Control Criteria of ISMAP

June 3, 2020
(Last revised on April 1, 2022)

ISMAP Steering Committee

The original texts of the Standards are prepared in the Japanese language, and these translations are to be used solely as reference material to aid in the understanding of the Standards. For all purposes of interpreting and applying the Standards in practice, users should consult the original Japanese texts available on the following website:
https://www.ipa.go.jp/security/ismap/policy.html

Revision history

Date	Contents of revision
June 3, 2020	ISMAP regulations coming into effect
August 20, 2020	Minor revisions including correction of errors
December 25, 2020	Addition of Appendix 1 Minor revisions including correction of errors
March 12, 2021	Revised the definition of "1.3.15 Cryptography" Minor revisions including correction of errors
June 22, 2021	Revised the description of "2.2.5 Assessment period"
April 1, 2022	Added descriptions of Control Objective to controls criteria in Chapter 5 Revised detailed controls corresponding to the revision of "The Common Standards for Information Security Measures for Government Agencies and Related Agencies" made in July, 2021 Revised the description of "1.2 Characteristics of the criteria" Revised the description of "2.2.3 Overall picture of the system and internal control" Revised the description of "2.2.4 Basic statement requirements" Minor revisions including correction of errors

Table of Contents

Chapter 1 General

1.1 Purpose of the Control Criteria of ISMAP

The purpose of the Control Criteria of ISMAP (below, the “Control Criteria") is to provide a list of security measures that cloud service providers shall implement when applying for registration to the ISMAP Cloud Service List, and how to use them. In principle, the Control Criteria are used as a premise for assessors when conducting assessments in accordance with the ISMAP (below, the “program") Information Security Assessment Criteria, etc.

1.2 Characteristics of the criteria

In this program, a framework using the mechanism of an information security assessment is used. This is based on the viewpoint that a certain level of knowledge has already been accumulated, that it is possible to secure a certain level of evaluation, and that it is possible to perform continuous checks after operation by a security assessment on the information system conducted by the private sector.

From this viewpoint, the Control Criteria was developed based on the Cloud Information Security Management Standard (FY 2016 version) organized in accordance with the standards based on international standards (JIS Q 27001:2014, JIS Q 27002:2014, JIS Q 27017:2016) (hereinafter referred to as “Cloud Information Security Management Standard”), while referring to the Common Standards for Information Security Measures for Government Agencies and Related Agencies (FY 2018 version) (hereinafter referred to as “Common Standards”) and NIST SP800-53 rev.4 (hereinafter referred to as “SP800-53”).

As for the governance criteria, JIS Q 27014:2015 issued after the formulation of the Cloud Information Security Management Standard was referred.

The main features of the Control Criteria are as follows.

（1） The control criteria is implemented by cloud service providers.

（2） It has been developed assuming that the information is classified as confidential 2, which is the most commonly handled information rating category for the government.

（3） Cryptographic deletion is also defined as one of the methods of data deletion (or erasure).

1.3 Terms and definitions

Other than the terms and definitions shown in this section, the definitions of terms in the ISMAP Basic Regulations, the ISMAP Cloud Service Registration Rules, and the following standards shall apply.

- JIS Q 27001:2014 (ISO/IEC 27001:2013)
- JIS Q 27002:2014 (ISO/IEC 27002:2013)
- JIS Q 27014:2015 (ISO/IEC 27014:2013)
- JIS Q 27017:2016 (ISO/IEC 27017:2015)

1.3.1 Information security governance

A corporate governance system that also takes into account social responsibility, and an internal control system as a supporting mechanism established and implemented within a company from the perspective of information security.

1.3.2 Cloud computing

A form of information processing that enables shared computer resources (servers, storage, applications, etc.) to be allocated appropriately and in response to customers' requests and provided over a network.

[Note] A broader definition can be used in some cases.

1.3.3 Cloud service

A service that provides cloud computing.

1.3.4 Cloud service provider

A business or organization that provides a cloud service.

A provider can develop and operate information systems using a cloud service, or can provide its own cloud service using another cloud service.

1.3.5 Cloud service customer

An organization that uses a cloud service.

1.3.6 Cloud service individual customer

An individual who uses a cloud service at a cloud service customer (an organization that uses a cloud service).

1.3.7 Supplier

A party who supplies a part of resources, etc. to a service provider for the service provider to provide a cloud service.

1.3.8 Outsourcer

An external party that is outsourced with part or all of the information processing operations.

1.3.9 Information

A term used when no particular distinction is made between information handled by a cloud service provider and information handled by a cloud service customer.

1.3.10 Information handled by a cloud service provider

Among the various types of information handled by a cloud service provider, refers to cloud service derived data and contract data.

1.3.11 Information handled by a cloud service customer

Among the various types of information handled by a cloud service customer, refers to the data that is input to the cloud service or generated by cloud service customers or their agents executing the capabilities of the cloud service using the public interface of the cloud service, and for which cloud service customers are responsible for management. For example, this would include data created and held by a cloud service customer on a cloud service.

1.3.12 Cloud service derived data

Refers to data that is derived from the information handled by a cloud service provider and is generated on the cloud computing environment through the use of a cloud service by a cloud service customer, and for which a cloud service provider is responsible for management. For example, this would include attributes of cloud service customers, account information, and tags for data retrieval.

1.3.13 Contract data

Among the information handled by a cloud service provider, refers to data related to contracts, and for which a cloud service provider is responsible for management.

1.3.14 Deletion (or erasure)

Deletion includes Cryptographic deletion in addition to physical deletion in which the media is physically destroyed and electromagnetic deletion in which the media is deleted by a demagnetizer. Cryptographic deletion refers to a method in which the original data is encrypted and then the encryption key is deleted to make it impossible to decrypt the original data.

1. 3. 15 Cryptography

Cryptography refers to e-government recommended ciphers with security and implementation performance have been confirmed by the Cryptographic Technology Research and Evaluation Committee (CRYPTREC) and related committees, or cryptography with equivalent or higher security.

1. 3. 16 Customer

When the term "customer" is not used in a restrictive way such as "cloud service customer," it refers to a person who uses or handles the system involved in the relevant controls in some way.

1. 3. 17 Control objectives

Control objectives that cloud service providers should achieve in order to respond to risks. They are expressed by a three-digit number (X.X.X) in the Control Criteria.

1. 3. 18 Detailed controls

Matters that a cloud service provider should select and fulfill to realize the control objectives. They are expressed by a four-digit number (X.X.X.X) in the Control Criteria.

1. 3. 19 Individual controls

Individual control specifically designed by a cloud service provider in its own cloud service for each of the detailed controls selected by the provider.

1. 3. 20 Design assessment

An assessment on whether the cloud service provider has selected control objectives and detailed controls in accordance with the Control Criteria of ISMAP, and that the necessary control is established at a certain point in the assessment period.

1. 3. 21 Operational assessment

An assessment on whether the cloud service provider has selected control objectives and detailed controls in accordance with the Control Criteria of ISMAP, and that the established controls are operating effectively over the assessment period.

1. 3. 22 Work client

Refers to a person who enters a service agreement with a work implementer to request assessment in this program, and refers to a cloud service provider.

1. 3. 23 Work implementer

A person who belongs to the assessor and performs the assessment work under this program.

