



JAPANESE
INDUSTRIAL
STANDARD

Translated and Published by
Japanese Standards Association

JIS Q 15001 : 2017

**Personal information protection
management systems—
Requirements**

ICS 35.080

Reference number : JIS Q 15001 : 2017 (E)

PROTECTED BY COPYRIGHT

 **Documents**
Document Sharing Hub
44 S

Date of Establishment: 1999-03-20

Date of Revision: 2017-12-20

Date of Public Notice in Official Gazette: 2017-12-20

Investigated by: Japanese Industrial Standards Committee
Standards Board for IEC area
Technical Committee on Information

JIS Q 15001:2017, First English edition published in 2018-05

Translated and published by: Japanese Standards Association
Mita MT Building, 3-13-12, Mita, Minato-ku, Tokyo, 108-0073 JAPAN

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

© JSA 2018

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 BY COPYRIGHT

Contents

	Page
0 Introduction	1
0.1 Summary	1
0.2 Relevance to other management system standards	1
1 Scope	2
2 Normative references	2
3 Terms and definitions	2
4 Context of the organization	9
4.1 Understanding the organization and its context	9
4.2 Understanding the needs and expectations of interested parties	9
4.3 Determining the scope of the personal information protection management system	9
4.4 Personal information protection management system	10
5 Leadership	10
5.1 Leadership and commitment	10
5.2 Policy	10
5.3 Organizational roles, responsibilities and authorities	11
6 Planning	11
6.1 Actions to address risks and opportunities	11
6.2 Personal information protection objectives and planning to achieve them	13
7 Support	13
7.1 Resources	13
7.2 Competence	14
7.3 Awareness	14
7.4 Communication	14
7.5 Documented information	14
8 Operation	15
8.1 Operational planning and control	15
8.2 Personal information protection risk assessment	16
8.3 Personal information protection risk treatment	16
9 Performance evaluation	16
9.1 Monitoring, measurement, analysis and evaluation	16
9.2 Internal audit	16
9.3 Management review	17
10 Improvement	18
10.1 Nonconformity and corrective action	18

10.2	Continual improvement	18
Annex A (normative)	Control objectives and controls	19
Annex B (informative)	Supplements concerning controls	35
Annex C (informative)	Control objectives and controls regarding safety control measures	64
Annex D (informative)	Tables of correspondence between current and previous editions	78
Bibliography		82

Foreword

This Japanese Industrial Standard has been revised by the Minister of Economy, Trade and Industry, through deliberations at the Japanese Industrial Standards Committee in accordance with the Industrial Standardization Law. Consequently **JIS Q 15001:2006** 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 patent rights, applications for a patent after opening to the public or utility model rights. The relevant Minister and the Japanese Industrial Standards Committee are not responsible for identifying any of such patent rights, applications for a patent after opening to the public or utility model rights.

Personal information protection management systems—Requirements

0 Introduction

This Japanese Industrial Standard was first established in 1999, then revised once (this revised edition hereafter referred to as the previous edition) in 2006. The revision at this time has been made to bring the contents of this Standard into conformance with the revised stipulations in the laws related to protection of personal information.

No corresponding International Standard has been established at this point. Tables of correspondence between this Standard and the previous edition are shown in Annex D.

0.1 Summary

This Standard has been prepared to provide the requirements for establishing, implementing, maintaining and continually improving personal information protection management systems. Adoption of a personal information protection management system is an organizational strategic decision. The establishment and implementation of a personal information protection management system of an organization are affected by the needs and objectives of the organization, the requirements for personal information protection, the process used by the organization, and the size and structure of the organization. All of these factors are expected to change with time.

The personal information protection management system brings a feeling of trust to the interested parties that, by applying a risk management process, personal information protection is maintained and the risks are appropriately controlled.

It is important to regard a personal information protection management system as a part of the whole organizational process and management structure and to incorporate it into the structure, and to take into consideration the personal information protection in designing the processes, information systems and controls. The personal information protection management system is expected to be introduced on a scale matching the needs of the organization.

This Standard may be used by an organization to evaluate internally its own capability of meeting the personal information protection requirements or by external parties to make such evaluation on the organization.

The sequence of the requirements in this Standard neither reflects the order of their importance nor reflects the order of implementation. The list item symbols in this Standard, such as **a)**, **b)** or **1)**, **2)**, are provided only for the purpose of easy reference.

