Q 20000 series consists of the following 2 parts under the general title “*Information technology—Service management*”:

Part 1: Service management system requirements

Part 2: Code of practice

Information technology— Service management—Part 1: Service management system requirements

0.1 Introduction

This Japanese Industrial Standard has been prepared based on the second edition of **ISO/IEC 20000-1** published in 2011 without any modifications of technical contents.

The portions with dotted underlines are the matters not given in the corresponding International Standard.

The information in NOTES in this Standard are guidance on understanding or clarifying the contents of related requirements.

0.2 Service management system requirements

The requirements in this Standard 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 Standard requires an integrated process approach when the service provider plans, establishes, implements, operates, monitors, reviews, maintains and improves a service management system (SMS).

NOTE : The term “service” in this Standard represents “information technology service”.

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 Standard 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 Standard 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 Standard, 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 Standard is based on the PDCA methodology.

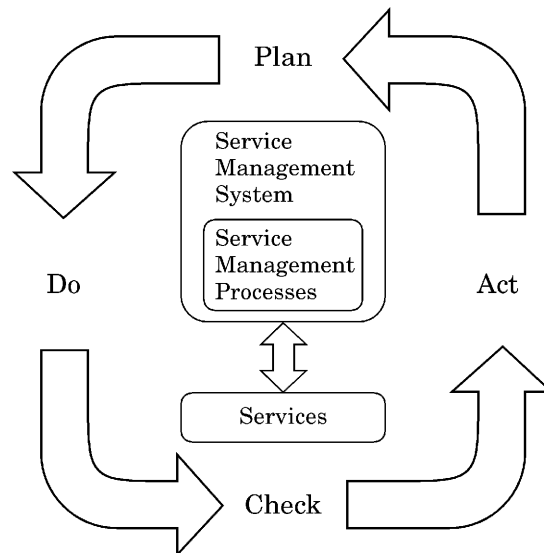


Figure 1 PDCA methodology applied to service management

This Standard 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 **JIS Q 9001** or an information security management system based on **JIS Q 27001:2006**.

This Standard is intentionally independent of specific guidance. The service provider can use a combination of generally accepted guidance and its own experience.

1 Scope

1.1 General

This Standard 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 Standard 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 Standard.

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.