Chapter 2 Structure

2. 1 Structure of the Control Criteria

These Control Criteria consist of the governance criteria, management criteria, and controls criteria. The conceptual diagram below shows the relationship between the entities assumed to be covered by each criterion and the granularity of each item. (Figure 1)

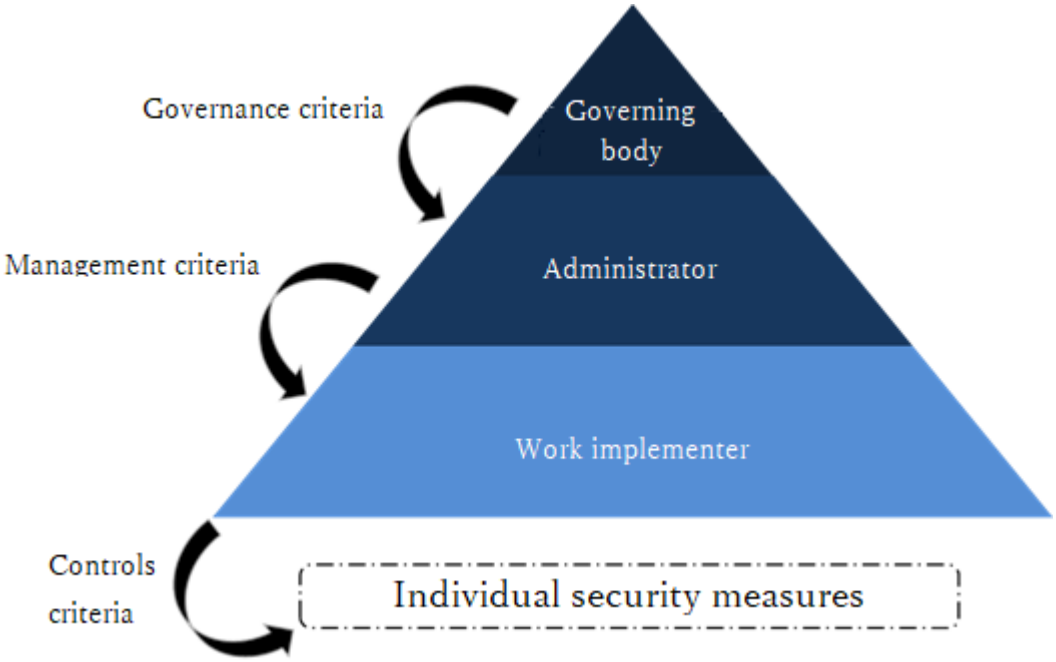

Figure 1: Structure of the Control Criteria

The governance criteria were developed by carefully examining the contents of JIS Q 27014 (ISO/IEC 27014) as matters that should be implemented by the governing body, and reorganizing the four-digit part of the process (X.X.X.X) from the perspective of assessment feasibility.

Management criteria specify the items that administrators should implement for planning, execution, inspection, and treatment of information security management, as well as the implementation items necessary for risk communication.

Controls criteria provide options for selecting controls in accordance with the risk response policy at the stage of establishing information security management in the organization. Each item in the controls criteria consists of control objectives and detailed controls.

Controls that should be specifically considered by cloud service providers as unique to cloud services are indicated as "Controls No. P". In addition, controls that are not mere options for implementing controls, but are themselves basic statement requirements, are indicated as "Controls No. B". "Controls No. PB" indicates both meanings.

2. 2 Contents to be described in the statement

When making the statement, the cloud service provider is required to provide the

following information in writing in accordance with the format specified in the ISMAP Cloud Service Registration Rules. In addition, unless a specific statement of change is made, the statement is considered valid as the responsibility of the cloud service provider.

Of the following items, the name of the cloud service, scope of the statement, and control measures as control objectives being implemented among the basic statement requirements, assessment period, and subsequent events are disclosed to the public in the ISMAP Service List.

2.2.1 Name of the cloud service

State the name of the cloud service covered.

2.2.2 Scope of the statement

Even if it is the name of one cloud service, if there are multiple services under the cloud service, etc., state specifically which service is covered by the statement.

In addition, if the service described here is provided using a service that is not covered by this statement, the scope and the service used is clearly described, and a statement is made that the service is not covered by the statement. However, if the service is based on a cloud service that is not covered by the statement, that service needs to be registered in the ISMAP Cloud Service List.

In addition, the regions covered are stated.

2.2.3 Overall picture of the system and internal control

Describe an overview of the cloud service provider itself, an overview of the cloud service, the logical structure of the system for providing the cloud service (from the physical layer to the application layer), the scope of services covered by the statement, detailed status of internal controls, and targets and their rationale for the same population as defined in Section 3.2 of ISMAP Standard Assessment Procedure, etc.

2.2.4 Basic statement requirements

The following controls shall be implemented as the subject of the statement. If a service is based on a cloud service that is not covered by the statement, and if the service is registered in the ISMAP Cloud Service List, the assessment procedure related to the control can be omitted by taking over the control implemented by the service that is not covered.

(1) Governance criteria

In principle, all of them shall be implemented.

(2) Management criteria

In principle, all of them shall be are implemented.

(3) Controls criteria

In principle, all controls as control objectives shall be implemented. Detailed controls with a "B" at the end (X.X.X.X.B and X.X.X.X.PB) should also be implemented in principle.

Other detailed controls shall be selected as necessary according to the organization, environment, technology, etc. of the service to be described.

For each of the mandatory detailed controls and selected detailed controls, individual controls shall be described. If the content of individual control measures

has been changed during the assessment period, the content of the individual control measures before and after the change and the applicable period shall be described.

On the other hand, a cloud service provider can exclude controls as control objectives that cannot be reasonably applied in light of the services they provide, by providing reasons for such exclusion. In this case, detailed controls with a "B" at the end of the detailed controls included in the exempted controls as control objectives can also be exempted. As for detailed controls, although they are optional as mentioned above, for detailed controls that are not selected, the reason for not selecting them needs to be stated. However, the reasons for not selecting the measures are not subject to assessment

Refer to Attached table 3 for the items of the optional detailed controls. In addition, the contents of Appendix 1 are taken into consideration in selecting and implementing detailed controls.

2.2.5 Assessment period

Among the contents of the statement, describe the assessment period.

The assessment period is a maximum of one year, and the assessment period when applying for the next registration is the day after the last day of the previous assessment period, so that the assessment shall be conducted without gaps between periods. If the assessment period is shorter than one year, a minimum operation period of three months is necessary.

2.2.6 Subsequent events

Subsequent events occurring after the assessment period or the assessment reference date but before the date of the Assessment Report are to be described.

2.2.7 Special notes

If there are any special matters to be noted in conducting the assessment under this program, state them and their details.

2.2.8 Contents to be described in the Written Representation

The cloud service provider shall provide a written statement by management to the assessor in accordance with the form prescribed in the ISMAP Cloud Service Registration Rules to confirm the following matters or to support other assessment evidence.

(1) Statement that with respect to the cloud services subject to the statement, based on the content of the services and the results of the security risk analysis, the cloud service provider is responsible for selecting controls and detailed controls as control objectives in accordance with the Control Criteria, establishing the necessary control, and declaring that these controls have been operating effectively over the target period

(2) Statement that a structure has been established to independently evaluate the accuracy of the statement made and an assessment is being conducted

(3) Statement of responsibility for the interpretation of the requirements of the

Control Criteria

（4） Statement that the cloud service provider knows that the assessment in this program is in accordance with the Information Security Audit Criteria

（5） Statement that there are restrictions on the distribution and use of the Assessment Report

（6） Statement that all information, interviews, and opportunities for questioning requested by the work implementer have been provided

（7） Whether or not there have been any events since the end of the assessment period up to the date of the Written Representation that could significantly change the state of control and information security of the cloud services subject to the statement (and if so, the details)

（8） Whether or not there is any information on fraudulent or illegal activities that can affect the implementation of the work (and if any, the details)

Chapter 3 Governance criteria

3 governance of information security

Information security governance is the system that guides and manages the information security activities of an organization. Information security objectives and strategies need to be aligned with business objectives and strategies, and need to also comply with laws, regulations, and contracts. In addition, information security governance is assessed, evaluated, and implemented through risk management techniques carried out by internal control mechanisms.

3.1 Information security governance process

3.1.1 Overview

The governing body performs the evaluate, direct, monitor and communicate processes to govern information security. In addition, the assurance process provides an independent and objective opinion of information security governance and the level achieved.

3.1.2 Evaluate

1st paragraph of 3.1.2 corresponds to the 1st(last) sentence (beginning with "“Evaluate” is the governance') of the 1st paragraph of the 5.3.2 in ISO/IEC 27014:2013.