0.2 Relevance to other management system standards

This Standard refers to Annex SL of Consolidated ISO Supplement of ISO/IEC Directives Part 1 for the High Level Structure (HLS), common sub-clause titles, identical core text and common terms and core definitions, thereby ensuring relevance to other management system standards adopting Annex SL.

These common efforts specified in Annex SL are useful for an organization operating two or more management systems.

1 Scope

This Standard specifies the requirements for establishing, implementing, maintaining and improving a personal information protection management system regarding the personal information which the organization uses for its own business. The requirements specified in this Standard are intended to be applicable to all organizations independent of type or size of their businesses. The organizations here mean the personal information handling business operators as specified by the Act on Protection of Personal Information (Act No. 57, 2003) (hereafter referred to as Personal Information Protection Act).

NOTE : The term “business” in “the organization uses for its business” means what is accepted as a business by socially accepted norms and does not necessarily refer to profit-making businesses only. Therefore, personal information of a worker is the information used for the business.

2 Normative references

This Standard has no normative references.

3 Terms and definitions

For the purpose of this Standard, the terms and definitions provided in the Personal Information Protection Act, as well as the following, apply.

3.1 organization

person or group of people containing a responsible and authoritative top management, which has its own functions with responsibilities, authorities and relationships to achieve its objectives (3.8)

3.2 interested party

person or organization (3.1) that can affect, be affected by, or perceive themselves to be affected by a decision or activity

(see 2.41 of JIS Q 27000:2014)

3.3 requirement

need or expectation that is stated explicitly, generally implied or obligatory

(see 2.63 of JIS Q 27000:2014)

NOTE : “Generally implied” means that it is custom or common practice for the organization and interested parties that the need or expectation under consideration is implied.

3.4 management system

set of interrelated or interacting elements of an organization (3.1) to establish policies (3.7) and objectives (3.8) and processes (3.12) to achieve those objectives

NOTE 1 A management system can address a single discipline or several disciplines.

NOTE 2 The system elements include the organization's structure, roles and responsibilities, planning, operation.

3.5 top management

person or group of people who direct and control an organization (3.1) at the highest level

NOTE : Top management has the power to delegate authority and provide resources within the organization.

3.6 effectiveness

extent to which planned activities are realized and planned results achieved

(see 2.24 of JIS Q 27000:2014)

3.7 policy

intentions and direction of an organization (3.1) as formally expressed by its top management (3.5)

(see 2.60 of JIS Q 27000:2014)

3.8 objective

result to be achieved

NOTE 1 An objective can be strategic, tactical, or operational.

NOTE 2 Objectives can relate to different disciplines (such as financial, health and safety, and environmental goals) and can apply at different levels [such as strategic, organization-wide, project, product and process (3.12)].

NOTE 3 An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as a personal information protection objective or by the use of other words with similar meaning (e.g. aim, goal, or target).

NOTE 4 In the context of personal information protection management systems, information protection objectives are set by the organization, consistent with the internal policy for personal information protection, to achieve specific results.

3.9 risk

effect of uncertainty on objectives

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

NOTE 2 Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event (3.28), its consequence (3.24), or likelihood (3.29).

NOTE 3 Risk is often characterized by reference to potential events (3.28) and consequences (3.24), 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 (3.29) of occurrence.

3.10 competence

ability to apply knowledge and skills to achieve intended results

(see **2.11** of **JIS Q 27000:2014**)

3.11 documented information

information required to be controlled and maintained by an organization (**3.1**) and the medium on which it is contained

(see **2.23** of **JIS Q 27000:2014**)

NOTE 1 Documented information can be in any format and media and from any source.

NOTE 2 Documented information can refer to

- the management system (**3.4**), including related processes (**3.12**);
- information created in order for the organization to operate (documentation);
- evidence of results achieved (records).

3.12 process

set of interrelated or interacting activities which transforms inputs into outputs

(see **2.61** of **JIS Q 27000:2014**)

3.13 performance

measurable result

(see **2.59** of **JIS Q 27000:2014**)

NOTE 1 Performance can relate either to quantitative or qualitative findings.

NOTE 2 Performance can relate to the management of activities, processes (**3.12**), products (including services), systems or organizations (**3.1**).