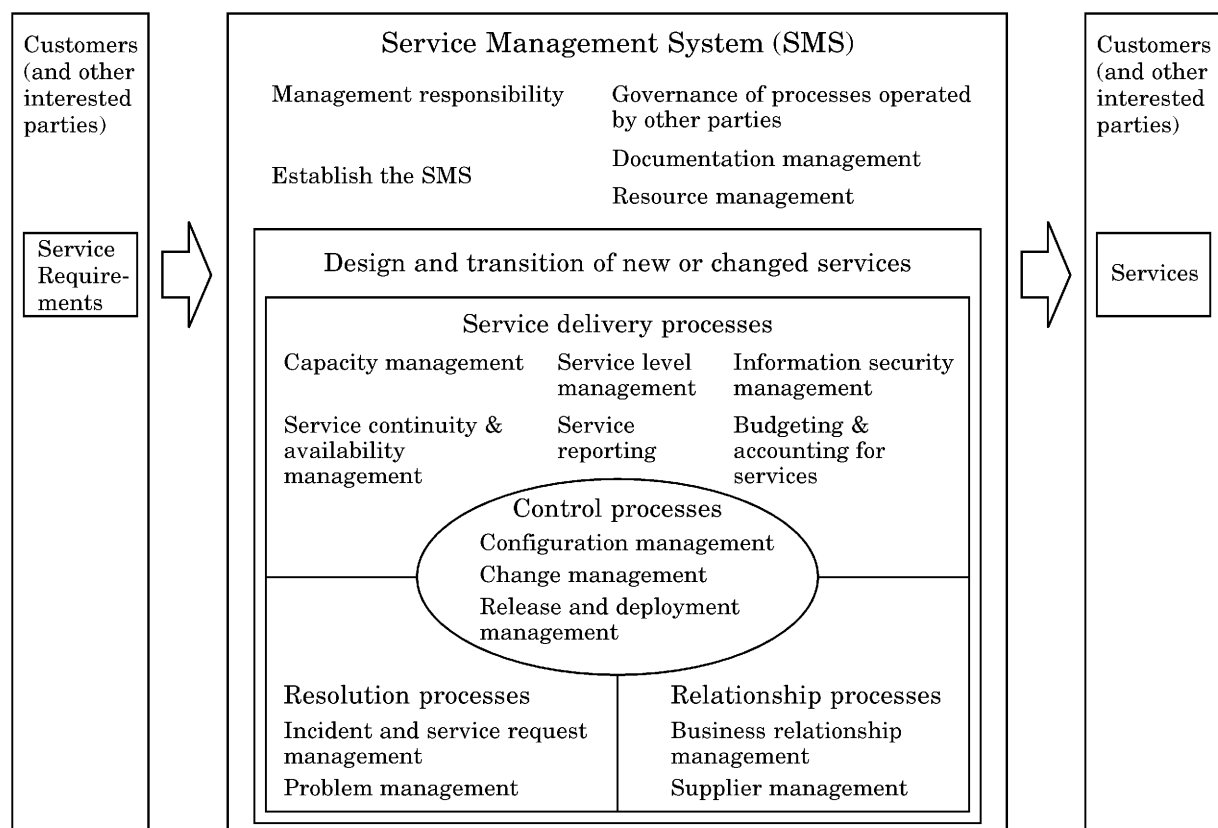


Figure 2 Service management system (SMS)

1.2 Application

All requirements in this Standard 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 Standard, 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 of 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 Standard excludes the specification for a product or tool. However, organizations can use this Standard to help them develop products or tools that support the operation of an SMS.

NOTE 1 The International Standard corresponding to this Standard and the symbol of degree of correspondence are as follows.

ISO/IEC 20000-1:2011 *Information technology—Service management—Part 1: Service management system requirements* (IDT)

In addition, symbols which denote the degree of correspondence in the contents between the relevant International Standard and **JIS** are IDT (identical), MOD (modified), and NEQ (not equivalent) according to **ISO/IEC Guide 21-1**.

NOTE 2 **ISO/IEC TR 20000-3** provides guidance on scope definition and applicability of this Standard. This includes further explanation about the governance of processes operated by other parties.

2 Normative references

No normative references are cited. This clause is included in order to ensure clause numbering is identical with **JIS Q 20000-2** which is to be revised.

3 Terms and definitions

For the purposes of this Standard, 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 **JIS Q 9000:2006**.

3.6 corrective action

action to eliminate the cause or reduce the likelihood of recurrence of a detected non-conformity or other undesirable situation

NOTE : Adapted from **JIS Q 9000:2006**.

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 **JIS Q 9000:2006**.

3.8 document

information and its supporting medium

[**JIS Q 9000:2006**]

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 this Standard, documents, except for records, state the intent to be achieved.

3.9 effectiveness

extent to which planned activities are realized and planned results achieved

[**JIS Q 9000:2006**]

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 Standard which would not be appropriate for this definition.

NOTE 3 The term “accessibility” in the corresponding International Standard has the same meaning as the “availability” used in the definition of “information security” in **JIS Q 27001:2006**.

NOTE 4 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 **JIS Q 9000:2006**.

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

[**JIS Q 9000:2006**]

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.

[JIS Q 9000:2006]

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 JIS Q 9000:2006.

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

[JIS Q 9000:2006]

NOTE : Procedures can be documented or not.

3.21 process

set of interrelated or interacting activities which transforms inputs into outputs

[JIS Q 9000:2006]

3.22 record

document stating results achieved or providing evidence of activities performed

[JIS Q 9000:2006]

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