2nd paragraph of 3.1.2 corresponds to the 1st sentence (beginning with 'To perform the “evaluate” ') of the 2nd paragraph of the 5.3.2 in ISO/IEC 27014:2013.

3.1.2.1 3.1.2.1 corresponds to the 1st & 2nd of 2 bullet points (beginning with 'ensure that business' & 'ensure that information') in the 2nd paragraph of the 5.3.2 in ISO/IEC 27014:2013.

3.1.2.2 3.1.2.2 corresponds to the 1st of 2 bullet points (beginning with 'respond to information') in the 3rd paragraph of the 5.3.2 in ISO/IEC 27014:2013.

3.1.2.3 The governing body ensures that managers refer to the governing body regarding new information security projects with a significant impact.

3.1.3 Direct

1st paragraph of 3.1.3 corresponds to the 1st & 2nd(last) sentence (beginning with "“Direct” is the governance' & 'Direction can include') of the 1st paragraph of the 5.3.3 in ISO/IEC 27014:2013.

2nd paragraph of 3.1.3 corresponds to the 1st sentence (beginning with 'To perform the “direct” ') of the 2nd paragraph of the 5.3.3 in ISO/IEC 27014:2013.

3.1.3.1 3.1.3.1 corresponds to the 1st of 3 bullet points (beginning with 'determine the organisation’s') in the 2nd paragraph of the 5.3.3 in ISO/IEC 27014:2013.

3.1.3.2 The governing body approves information security strategies and policies.

(a) The governing body ensures that managers develop and implement information security strategies and policies.

(b) The governing body has managers adjust the objectives of information security in accordance with the business objectives.

3.1.3.3 3.1.3.3 corresponds to the 3rd of 3 bullet points (beginning with 'allocate adequate investment') in the 2nd paragraph of the 5.3.3 in ISO/IEC 27014:2013.

3.1.3.4 The governing body has managers promote a positive culture of information security.

3.1.4 Monitor

1st paragraph of 3.1.4 corresponds to the 1st(last) sentence (beginning with '“Monitor” is the governance') of the 1st paragraph of the 5.3.4 in ISO/IEC 27014:2013.

2nd paragraph of 3.1.4 corresponds to the 1st sentence (beginning with 'To perform the “monitor” ') of the 2nd paragraph of the 5.3.4 in ISO/IEC 27014:2013.

3.1.4.1 The governing body evaluates the effectiveness of information security management activities.

(a) The governing body has managers select appropriate performance indicators from a business perspective.

(b) The governing body has managers provide feedback to the governing body on information security performance outcomes, including the implementation of measures previously identified by the governing body and their impact on the organization.

3.1.4.2 3.1.4.2 corresponds to the 1st of 3 bullet points (beginning with 'ensure conformance with') in the 2nd paragraph of the 5.3.4 in ISO/IEC 27014:2013.

3.1.4.3 3.1.4.3 corresponds to the 1st of 3 bullet points (beginning with 'consider the changing') in the 3rd paragraph of the 5.3.4 in ISO/IEC 27014:2013.

3.1.4.4 3.1.4.4 corresponds to the 3rd of 3 bullet points (beginning with 'alert the governing') in the 3rd paragraph of the 5.3.4 in ISO/IEC 27014:2013.

3.1.5 Communicate

1st paragraph of 3.1.5 corresponds to the 1st(last) sentence (beginning with 'Communicate” is the bi-directional') of the 1st paragraph of the 5.3.5 in ISO/IEC 27014:2013.

2nd paragraph of 3.1.5 corresponds to the 1st sentence (beginning with 'One of the methods to ') of the 2nd paragraph of the 5.3.5 in ISO/IEC 27014:2013.

3rd paragraph of 3.1.5 corresponds to the 1st sentence (beginning with 'To perform the “Communicate”') of the 3rd paragraph of the 5.3.5 in ISO/IEC 27014:2013.

3.1.5.1 3.1.5.1 corresponds to the 1st of 3 bullet points (beginning with 'report to external') in the 3rd paragraph of the 5.3.5 in ISO/IEC 27014:2013.

3.1.5.2 The governing body has managers inform the results of external reviews that identify information security issues and request corrective actions.

3.1.5.3 3.1.5.3 corresponds to the 3rd of 3 bullet points (beginning with 'recognize regulatory obligations') in the 3rd paragraph of the 5.3.5 in ISO/IEC 27014:2013.

3.1.5.4 The governing body has managers advise the governing body of issues that require attention and, preferably, decisions.

3.1.5.5 The governing body has managers explain to relevant stakeholders the detailed actions to be taken in support of the governing body's direction and decisions, consistent with the governing body's direction and decisions.

3.1.6 Assure

Assurance is a governance process in which the governing body contracts an independent and objective assessment, review, or certification. Assurance identifies and validates the objectives and actions associated with the execution of governance activities and the performance of operations to achieve the desired level of information security.

2nd paragraph of 3.1.6 corresponds to the 1st sentence (beginning with 'To perform the “assure” ') of the 2nd paragraph of the 5.3.6 in ISO/IEC 27014:2013.

3.1.6.1 The governing body seeks independent and objective opinions from assessors,

etc. on how accountable the company is to the required level of information security.

3.1.6.2 The governing body engages managers to support assessments, reviews, or certifications contracted by the governing body.

Chapter 4 Management criteria

4.1 Management criteria

The management criteria establish criteria for establishing, implementing, operating, monitoring, maintaining, and improving information security management, which is an activity coordinated to direct and control the organization with respect to information security, based on JIS Q 27001:2014. In principle, the management criteria need to be all be implemented.

4.2 Contents of description

The same as "Management Criteria" in "Information Security Management Standard".

In cloud services, it is necessary to consider and implement the controls, etc. of cloud service providers in consideration of the environment of cloud service users. For this reason, it is extremely important to exchange information among cloud service users and cloud service providers regarding the information security risks in cloud services and their measures.

The information security risk communication is specified in Chapter 4.9 as a matter to be especially considered in cloud services.

4.3 Legend

Chapter 4.4 and subsequent chapters have the following structure.

4.4 Establishment of information security management [27001-4]

4.4.1 Roles, responsibilities, and authorities of the organization [27001-5.3 / 5.1]

4.4.1.1 Top management demonstrate leadership and commitment to information security management. [27001-5.1b) / 5.1e) / 5.1f)]

In doing so, the following are performed.

・Integrate the information security management requirements required by the organization into the organization's processes

:

[27001-X.X.X] indicates the relevant clause (X.X.X) in JIS Q 27001:2014.

4.4 Establishment of information security management [27001-4.4]

The scope of application as the foundation is determined and the policy is established in order to establish information security management. Conduct information security risk assessment, and plan and implement response based on this. As a result, create a foundation for the implementation of effective information security management by the organization.

4.4.1 Roles, responsibilities, and authorities of the organization [27001-5.3 / 5.1]

4.4.1.1 Top management demonstrate leadership and commitment to information

security management. [27001-5.1b) / 5.1e) / 5.1f)]

- Integrate the information security management requirements required by the organization into the organization's processes.
- Ensure that information security management achieves its intended results.
- Lead and support people to contribute to the effectiveness of information security management.

In addition, the leadership and commitment of top management are confirmed as follows

- The intentions, judgments and instructions of the top management concerning information security management are recorded in the minutes of the management meetings, etc.
- The intentions, judgments, and instructions of the top management are included in the formulation of the information security policy, information security objectives, and plans to achieve them.
- Top management determines the risk level as the level of security to be achieved.
- The intentions, judgments, and instructions of top management are included in the implementation of the security control measures selected according to the risk level.
- The items to be checked in the internal assessment include the information security requirements, etc. required by the top management.
- The intentions, judgments, and instructions of top management are included in the internal assessment reports, corrective actions based on the reports, and minutes of the management review.

4.4.1.2 Top management assign and communicate the following responsibilities and authorities for the organization's roles. [27001-5.3]

- Conform the information security management as the requirements of the Control Criteria.
- Report the performance assessment of information security management to the top management.