3.14 monitoring

determining the status of a system, a process (**3.12**) or an activity

(see **2.52** of **JIS Q 27000:2014**)

NOTE : To determine the status, there may be a need to check, supervise or critically observe.

3.15 measurement

process (**3.12**) to determine a value

3.16 audit

systematic, independent and documented process (**3.12**) for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

(see **2.5** of **JIS Q 27000:2014**)

NOTE 1 An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines).

NOTE 2 “Audit evidence” and “audit criteria” are defined in **JIS Q 19011**.

3.17 conformity

fulfilment of a requirement (**3.3**)

(see **2.13** of **JIS Q 27000:2014**)

3.18 nonconformity

non-fulfilment of a requirement (**3.3**)

(see **2.53** of **JIS Q 27000:2014**)

3.19 corrective action

action to eliminate the cause of a nonconformity (**3.18**) and to prevent recurrence

(see **2.19** of **JIS Q 27000:2014**)

3.20 continual improvement

recurring activity to enhance performance (**3.13**)

(see **2.15** of **JIS Q 27000:2014**)

3.21 analytical model

algorithm or calculation combining one or more base measures (**3.23**) and/or derived measures (**3.27**) with associated decision criteria

(see **2.2** of **JIS Q 27000:2014**)

3.22 attribute

property or characteristic of an object (**3.33**) that can be distinguished quantitatively or qualitatively by human or automated means

(see **2.4** of **JIS Q 27000:2014**)

3.23 base measure

measure (**3.30**) defined in terms of an attribute (**3.22**) and the method for quantifying it

(see **2.10** of **JIS Q 27000:2014**)

NOTE : A base measure is functionally independent of other measures.

3.24 consequence

outcome of an event (**3.28**) affecting objectives (**3.8**)

(see **2.14** of **JIS Q 27000:2014**)

NOTE 1 An event can lead to a range of consequences.

NOTE 2 A consequence can be certain or uncertain and in the context of personal information protection is usually negative.

NOTE 3 Consequences can be expressed qualitatively or quantitatively.

NOTE 4 Initial consequences can escalate through knock-on effects.

3.25 control

measure that is modifying risk (**3.9**)

(see **2.16** of **JIS Q 27000:2014**)

NOTE 1 Controls include any process, policy, device, practice, or other actions which modify risk.

NOTE 2 Controls may not always exert the intended or assumed modifying effect.

3.26 decision criteria

thresholds, targets, or patterns used to determine the need for action or further investigation, or to describe the level of confidence in a given result

(see **2.21** of **JIS Q 27000:2014**)

3.27 derived measure

measure (**3.30**) that is defined as a function of two or more values of base measures (**3.23**)

(see **2.22** of **JIS Q 27000:2014**)

3.28 event

occurrence or change of a particular set of circumstances

(see **2.25** of **JIS Q 27000:2014**)

NOTE 1 An event can be one or more occurrences, and can have several causes.

NOTE 2 An event can consist of something not happening.

NOTE 3 An event can sometimes be referred to as an “incident” or “accident”.

3.29 likelihood

chance of something happening

(see **2.45** of **JIS Q 27000:2014**)

3.30 measure

variable to which a value is assigned as the result of measurement (**3.15**)

(see **2.47** of **JIS Q 27000:2014**)

NOTE : The term “measures” is used to refer collectively to base measures, derived measures, and indicators.

3.31 measurement function

algorithm or calculation performed to combine two or more base measures (**3.23**)

(see **2.49** of **JIS Q 27000:2014**)

3.32 measurement method

logical sequence of operations, described generically, used in quantifying an attribute (**3.22**) with respect to a specified scale (**3.34**)

(see **2.50** of **JIS Q 27000:2014**)

NOTE : The type of measurement method depends on the nature of the operations used to quantify an attribute. Two types can be distinguished as follows:

- **subjective**: quantification involving human judgment;
- **objective**: quantification based on numerical rules.