In addition, confirm that the following responsibilities and authorities are assigned to ensure that information security management conforms to the requirements of the Control Criteria.

- Responsibilities and authorities to formulate documents such as information security policies that include security requirements
- Risk owners who have the responsibility and authority to operate and manage the risks in the risk assessment
- Responsibility and authority to educate and disseminate controls that meet security requirements
- Responsibility and authority to assess whether security requirements are being met
- Responsibility and authority to report the results and effects of each process to top management
- Responsibility and authority to disseminate the results and effects of each process within the organization

4.4.1.3 Top management support the role of management team to enable them to

exercise leadership in their areas of responsibility. [27001-5.1h)]

Top management confirms that the necessary authority is delegated to the management team so that the management team can exercise leadership in its area of responsibility, organization, etc.

4.4.2 Understanding of the organization and its situation [27001-4.1]

4.4.2.1 The organization determines the following issues that are relevant to the organization's objectives and that affect the organization's ability to achieve the intended outcomes of information security management. [27001-4.1]

・External issues

・Internal issues

Determination of these issues refers to the determination of the external and internal conditions of the organization. External and internal conditions include the following.

a) External conditions

・Cultural, social, political, legal, regulatory, financial, technological, economic, natural, and competitive environment, whether international, national, regional, or concerning neighboring regions

・Key drivers and trends that influence the organization's objectives

・Relationships with external stakeholders and the perceptions and values of external stakeholders

b) Internal conditions

・Governance, organizational structure, roles, and accountability

・Policies, objectives, and strategies developed to achieve them

・Capabilities in terms of resources and knowledge (for example, capital, time, personnel, processes, systems, and technologies)

・Information systems, information flows, and decision-making processes (including both formal and informal)

・Relationships with internal stakeholders and the perceptions and values of internal stakeholders

・Organizational culture

・Standards, guidelines, and models adopted by the organization

・Form and scope of the contractual relationship

4.4.3 Understanding stakeholder needs and expectations [27001-4.2]

4.4.3.1 The organization determines the following to understand the needs and expectations of stakeholders. [27001-4.2]

・Stakeholders relevant to information security management

・Requirements of stakeholders related to information security

Stakeholder requirements can include legal and regulatory requirements as well as contractual obligations, and stakeholders can include the following.

・A person or organization that has the role and authority to drive the information security management process within the organization. For example, this includes the following.

-A person or organization that formulates the policy concerning information security (top management, etc.)

-A person or organization (general affairs department, information system department, etc.) that ensures that the security control measures are thoroughly implemented in all organizations
-A person or organization (assessment office, etc.) that conducts information security assessments
-Information security experts in the organization

・Business partners, suppliers, and other stakeholders in the supply chain
・Parent company and group companies
・Ministries and government agencies that supervise the security of the organization
・Security organizations and associations to which the organization belongs

4.4.4 Determine the scope of application [27001-4.3]

In order to establish, implement, operate, monitor, review, maintain, and improve information security management, first clarify the scope of application, and establish a foundation for building an information security management system that suits the organization.

4.4.4.1 The organization clarifies the boundaries and applicability of information security management and determine the scope of application. [27001-4.3]

a) The organization defines the scope and boundary of application, taking into account the following points.
・Its own business
・Structure
・Location
・Assets
・Technology characteristics
・External and internal issues
・Stakeholder requirements related to information security
・Interfaces and dependencies between activities performed by the organization and those performed by other organizations

b) The objectives and goals of information security management vary depending on the characteristics of the organization.

c) The requirements for information security management include both external and internal conditions depending on the business of each organization, and the scope of application is defined in consideration of these.
・External conditions include the following.
-Cultural, social, political, legal, regulatory, financial, technological, economic, natural, and competitive environment, whether international, national, regional, or concerning neighboring regions
-Key drivers and trends that influence the organization's objectives
-Relationships with external stakeholders and the perceptions and values of external stakeholders
・Internal conditions include the following
-Governance, organizational structure, roles, and accountability
-Policies, objectives, and strategies developed to achieve them

-Capabilities in terms of resources and knowledge (for example, capital, time, personnel, processes, systems, and technologies)
-Information systems, information flows, and decision-making processes (including both formal and informal)
-Relationships with internal stakeholders and the perceptions and values of internal stakeholders
-Organizational culture
-Standards, guidelines, and models adopted by the organization
-Form and scope of the contractual relationship

4.4.5 Establishment of policy [27001-5.2 / 6.2 / 5.1].

4.4.5.1 Top management establishes an information security policy for the organization that fulfills the following. [27001-5.2]

・It is appropriate for the organization's objectives.
・Information security objectives or a framework for establishing information security objectives
・It includes a commitment to meet applicable requirements related to information security.
・It includes a commitment to the continuous improvement of information security management.

In addition, the information security policy describes the concept that forms the basis for decisions in information security management, and is carefully prepared in accordance with the organization's strategy.

4.4.5.2 The organization formulates information security objectives and a plan to achieve them. [27001-6.2]

a) The information security objectives fulfill the following.

・They are consistent with the information security policy.
・They are measurable (where feasible).
・They take into account applicable information security requirements and the results of risk assessment and risk response.

b) Information security objectives are communicated to relevant stakeholders and updated as necessary, and the following are determined in plans to achieve the objectives.

・Implementation items
・Necessary resources
・Responsible person
・Achievement deadline
・Evaluation method of the results

4.4.5.3 Top management demonstrate leadership and commitment to information security management through the following. [27001-5.1a)]

・Establish information security policies and objectives.
・Establish information security policies and objectives which are consistent with the strategic direction of the organization.

The information security policy is documented so that it can be communicated to the organization and made available to stakeholders in an appropriate manner, and evidence

of top management's commitment to the information security policy is documented in the following manner.

・Signatures on the documented information security policy

・Minutes of meetings in which the information security policy was discussed

・These are implemented to clarify the responsibilities of top management.

4.4.6 Activities to address risks and opportunities [27001-6.1]

4.4.6.1 Determine risks and opportunities. [27001-6.1.1]

a) The organization determine the risks and opportunities that need to be addressed, taking into account external and internal issues and the information security-related requirements of stakeholders, in order to support the following.

・Information security management achieves the organization's intended results.

・Prevent or reduce undesirable impacts.

・Achieve continuous improvement.

In making this decision, the organization plans the following.

・Activities to address the determined risks and opportunities

・How activities to address risks and opportunities are integrated into the information security management process and implemented

・Methods for evaluating the effectiveness of activities to address risks and opportunities

b) As a record of activities to address risks and opportunities, it is confirmed that specific action plans (plans that specify the timing, contents, implementers, locations, and resources required for implementation) are prepared, and when preparing such plans, consideration is given to ensure that each action plan is implemented as part of the information security management process. In addition, it is confirmed that a method to evaluate the effectiveness of the action (method to evaluate the status of implementation and the effect of the implementation) is prepared.

4.4.7 Information security risk assessment [27001-6.1.2]

4.4.7.1 The organization defines and applies an information security risk assessment process through the following. [27001-6.1.2a) / 6.1.2b)]

a) Establish and maintain information security risk criteria, including the following.

・Risk acceptance criteria

・Criteria for conducting information security risk assessments.

b) Consideration is given to ensure that risk acceptance criteria reflect the following.

・The organization's values

・Objectives

・Resources

c) The following points are considered when formulating risk acceptance criteria.

・The nature and type of causes and possible effects, and how they are measured.

・Frequency of occurrence

・Frequency of occurrence, time frame for considering frequency of occurence and consequences

・How to determine the risk level

・Views of stakeholders

・Risk criteria can be imposed on the organization or developed based on legal and regulatory requirements and other requirements agreed to by the organization.

d) The following results are produced when information security assessments are repeated.

・The results of information security risk assessments are consistent and valid.

・The results of the information security risk assessment are comparable.

Because there is no standard risk assessment method for information security management, and each organization often selects the one that best suits its needs, it is necessary to use tools as necessary.

4.4.7.2 The organization identifies information security risks through the following. [27001-6.1.2c)]

a) Apply the information security risk assessment process to identify the risks associated with loss of confidentiality, integrity, and availability of information.

b) Identify the risk owners in the process of identifying risks.

c) Take the following into consideration when identifying risks.

・Risks for which the source or cause of the risk is not known are identified, regardless of whether the source is under the control of the organization.

・Carefully consider the specific chain of consequences, including spillover and cumulative effects.

・In addition to identifying what could happen, scenarios are considered that show possible causes and what consequences could be caused

・All significant causes and consequences

・The following are identified

-Risk sources

-Affected areas and events

-Causes and possible consequences

A comprehensive list of risks, including risks associated with failure to pursue certain opportunities, is developed, as risks not identified at this stage will be excluded from future analysis.

4.4.7.3 The organization analyzes information security risks through the following. [27001-6.1.2d)]

a) Perform risk analysis through the following procedure.

・Identify the possible consequences of the identified risks if they actually occur.

・Analyze the frequency of occurrence of the identified risks.

・Determine the level of risk.

・ The following points are considered based on the identified threats and vulnerabilities.

-Business impact of a security incident

-Frequency of security incidents

-Effectiveness of controls, if any

b) The following points are also be considered in the risk analysis.

・Causes and sources of risks

・Favorable and unfavorable consequences of risks

・Frequency of occurrence of risks

・Factors affecting the consequences and frequency of occurrence of risks

The risk analysis can be conducted qualitatively, semi-quantitatively, quantitatively, or through a combination of these methods, depending on the situation.

4.4.7.4 The organization evaluates information security risks through the following. [27001-6.1.2e)]

・Compare the risk level determined as a result of the risk analysis with the risk criteria.

・Prioritization is performed for risk response.

・The results of the risk assessment are stored for use in future improvements.

When performing prioritization for risk responses, a broader range of situations, the level of risk accepted by others and laws, regulations, and other requirements are considered.

4.4.8 Information security risk response [27001-6.]

4.4.8.1 The organization selects appropriate information security risk response options, taking into account the results of the information security assessment. [27001-6.1.3a)]

Information security risk response options include the following.

・Avoidance of risk by deciding not to initiate or continue activities that create risk

・Acceptance of risk or bearing of risk for the purpose of an opportunity

・Elimination of sources of risk

・Changing the frequency of occurrence

・Changing the outcome

・Sharing risks with others (including through contracts and risk finance)

・Retention of risk through decision-making based on information

Furthermore, the reasons for selecting any of the options are clarified and described in order to help evaluate and improve the risk response.

4.4.8.2 The organization determines all controls necessary to implement the selected information security risk response. [27001-6.1.3b)]

The purpose of the controls (control objectives) and the controls are discussed after determining the policy for risk response. Select appropriate information security measures by balancing the effects of the measures with the cost and effort required for the measures, taking into account the following.

・Acceptable level of risk

・Relevant laws and regulations

・Regulatory and contractual requirements

・Other social responsibilities

In selecting specific controls, appropriate controls are selected from the controls criteria corresponding to the control objectives. However, because the controls criteria do not cover everything, other controls can be added depending on the business and operations of the organization.

4.4.8.3 The organization verifies that no controls have been overlooked. [27001-6.1.3c)]

The organization refers to the controls criteria to ensure that no necessary controls have been overlooked, and other control objectives and controls can be added if control

objectives and controls other than those shown in the controls criteria become necessary.

4.4.8.4 The organization formulates an information security risk response plan. [27001-6.1.3e)]

a) The information security risk response plan includes the following.

- Rationale for the selection of response options, including expected effects
- The person who approves the information security risk response plan and the person responsible for the implementation of the response plan
- Details of response
- Necessary resources
- Cost, effort, and constraints
- Requirements for later reporting and monitoring
- Targets for each milestone in the response process
- Response timing and schedule

b) Responsibility and authority

In information security management, final approval is almost always given by the top management, and the responsibility is concentrated on the top management.

On the other hand, the risk owners have the responsibility and authority for information security risk assessment and risk response.

Because the risk owners are often the top management or those who are appointed by the top management and to whom the responsibility and authority are delegated, the responsibilities of the top management and risk owners are clarified in the information security management.

4.4.8.5 The organization obtains approval from the risk owners for the information security risk response plan and have the risk owners accept the residual information security risks. [27001-6.1.3f)]

Once control objectives and controls have been selected for all risks, the residual risks are clarified and a plan for future action is developed. The following points are taken into account when preparing the plan.

- When it will be technically feasible
- When it will be feasible in terms of costs

Residual risks are periodically reviewed and, if necessary, targeted for action, and residual risks after risk response are recognized by the governing body and other stakeholders in addition to the risk owners.

In addition, approved minutes of meetings are kept correctly to clarify the responsibility of risk owners.

4.5 Implementation of information security management [27001-8]

4.5.1 Resource management [27001-7.1 / 5.1]

4.5.1.1 The organization determines and provides the resources necessary to establish, implement, maintain, and continuously improve information security management. [27001-7.1]

In order to meet the control objectives, the organization continuously implements the controls and secure the management resources so that they can be provided appropriately at the right time to cope with changes in the environment, such as an increase in the

number of personnel and systems.

4.5.1.2 Top management allocates the following resources to ensure that the resources required for information security management are available. [27001-5.1c)]

- People or organizations required for each process of information security management
- Facilities, equipment, and systems required for each process of information security management
- Costs required for the above

4.5.2 Competence, awareness [27001-7.2 / 7.3 / 5.1]

4.5.2.1 Top management communicates the importance of effective information security management and compliance with its requirements. [27001-5.1d)]

Together with the information security policy, top management communicates to the stakeholders that while top management is responsible for information security management, implementation requires the cooperation of the entire organization.

In addition, standards such as information classification are established so that organizations can make the same decisions according to the same regulations. In the case of information such as personal information, which can have partially different interpretations by different organizations, stakeholders are communicated to after clarifying your company's approach in addition to the general approach.

4.5.2.2 The organization determines the competencies required for the person (or people) under its control to perform tasks that affect the organization's information security performance. [27001-7.2a)]

The organization identifies the tasks related to and affecting information security management, and create a separation of duties that clarifies the roles. The following points are clarified in these separation of duties.

- Job title
- Job description
- Scope of responsibility of the responsible person
- Knowledge required for the job
- Qualifications required for the job
- Experience required for the job

Because such knowledge, qualifications, and experience can change due to changes in the environment or objectives, they are reviewed from time to time to ensure that they are up-to-date.

4.5.2.3 The organization ensures that the person (or people) under its control who perform tasks that affect the organization's information security performance are equipped with competence based on appropriate education, training, or experience. [27001-7.2b)]

Applicable actions include, for example, providing education and training, mentoring, and reassignment of currently employed people (in cases where education and training are deemed to not be too late, personnel with appropriate competence can be hired, and in cases where the work is not closely related to internal operations, it can be outsourced.)

4.5.2.4 The organization takes actions to ensure that employees acquire the necessary competencies and evaluate the effectiveness of the actions taken. [27001-7.2c)]

Education and training are important as a means of acquiring the necessary competence. Education is conducted to provide the necessary knowledge, and training is conducted to provide the necessary skills and experience. The content of training is effective, including not only general knowledge of threats and vulnerabilities, but also content that reflects the characteristics of the organization, such as business risks.

The following are conducted to confirm whether or not the necessary competencies have been acquired as a result of the education and training.

- Confirmation test of knowledge
- Practical tests of skills
- Benchmarking using checklists, etc.

The results of these tests are recorded to ensure objectivity in personnel selection.

4.5.2.5 The organization keeps track of personal competencies and retains appropriate documented information as evidence for a period of time determined by the organization. [27001-7.2d)]

The following are considered and implemented regularly for education and training.

- Basic plan for education and training
- Education and training implementation plan
- Confirmation tests or evaluation reports

In the case of partial exemption of education and training, it is clarified which skills, experience and qualifications are applicable, an investigation is performed for each responsible person, and a list is created. Clarify and update expiration dates for qualifications.