3.33 object

item characterized through the measurement (3.15) of its attributes (3.22)

(see 2.55 of JIS Q 27000:2014)

3.34 scale

ordered set of values, continuous or discrete, or a set of categories to which the attribute (3.22) is mapped

(see 2.80 of JIS Q 27000:2014)

NOTE : The type of scale depends on the nature of the relationship between values on the scale. Four types of scale are commonly defined as follows:

- **nominal**: the measurement values are categorical;
- **ordinal**: the measurement values are rankings;
- **interval**: the measurement values have equal distances corresponding to equal quantities of the attribute;
- **ratio**: the measurement values have equal distances corresponding to equal quantities of the attribute, where the value of zero corresponds to none of the attribute.

These are just examples of the types of scale.

3.35 threat

potential cause of an unwanted incident, which may result in harm to a system or organization

(see 2.83 of JIS Q 27000:2014)

3.36 vulnerability

weakness of an asset or control (3.25) that can be exploited by one or more threats (3.35)

(see 2.89 of JIS Q 27000:2014)

3.37 residual risk

risk (3.9) remaining after risk treatment (3.38)

(see 2.64 of JIS Q 27000:2014)

NOTE 1 Residual risk can contain unidentified risk.

NOTE 2 Residual risk can also be known as “retained risk”.

3.38 risk treatment

process (3.12) to modify risk (3.9)

(see 2.79 of JIS Q 27000:2014)

NOTE 1 Risk treatment can involve the following:

- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- taking or increasing risk in order to pursue an opportunity;
- removing the risk source;
- changing the likelihood;
- changing the consequences;
- sharing the risk with another party or parties (including contracts and risk financing);
- retaining the risk by informed choice.

NOTE 2 Risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention” and “risk reduction”.

NOTE 3 Risk treatment can create new risks or modify existing risks.

3.39 principal

a specific individual identifiable by personal information

3.40 personal information protection manager

a person designated by the top management within the business entity, who has the responsibility and authority to implement and operate a personal information protection management system

NOTE : “Personal information protection manager” is responsible for the entire matters relating to handling of personal information, covering the security control aspects as well as overall organizational management.

3.41 personal information protection auditor

a person designated by the top management within the business entity who is in an equitable and objective position and has the responsibility and authority to conduct and report audits

3.42 worker

person who is engaged in the organizational business of a personal information handling business operator under its direct or indirect instructions and supervision, including employees (regular employees, contract employees, temporary employees, part-time employees, short-term employees, etc.) who are in employment relations with that organization as well as those who are not (board members, executive officers, trustees, corporate auditors, auditor-secretaries, temporary dispatch workers, etc.)

3.43 personal information protection risk

undesirable effects in different aspects of handling personal information (a series of steps in handling of the personal information, from acquisition and input, transfer and transmission, use and processing, storage and backup, and up to erasure and disposal), such

as leakage, loss or damage of personal information, violation of relevant laws and regulations, guidelines and other codes stipulated by the State, assumed economical disadvantages and loss of social credibility, and infringement of the principal's rights and interests

3.44 emergency

situation where one or more threats (**3.35**) of personal information protection risk (**3.43**) has/have actualized

3.45 personal information protection

protection of personal information implemented by an organization which uses the information for its business, while taking into consideration the usefulness of the personal information and the individuals' rights and interests

3.46 risk owner

person or entity with the accountability and authority to manage a risk (**3.9**)
(see **2.78** of **JIS Q 27000:2014**)

4 Context of the organization

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its personal information protection management system.

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

- a) interested parties that are relevant to the personal information protection management system; and
- b) the requirements of these interested parties relevant to information protection.

NOTE : The requirements of interested parties may include legal and regulatory requirements and contractual obligations.

4.3 Determining the scope of the personal information protection management system

The organization shall determine the boundaries and applicability of the personal information protection management system to establish its scope.

When determining this scope, the organization shall consider:

- a) the external and internal issues referred to in **4.1**;
- b) the requirements referred to in **4.2**; and
- c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.

The scope shall be available as documented information.

4.4 Personal information protection management system

The organization shall establish, implement, maintain and continually improve an personal information protection management system, in accordance with the requirements of this Standard.