4.5.2.6 All people working under the control of the organization are aware of the information security policy. [27001-7.3a)]

The purpose and importance of the organization's information security activities are communicated as part of the information security policy notification and education, to increase the understanding of the people involved as to why the controls are being implemented.

4.5.2.7 People working under the control of the organization recognize their own contribution to the effectiveness of information security management, including the benefits derived from improved information security performance. [27001-7.3b)]

Clarify the role of each person and their contribution to the effectiveness of information security management by communicating the following points to people working under the control of the organization.

- Their respective roles in information security management
- The tasks and procedures to execute the roles (including the reporting procedures when anomalies are detected)
- Location of documents describing the above

4.5.2.8 People working under the control of the organization are aware of the implications of not complying with the requirements of information security management. [27001-7.3c]

4.5.3 Communication [27001-7.4]

4.5.3.1 The organization determines the need to conduct internal and external communications related to information security management. [27001-7.4]

a) The following are considered when implementing internal and external communications.

・The content of the communication (what is to be communicated)

・The timing of the communication

・Target audience of the communication

・The person who conducts communication

・Communication implementation process

b) Internal communication is conducted with the following parties as appropriate and on a regular basis.

・Top management

・Persons authorized to ensure that information security management complies with the requirements of this management standard

・Those who have the authority to report the performance of information security management to top management or within the organization

・Employees in the organization

c) Communication is conducted with the following parties in external communication, as necessary.

・Suppliers, partners, and other stakeholders in the supply chain

・Parent company and group companies

・Ministries and government agencies that oversee the security of the organization

・Security organizations and associations to which the organization belongs

4.5.4 Planning and management of information security management [27001-8.1]

4.5.4.1 The organization plans, implements, and manages the processes necessary to implement activities that address risks and opportunities to meet information security requirements. [27001-8.1]

4.5.4.2 The organization implements a plan to achieve its information security objectives. [27001-8.1]

4.5.4.3 The organization maintains documented information to provide confidence that the plan has been implemented as planned. [27001-8.1]

The organization confirms that the following information is collected in the documented information.

・Implementation status of controls

・Effectiveness of the controls

・Changes in the environment surrounding the controls

The organization also establishes a system for identifying and determining this information.

4.5.4.4 The organization manages planned changes, reviews the consequences of unintended changes, and takes action to mitigate adverse effects, as necessary. [27001-8.1]

4.5.4.5 The organization determines and controls the processes to be outsourced. [27001-8.1]

4.5.5 Implementation of an information security risk assessment [27001-8.2.8.3]

4.5.5.1 The organization performs an information security risk assessment in any of the

following cases. [27001-8.2]

・At predetermined intervals

・When a significant change is proposed

・When a significant change occurs

4.5.5.2 The organization implements an information security risk response plan. [27001-8.3]

Measures are taken to ensure that the identified individual responsibilities are fulfilled in the implementation of the information security risk response plan.

4.5.5.3 Top management provides sufficient management resources for the information security risk response plan.

The information security risk response plan requires adequate management resources, and the following points are considered.

・Costs, manpower, man-hours, and technology for the implementation and operation of controls

・Costs for temporary response in the event of a security incident

・Costs for other risk responses

The management resources required to measure the effectiveness of the controls in implementation are considered and budgeted.

4.6 Monitoring and review of information security management [27001-5.1 / 8.2 / 9 / 10.2]

4.6.1 Continual improvement of effectiveness [27001-10.2 / 8.2 / 9.2 / 9.3 / 5.1]

4.6.1.1 The organization continuously improves the appropriateness, adequacy, and effectiveness of its information security management by implementing the following. [27001-10.2 / 8.2 / 9.2 / 9.3]

・Periodic information security risk assessment

・Periodic information security internal assessments

・Periodic management review by top management

In the process of continuous improvement, nonconformities are detected and dealt with not only with the controls that have been implemented so far, but also by responding to new threats and vulnerabilities due to changes in the environment.

4.6.1.2 Top management promotes continuous improvement. [27001-5.1g)]

Assign roles, responsibilities, and authorities for implementing 4.6.1.1. and communicate them to relevant personnel for implementation.

4.6.2 Performance evaluation [27001-9]

4.6.2.1 The organization continuously evaluates information security performance and the effectiveness of information security management to determine the following. [27001-9.1]

・Scope of monitoring and measurement required (including information security processes and controls)

・Methods of monitoring, measurement, analysis, and evaluation to ensure valid results (methods that produce comparable and reproducible results)

・Timing and frequency of monitoring and measurement

・The person who conducts monitoring and measurement
・Timing and frequency of analysis (including causality and correlation) and evaluation of the results of monitoring and measurement
・The person who conducts the analysis and evaluation of the results of monitoring and measurement
・Response measures in accordance with the results of the analysis and evaluation
・Frequency of reporting the results of the analysis and evaluation

4.6.2.2 The organization conducts internal assessments at predetermined intervals. [27001-9.2a) / 9.2b)]

a) The following are confirmed when conducting internal assessments.
・Confirm compliance with the following.
-Requirements stipulated by the organization itself regarding information security management
-Requirements of this management criteria
・Information security management is effectively implemented and maintained.

b) Internal assessments are conducted on a regular basis to comprehensively confirm the effectiveness of controls, and the plans and results are managed in the following documents.
・Basic plan for internal assessments
・Internal assessment implementation plan
・Internal assessment report

The scope, purpose, management system, and period or date of the assessment are determined in advance in the basic plan, the timing and location of the assessment, the personnel in charge of the assessment and their assignments, and the detailed assessment methods are determined in advance in the implementation plan. An implementation report is prepared in order to prove that the assessment was conducted as planned.

c) The following items are included in the assessment of conformity
・Relevant legal or regulatory requirements
・Information security requirements identified through information security risk assessment, etc.

d) The assessment of the effective implementation and maintenance of information security management include the following items
・Effectiveness and maintenance of controls
・Whether controls are being implemented as expected.

4.6.2.3 The organization plans, establishes, implements, and maintains an assessment program that includes requirements and reporting on frequency, methods, responsibilities, and plans. [27001-9.2c)]

The assessment program takes into account the importance of the processes involved and the results of previous assessments.

Because assessments can not only be conducted for the entire scope at once, but also for only a part of the scope, and since it is important to clarify the objectives of each assessment and to implement an appropriate assessment plan, the following points are considered in the development of the assessment program.

・Objectives and key targets of the assessment
・The status and importance of the assessment process to be covered
・The status and importance of the area to be assessed
・Previous assessment results

4.6.2.4 The organization clarifies the assessment criteria and scope. [27001-9.2d)]

The assessment program includes not only the overall assessment schedule, but also the following.

・Assessment criteria (including the following)
  -Objectives, authority, and responsibilities
  -Independence, objectivity, and professional ethics
  -Professional competence
  -Work obligations
  -Quality control
  -How the assessment is conducted
  -Format of the assessment report
・Scope of the assessment
・Frequency or timing of the assessment
・Assessment method (separate information security assessment criteria are developed and prepared for both internal assessments and assessments by external organizations to ensure high quality assessments)

4.6.2.5 The organization selects assessors and conducts assessments that ensure the objectivity and impartiality of the assessment process. [27001-9.2e)]

The organization selects assessors in accordance with the assessment criteria and consider the following.

・Independence in terms of appearance
・Mental independence
・Professional ethics and integrity

In the case of internal assessors, they are assigned other personnel so that they do not conduct an assessment on the work they are engaged in themselves.

4.6.2.6 The organization ensures that the results of the assessment are reported to the relevant management team. [27001-9.2f)]

4.6.2.7 The organization maintains documented information as evidence of the assessment program and assessment results. [27001-9.2g)]

The assessment procedures reflect and document the following, and are used for mutual communication.

・Responsibilities and requirements for planning and conducting the assessment
・Responsibilities and requirements for reporting results and maintaining records

The requirements are essential to ensure assessment quality, and the responsible person and the assessor conducts the assessment with the same objective.