5 Leadership

5.1 Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the personal information protection management system by:

- a) ensuring the internal policy for personal information protection and the personal information protection objectives are established and are compatible with the strategic direction of the organization;
- b) ensuring the integration of the personal information protection management system requirements into the organization's processes;
- c) ensuring that the resources needed for the personal information protection management system are available;
- d) communicating the importance of effective personal information protection management and of conforming to the personal information protection management system requirements to the interested parties;
- e) ensuring that the personal information protection management system achieves its intended outcome(s);
- f) directing and supporting persons to contribute to the effectiveness of the personal information protection management system;
- g) promoting continual improvement; and
- h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

5.2 Policy

5.2.1 Internal policy for personal information protection

Top management shall establish an internal policy for personal information protection that:

- a) is appropriate to the purpose of the organization;
- b) includes personal information protection objectives (see **6.2**) or provides the framework for setting personal information protection objectives;
- c) includes a commitment to satisfy applicable requirements related to personal information protection; and
- d) includes a commitment to continual improvement of the personal information protection management system.

The internal policy for personal information protection shall:

- e) be available as documented information;
- f) be communicated within the organization; and
- g) be available to interested parties, as appropriate.

5.2.2 Outward policy for personal information protection

Top management shall document and make accessible to public the outward policy for personal information protection that:

- a) is not inconsistent with the internal policy for personal information protection established in accordance with **5.2.1**.

5.3 Organizational roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for roles relevant to personal information protection are assigned and communicated to the interested parties.

Top management shall assign the responsibility and authority for:

- a) ensuring that the personal information protection management system conforms to the requirements of this Standard; and
- b) reporting on the performance of the personal information protection management system to top management.

NOTE : Top management may also assign responsibilities and authorities for reporting performance of the personal information protection management system within the organization.

6 Planning

6.1 Actions to address risks and opportunities

6.1.1 General

When planning for the personal information protection management system, the organization shall consider the issues referred to in **4.1** and the requirements referred to in **4.2** and determine the risks and opportunities that need to be addressed to:

- a) ensure the personal information protection management system can achieve its intended outcome(s);
- b) prevent, or reduce, undesired effects; and
- c) achieve continual improvement.

The organization shall plan:

- d) actions to address these risks and opportunities; and
- e) how to
 - 1) integrate and implement the actions into its personal information protection management system processes; and
 - 2) evaluate the effectiveness of these actions.

6.1.2 Personal information protection risk assessment

The organization shall define and apply an personal information protection risk assessment process that:

- a) establishes and maintains personal information protection risk criteria that include:
 - 1) the risk acceptance criteria; and
 - 2) criteria for implementing personal information protection risk assessments;
- b) ensures that repeated personal information protection risk assessments produce consistent, valid and comparable results;
- c) specifies the personal information protection risks:
 - 1) apply the personal information protection risk assessment process to identify risks associated with inappropriate handling of personal information within the scope of the personal information protection management system; and
 - 2) specify the risk owners;
- d) analyses the personal information protection risks:
 - 1) assess the potential consequences that would result if the risks identified in **6.1.2 c) 1)** were to materialize;
 - 2) assess the realistic likelihood of the occurrence of the risks identified in **6.1.2 c) 1)**; and
 - 3) determine the levels of risk;
- e) evaluates the personal information protection risks:
 - 1) compare the results of risk analysis with the risk criteria established in **6.1.2 a)**; and
 - 2) prioritize the analysed risks for risk treatment.

The organization shall retain documented information about the personal information protection risk assessment process.

6.1.3 Personal information protection risk treatment

The organization shall define and apply an personal information protection risk treatment process to:

- a) select appropriate personal information protection risk treatment options, taking account of the risk assessment results;
- b) determine all controls that are necessary to implement the personal information protection risk treatment option(s) chosen;

NOTE : Organizations can design controls as required, or specify them from any source.

- c) compare the controls determined in **6.1.3 b)** above with those in Annex A and verify that no necessary controls have been omitted;

NOTE 1 Annex A contains a comprehensive list of control objectives and controls. Users of this Standard are directed to Annex A to ensure that no necessary controls are overlooked.

NOTE 2 Control objectives are implicitly included in the controls chosen. The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may be needed.

- d) plan personal information protection risk treatment;
- e) obtain risk owners' approval of the personal information protection risk treatment plan and acceptance of the residual information protection risks.

The organization shall retain documented information about the personal information protection risk treatment process.

NOTE : The personal information protection risk assessment and treatment process in this Standard aligns with the principles and generic guidelines provided in **JIS Q 31000**.

6.2 Personal information protection objectives and planning to achieve them

The organization shall establish personal information protection objectives at relevant functions and levels.