4.6.3 Management review [27001-9.3]

4.6.3.1 Top management conducts management reviews at predetermined intervals.

[27001-9.3]

The following points are considered and documented in order to conduct management reviews at predetermined intervals.

・Basic plan for management review

・Management review implementation plan

・Implementation report for management review

The objective and timing of implementation are determined in the basic plan, and detailed assessment methods are determined in advance in the implementation plan.

4.6.3.2 Top management considers the following in the management review. [27001-9.3]

・Status of actions taken as a result of the previous management reviews

・Changes in external and internal issues related to information security management

・Feedback on information security performance, including the following

-Nonconformities and corrective actions

-Results of monitoring and measurement

-Assessment results

--Achievement of information security objectives

・Feedback from stakeholders

・Results of information security risk assessment and status of information security risk response plan

・Opportunities for continual improvement

In addition, activities and events that are expected to constitute such information are recorded and reported as necessary, and those that are highly urgent are defined in advance, and standards are established so that everyone can make the same decision.

4.6.3.3 Outputs from management reviews include decisions on opportunities for continuous improvement and the need for any changes in information security management. [27001-9.3]

The following activities are implemented and improvement measures are considered in order to reflect the results of the management review in improvement measures.

・Improvement of the effectiveness of information security management

・Updates to information security risk assessment and information security risk response plan

・Modification of procedures and controls in consideration of internal and external events that can impact information security management

・Identification of required management resources

・Improvement of performance measurement methods

Records of the information security risk response options selected are referred to when planning improvement measures.

4.6.3.4 The organization retains documented information as evidence of the results of management reviews. [27001-9.3]

Because the results of management reviews are used for the next management review, the results are specifically recorded so that the details and results can be understood.

4.7 Maintenance and improvement of information security management [27001-10]

4.7.1 Corrective actions [27001-10.1]

4.7.1.1 The organization takes actions to correct nonconformities when they occur. [27001-10.1a)]

a) The following are performed when taking corrective action.

・Actions to control and correct the nonconformity

・Actions to address the consequences of the nonconformity

・The following are documented to ensure that corrective actions are implemented in accordance with procedures

-Evaluation of the need for the actions selected to ensure that the nonconformity is not recurring

-Determination of the corrective action required

-Implementation of the corrective action required

-Records of actions taken

-Review of the corrective actions taken

b) Nonconformities are detected through the following activities

・Periodic information security risk assessment

・Periodic information security internal assessments

・Periodic management reviews

・The following are documented in order to detect nonconformities in a procedural manner.

-Identification of nonconformities with information security management

-Determination of the cause of nonconformities with information security management.

In some cases, nonconformities cannot be determined through a single activity alone, so nonconformities are detected by considering the combined results.

4.7.1.2 The organization evaluates the need to take action to remove the cause of the nonconformity in order to prevent its recurrence or occurrence elsewhere. [27001-10.1b)]

The following are performed when evaluating the need.

・Review of the nonconformity

・Clarification of the cause of the nonconformity

・Clarification of the existence of similar nonconformities or the likelihood of their occurrence

4.7.1.3 The organization takes the necessary actions. [27001-10.1c)]

4.7.1.4 The organization reviews the effectiveness of all corrective actions taken. [27001-10.1d)]

4.7.1.5 The organization makes changes to its information security management when necessary. [27001-10.1e)]

4.7.1.6 The organization ensures that corrective actions are proportionate to the impact of the nonconformities defected. [27001-10.1]

4.7.1.7 The organization maintains the following documented information as evidence of corrective actions. [27001-10.1f) / 10.1g)]

・The nature of the nonconformity and the action taken
・Results of corrective actions

4.8 Management of documented information [27001-7.5]

4.8.1 Guidelines for documentation [27001-7.5.1]

4.8.1.1 The organization documents the following information required by information security management. [27001-7.5.1]

・Information security policy
・Information security objectives
・Information security risk assessment process
・Information security risk response process
・Results of information security risk assessment
・Information security risk response plan
・Results of performance measurement

While it does not matter which document these contents are stated in, the information needs to be structured in such a way that it is communicated to those who need to know the information, and such documents not be accessible to those who do not need to know them.

4.8.2 Creation, modification, and management of documents [27001-7.5.2 / 7.5.3]

4.8.2.1 The organization creates and update documented information by doing the following [27001-7.5.2]

・Description of appropriate identifying information (for example, title, date, author, and reference number)
・Selection of an appropriate format (for example, language, software version, charts) and medium (for example, paper, digital).
・Appropriate review and approval on appropriateness and validity
・Definition of the lifecycle of the documented information and development of procedures to handle it accordingly
・Review and approval of appropriateness before issuing documents
・Update and re-approval of documents as necessary
・Prevention of misuse of obsolete documents
・When obsolete documents are retained for any purpose, a description of appropriate identification information that identifies them as obsolete documents
・Updating of documents at a defined frequency in accordance with legal and regulatory requirements and changes in the environment

In addition, appropriate document management procedures are developed, taking into consideration whether all these activities are reflected in document management and whether these activities cause significant obstacles to business operations.

4.8.2.2 The organization manages documented information as required by information security management to ensure the following. [27001-7.5.3]

・The documented information is available and suitable for use when and where it is needed.

・Documented information is adequately protected (for example, against loss of confidentiality, improper use, and loss of integrity).
・Distribution, access, retrieval, and use of documented information
・Storage and preservation of documented information, including maintaining legibility
・Management of changes in documented information (for example, version control)
・Retention and disposal of documented information

In addition, documents determined to be necessary by the organization for the planning and operation of information security management are identified and managed as necessary, even if they are obtained from external sources.

4.9 Information security risk communication

Effective communication between stakeholders can have a significant impact on decision-making. Information security risk communication involves the exchange and sharing of information about information security risks between decision makers and other stakeholders (including cloud service users and outsourcers involved in the provision of cloud services), and agreement on how to manage those risks.

4.9.1 Risk communication plan

4.9.1.1 A risk communication plan is formulated.

A risk communication plan is formulated and documented for the following two categories.

・Risk communication plan for normal operations
・Risk communication plan for emergencies
・The risk communication plan pays attention to how to encourage communication between decision-makers and other stakeholders (including cloud service users and outsourcers involved in the provision of cloud services) and includes the following information.
・Effective information exchange and sharing with the participation of appropriate stakeholders
・Compliance with legal, regulatory, and governance requirements
・Provision of feedback and reporting on communications and discussions
・Use of communications to build trust in the organization
・Implementation of communication with stakeholders in the event of a crisis or unforeseen event

4.9.2 Implementation of risk communication

4.9.2.1 Establish a mechanism for implementing risk communication.

Establish a mechanism for discussing risks, prioritizing and responding appropriately to risks, accepting risks, and coordinating with key decision makers and stakeholders (including cloud service users and outsourcers involved in the provision of cloud services). This mechanism ensures the following items.

・Appropriate communication of the key components of the risk management framework and any subsequent modifications
・Appropriate internal reporting on the framework, its effectiveness and outcomes

・Provision of relevant information derived from the adaptation of risk management that is available at the appropriate level and time
・Processes for consultation with internal stakeholders

The mechanism can include, where appropriate, a process for compiling risk information from a variety of sources and can need to take into account the susceptibility of an impact from risk information. A committee is one place where this mechanism can be established.

4.9.2.2 Risk communication is conducted.

Risk communication is implemented on an ongoing basis at all stages of the risk management process to achieve the following.

・Provide assurance of the organization's risk management results
・Collect risk information
・Share the results of the risk assessment and provide a risk response plan
・Avoid or reduce the occurrence and consequences of information security violations due to a lack of mutual understanding between decision makers and stakeholders (including cloud service users and outsourcers involved in the provision of cloud services)
・Support decision making
・Obtain new information security knowledge
・Develop a response plans to reduce the consequences of all incidents in coordination with other organizations
・ Make decision makers and stakeholders (including cloud service users and outsourcers involved in the provision of cloud services) aware of their responsibility for risk
・Improve security awareness

Collaborate with the appropriate public relations or communications department within the organization to coordinate all risk communication-related tasks in the implementation of risk communication.