The personal information protection objectives shall:

- a) be consistent with the internal policy for personal information protection;
- b) be measurable (if practicable);
- c) take into account applicable personal information protection requirements, and results from risk assessment and risk treatment;
- d) be communicated; and
- e) be updated as appropriate.

The organization shall retain documented information on the personal information protection objectives.

When planning how to achieve its personal information protection objectives, the organization shall determine:

- f) what will be done;
- g) what resources will be required;
- h) who will be responsible;
- i) when it will be completed; and
- j) how the results will be evaluated.

7 Support

7.1 Resources

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the personal information protection management system.

7.2 Competence

The organization shall:

- a) determine the necessary competence of person(s) doing work under its control that affects its personal information protection performance;
- b) ensure that these persons are competent on the basis of appropriate education, training, or experience;
- c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and
- d) retain appropriate documented information as evidence of competence.

NOTE : Applicable actions may include, for example, the provision of training to, the mentoring of, or the re-assignment of currently employed persons; or the hiring or contracting of competent persons.

7.3 Awareness

Persons doing work under the organization's control shall be aware of:

- a) the internal and outward policies for personal information protection;
- b) their contribution to the effectiveness of the personal information protection management system, including the benefits of improved personal information protection performance; and
- c) the implications of not conforming with the personal information protection management system requirements.

7.4 Communication

The organization shall determine the need for internal and external communications relevant to the personal information protection management system, including:

- a) on what to communicate;
- b) when to communicate;
- c) with whom to communicate;
- d) who shall communicate; and
- e) the processes by which communication shall be effected.

7.5 Documented information

7.5.1 General

The organization's personal information protection management system shall include:

- a) documented information required by this Standard; and
- b) documented information determined by the organization as being necessary for the effectiveness of the personal information protection management system.

NOTE : The extent of documented information for a personal information protection management system can differ from one organization to another due to:

- 1) the size of organization and its type of activities, processes, products and services;
- 2) the complexity of processes and their interactions; and
- 3) the competence of persons.

7.5.2 Creating and updating

When creating and updating documented information the organization shall ensure appropriate:

- a) identification and description (e.g. a title, date, author, or reference number);
- b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and
- c) review and approval for suitability and adequacy.

7.5.3 Control of documented information

Documented information required by the personal information protection management system and by this Standard shall be controlled to ensure:

- a) it is available and suitable for use, where and when it is needed; and
- b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

For the control of documented information, the organization shall address the following activities, as applicable:

- c) distribution, access, retrieval and use;
- d) storage and preservation, including the preservation of legibility;
- e) control of changes (e.g. version control); and
- f) retention and disposition.

Documented information of external origin, determined by the organization to be necessary for the planning and operation of the personal information protection management system, shall be specified as appropriate, and controlled.

NOTE : Access implies a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.

8 Operation

8.1 Operational planning and control

The organization shall plan, implement and control the processes needed to meet personal information protection requirements, and to implement the actions determined in **6.1**. The organization shall also implement plans to achieve personal information protection objectives determined in **6.2**.

The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that outsourced processes are determined and controlled.

8.2 Personal information protection risk assessment

The organization shall perform personal information protection risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in **6.1.2 a)**.

The organization shall retain documented information about the personal information protection risk assessment process.

8.3 Personal information protection risk treatment

The organization shall implement the personal information protection risk treatment plan.

The organization shall retain documented information about the results of the personal information protection risk treatment.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

The organization shall evaluate the personal information protection performance and the effectiveness of the personal information protection management system.

The organization shall determine:

- a) what needs to be monitored and measured, including personal information protection processes and controls;
- b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;

NOTE : The methods selected should produce comparable and reproducible results to be considered valid.

- c) when the monitoring and measuring shall be performed;
- d) who shall monitor and measure;
- e) when the results from monitoring and measurement shall be analysed and evaluated; and
- f) who shall analyse and evaluate these results.

The organization shall retain appropriate documented information as evidence of the monitoring and measurement results.

9.2 Internal audit

The organization shall conduct internal audits at planned intervals to provide information on whether the personal information protection management system

- a) conforms to
 - 1) the organization's own requirements for its personal information protection management system; and
 - 2) the requirements of this Standard;
- b) is effectively implemented and maintained.

The organization shall:

- c) plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits;
- d) define the audit criteria and scope for each audit;
- e) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;
- f) ensure that the results of the audits are reported to relevant management; and
- g) retain documented information as evidence of the audit programme(s) and the audit results.

9.3 Management review

Top management shall review the organization's personal information protection management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

The management review shall include consideration of

- a) the status of actions from previous management reviews;
- b) changes in external and internal issues that are relevant to the personal information protection management system;
- c) feedback on the personal information protection performance, including trends in:
 - 1) nonconformities and corrective actions;
 - 2) monitoring and measurement results;
 - 3) audit results; and
 - 4) fulfilment of personal information protection objectives;
- d) feedback from interested parties;
- e) results of risk assessment and status of risk treatment plan; and
- f) opportunities for continual improvement.

The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the personal information protection management system. The organization shall retain documented information as evidence of the results of management reviews.

10 Improvement

10.1 Nonconformity and corrective action

When a nonconformity occurs, the organization shall:

- a) react to the nonconformity, and as applicable:
 - 1) take action to control and correct it; and
 - 2) deal with the consequences;
- b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:
 - 1) reviewing the nonconformity;
 - 2) determining the causes of the nonconformity; and
 - 3) determining if similar nonconformities exist, or could potentially occur;
- c) implement any action needed;
- d) review the effectiveness of any corrective action taken; and
- e) make changes to the personal information protection management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

The organization shall retain documented information as evidence of:

- f) the nature of the nonconformities and any subsequent actions taken, and
- g) the results of any corrective action.

10.2 Continual improvement

The organization shall continually improve the suitability, adequacy and effectiveness of the personal information protection management system.

Annex A (normative)

Control objectives and controls

The control objectives and controls listed in Table A.1 are directly derived from and aligned with those listed in the previous edition, **JIS Q 15001:2006**, clause **3**, and also have incorporated additions and modifications made in the revision of this Standard. These control objectives and controls are to be used in context with **6.1.3**.

For asterisked subclauses in Table A.1, relevant supplementary explanations are provided in Annex B.

The subclause numbering in this Table starts with **A.3** in order to facilitate cross-reference to the previous edition.

Table A.1 Control objectives and controls

A.3 Control objectives and controls		
A.3.1 General		
Objective: To operate personal information protection management system.		
A.3.1.1	General*	The controls specified in A.3.2 to A.3.8 shall be approved by persons authorized by top management according to the means determined by the organization.
A.3.2 Personal information protection policy*		
Objective: To define and publicise the principles of personal information protection.		
A.3.2.1	Internal policy for personal information protection*	Top management shall include in the documented information of the internal policy for personal information protection specified in 5.2.1 e) the matters regarding: a) appropriate acquisition, use, and provision of personal information taking the content and size of the business into consideration [including not handling personal information beyond the scope necessary for the achievement of the specific purpose of use (hereafter referred to as “use other than for intended purposes”) and taking measures for it]; b) strict abidance by laws and regulations, guidelines and other codes stipulated by the State related to the handling of personal information; c) prevention of leakage, loss or damage of personal information and correction of personal information; d) response to complaints and consultations; e) continuous improvement of a personal information protection management system; and f) names of person(s) in top management. Top management shall communicate the documented information of the internal policy for personal information protection within the organization and where appropriate, take measures to make it available to interested parties.

Table A.1 (continued)

A.3.2.2	Outward policy for personal information protection*	Top management shall include the following in the documented information of the outward policy for personal information protection, in addition to the matters to be included in the internal policy for personal information protection specified in A.3.2.1: a) dates of establishment and last revision; b) point of contact for inquiries concerning the contents of the outward policy for personal information protection. Top management shall take measures to make the documented outward policy for personal information protection accessible to the general public.
A.3.3 Planning Objective: To plan policies for treatment of personal information.		
A.3.3.1	Specification of personal information*	The organization shall establish and maintain the procedure for specifying all of the personal information which it uses for its business. The organization shall create a register for controlling the personal information which records items, purpose of use, storage location, storage method, persons having access, time limit of use and limit duration of storage of personal information and shall review and update the log at least once a year and at appropriate timings. The organization shall handle the specified personal information in the same manner as it would handle personal data.
A.3.3.2	Laws and regulations, guidelines and other codes stipulated by the State*	The organization shall establish and maintain procedures for specifying and referring to the laws and regulations, guidelines and other codes (hereafter referred to as "laws and regulations, etc.") stipulated by the State that are related to the handling of personal information.
A.3.3.3	Risk assessment and measures against risks*	The organization shall establish and maintain the procedure for implementing the necessary measures to prevent use of the personal information specified in accordance with A.3.3.1 beyond the scope necessary for achievement of the specific purpose of use. The organization shall, in handling of the personal information specified in accordance with A.3.3.1, establish and maintain the procedure for identifying and analysing the risks of personal information protection and taking necessary measures. The organization shall take all the measures that are practicable under current circumstances, and identify and control the untreated issues as residual risks. The organization shall review the identification, and analysis of, and measures taken against the personal information protection risks at least once a year and at appropriate timings.

Table A.1 (continued)

A.3.3.4	Resources, roles, responsibility and authority*	Top management shall assign the responsibility and authority at least for: a) personal information protection manager; b) personal information protection auditor. Top management shall appoint a personal information protection manager who has the ability to understand and practice the requirements of this Standard within the organization, give the manager the responsibility and authority concerning the implementation and operation of the personal information protection management system independent of any other responsibilities. The personal information protection manager shall report the operation status of the personal information protection management system to top management as the basis of review and improvement of the personal information protection management system. Top management shall appoint a personal information protection auditor within the organization who is in a fair and objective position, give the auditor the responsibility and authority to implement and report audits independent of any other responsibilities. The personal information protection auditor shall direct the audit, and prepare an audit report for reporting to top management. For the selection of auditor and implementation of audit, the objectivity and fairness of audit shall be ensured. A person appointed to the personal information protection auditor cannot be appointed to the personal information protection manager at the same time, and vice versa.
A.3.3.5	Internal regulations*	The organization shall document and maintain internal regulations including the provisions concerning: a) procedure for specifying personal information; b) specification of, reference to and maintenance of laws and regulations, guidelines and other codes stipulated by the State; c) personal information protection risk assessment and procedures for taking measures against risks; d) authority and responsibility for protecting personal information in each section and level of the organization; e) preparation for and response to states of emergency; f) acquisition, use and provision of personal information; g) appropriate control of personal information; h) response to a request etc. for disclosure etc. from the principal; i) education; j) control of documented information; k) response to complaints and consultations; l) inspection; m) corrective actions; n) management review; o) penal regulations with regard to the violation of internal regulations. The organization shall revise the internal regulations, as appropriate to its business, in order to ensure implementation of the personal information protection management system.

Table A.1 (continued)

A.3.3.6	Planning*	The organization shall propose, document, and maintain a plan including the following, which is required for ensuring the implementation of the personal information protection management system, at least once a year and at appropriate timings: a) planning and documentation of education implementation based on the requirements specified in A.3.4.5; b) planning and documentation of internal audit implementation based on the requirements specified in A.3.7.2.
A.3.3.7	Preparation for emergency*	The organization shall establish, implement and maintain the procedure for specifying emergencies and the procedure for how to respond to them. The organization shall establish and maintain the procedure for minimizing the effects of emergencies in consideration of personal information protection risk. The organization shall, to prepare for cases of emergencies, establish and maintain the procedures for: a) promptly notifying the principal of the content of the personal information of which leakage, loss or damage occurred, or putting these matters in a state readily accessible to the principal; b) publicly announcing facts, causes and measures as far as possible without delay from the viewpoint of prevention of secondary damages, avoidance of occurrence of similar emergencies, etc.; and c) reporting factual issues, causes and measures to the relevant organizations promptly.
A.3.4 Implementation and operation Objective: To handle the personal information in the operating stage.		
A.3.4.1	Operation procedure	The organization shall clarify the procedure of operation in order to ensure the implementation of the personal information protection management system.
A.3.4.2 Principle on acquisition, use and provision		
A.3.4.2.1	Specification of purpose of use*	The organization shall specify the purpose of use as far as possible, and handle the information within the scope necessary for the achievement of the purpose. In specifying the purpose of use, the organization shall pay attention so as to clarify, as concretely as possible, the scope of the use and provision of the personal information in order to make it possible to predict the influence of the use and provision of the acquired personal information on the principal.
A.3.4.2.2	Appropriate acquisition*	The organization shall acquire personal information legally and fairly.