Chapter 5 Controls criteria

5 Information security policies

5.1 Management direction for information security

Control Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

5.1.1 5.1.1 corresponds to the part of 5.1.1 Control in ISO/IEC 27002:2013.

5.1.2 5.1.2 corresponds to the part of 5.1.2 Control in ISO/IEC 27002:2013.

6 Organization of information security

6.1 Internal organization

Control Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

6.1.1 6.1.1 corresponds to the part of 6.1.1 Control in ISO/IEC 27002:2013.

6.1.1.13.PB 6.1.1.13.PB corresponds to the 6.1.1 Implementation guidance for Cloud service provider in ISO/IEC 27017:2015.

6.1.2 6.1.2 corresponds to the part of 6.1.2 Control in ISO/IEC 27002:2013.

6.1.3 6.1.3 corresponds to the part of 6.1.3 Control in ISO/IEC 27002:2013.

6.1.3.3.PB 6.1.3.3.PB corresponds to the 6.1. Implementation guidance for Cloud service provider in ISO/IEC 27017:2015.

6.1.4 6.1.4 corresponds to the part of 6.1.4 Control in ISO/IEC 27002:2013.

6.1.5 6.1.5 corresponds to the part of 6.1.5 Control in ISO/IEC 27002:2013.

6.2 Mobile devices and teleworking

Control Objective: To ensure the security of teleworking and use of mobile devices.

6.2.1 6.2.1 corresponds to the part of 6.2.1 Control in ISO/IEC 27002:2013.

6.2.2 6.2.2 corresponds to the part of 6.2.2 Control in ISO/IEC 27002:2013.

6.3.P Relationship between cloud service customer and cloud service provider

Control Objective: To clarify the relationship regarding shared roles and responsibilities between the cloud service customer and the cloud service provider for information security management.

6.3.1.P 6.3.1.P corresponds to the part of CLD.6.3.1 Control in ISO/IEC 27017:2015 Annex A.

6.3.1.1.PB 6.3.1.1.PB corresponds to the 1st(last) sentence (beginning with "The cloud service") of the 1st(last) paragraph of the Implementation guidance of CLD.6.3.1 in ISO/IEC 27017:2015 Annex A.

7 Human resource security

7.1 Prior to employment

Control Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

7.1.1 7.1.1 corresponds to the part of 7.1.1 Control in ISO/IEC 27002:2013.

7.1.2 7.1.2 corresponds to the part of 7.1.2 Control in ISO/IEC 27002:2013.

7.2 During employment

Control Objective: To ensure that employees and contractors are aware of and fulfil their

information security responsibilities.

7.2.1 7.2.1 corresponds to the part of 7.2.1 Control in ISO/IEC 27002:2013.

7.2.2 7.2.2 corresponds to the part of 7.2.2 Control in ISO/IEC 27002:2013.

7.2.2.19.PB Cloud service providers provide education and training to raise awareness among employees regarding the proper handling of cloud service customer data and cloud service derived data, and require contract parties to do the same.

7.2.3 7.2.3 corresponds to the part of 7.2.3 Control in ISO/IEC 27002:2013.

7.3 Termination and change of employment

Control Objective: To protect the organization's interests as part of the process of changing or terminating employment.

7.3.1 7.3.1 corresponds to the part of 7.3.1 Control in ISO/IEC 27002:2013.

8 Asset management

8.1 Responsibility for assets

Control Objective: To identify organizational assets and define appropriate protection responsibilities.

8.1.1 8.1.1 corresponds to the part of 8.1.1 Control in ISO/IEC 27002:2013.

8.1.1.6.PB 8.1.1.6.PB corresponds to the 8.1. Implementation guidance for Cloud service provider in ISO/IEC 27017:2015.

8.1.2 8.1.2 corresponds to the part of 8.1.2 Control in ISO/IEC 27002:2013.

8.1.2.7.PB The cloud service provider provides the cloud service customer with one of the following to manage the assets (including backups) of such customer.

(a) A function that encrypts the assets managed by the relevant customer before they are recorded (including backups) on a storage medium, and enables the relevant customer to manage and delete the encryption key

(b) Information necessary for the relevant customer to implement the function of encrypting the assets managed by the relevant customer before recording (including backup) them on the storage media, and manage and delete the cryptographic keys

8.1.3 8.1.3 corresponds to the part of 8.1.3 Control in ISO/IEC 27002:2013.

8.1.4 8.1.4 corresponds to the part of 8.1.4 Control in ISO/IEC 27002:2013.

8.1.5.P 8.1.5.P corresponds to the part of CLD.8.1.5 Control in ISO/IEC 27017:2015 Annex A.

8.2 Information classification

Control Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

8.2.1 8.2.1 corresponds to the part of 8.2.1 Control in ISO/IEC 27002:2013.

8.2.2 8.2.2 corresponds to the part of 8.2.2 Control in ISO/IEC 27002:2013.

8.2.2.7.PB The cloud service provider documents and discloses about the service functions that allow cloud service customers to classify and label the information and related assets handled by the cloud service customers.

8.2.3 8.2.3 corresponds to the part of 8.2.3 Control in ISO/IEC 27002:2013.

8.3 Media handling

Control Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

8.3.1 8.3.1 corresponds to the part of 8.3.1 Control in ISO/IEC 27002:2013.

8.3.2 8.3.2 corresponds to the part of 8.3.2 Control in ISO/IEC 27002:2013.

8.3.3 8.3.3 corresponds to the part of 8.3.3 Control in ISO/IEC 27002:2013.

9 Access control

9.1 Business requirements of access control

Control Objective: To limit access to information and information processing facilities.

9.1.1 9.1.1 corresponds to the part of 9.1.1 Control in ISO/IEC 27002:2013.

9.1.2 9.1.2 corresponds to the part of 9.1.2 Control in ISO/IEC 27002:2013.

9.2 User access management

Control Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.

9.2.1 9.2.1 corresponds to the part of 9.2.1 Control in ISO/IEC 27002:2013.

9.2.1.6.PB 9.2.1.6.PB corresponds to the 1st(last) sentence (beginning with "To manage access") of the 1st(last) paragraph of the Implementation guidance of 9.2.1 in ISO/IEC 27017:2015.

9.2.2 9.2.2 corresponds to the part of 9.2.2 Control in ISO/IEC 27002:2013.

9.2.2.8.PB 9.2.2.8.PB corresponds to the 9.2. Implementation guidance for Cloud service provider in ISO/IEC 27017:2015.

9.2.3 9.2.3 corresponds to the part of 9.2.3 Control in ISO/IEC 27002:2013.

9.2.3.11.PB Depending on the identified risks, cloud service providers provide sufficiently strong authentication technologies for administrator authentication of cloud service customers that are tailored to the management capabilities of the cloud service.

9.2.4 9.2.4 corresponds to the part of 9.2.4 Control in ISO/IEC 27002:2013.

9.2.4.9.PB 9.2.4.9.PB corresponds to the 9.2. Implementation guidance for Cloud service provider in ISO/IEC 27017:2015.

9.2.5 9.2.5 corresponds to the part of 9.2.5 Control in ISO/IEC 27002:2013.

9.2.6 9.2.6 corresponds to the part of 9.2.6 Control in ISO/IEC 27002:2013.

9.3 User responsibilities

Control Objective: To make users accountable for safeguarding their authentication information.

9.3.1 9.3.1 corresponds to the part of 9.3.1 Control in ISO/IEC 27002:2013.

9.4 System and application access control

Control Objective: To prevent unauthorized access to systems and applications.

9.4.1 9.4.1 corresponds to the part of 9.4.1 Control in ISO/IEC 27002:2013.

9.4.1.8.PB 9.4.1.8.PB corresponds to the 9.4. Implementation guidance for Cloud service provider in ISO/IEC 27017:2015.

9.4.2 9.4.2 corresponds to the part of 9.4.2 Control in ISO/IEC 27002:2013.

9.4.2.2.B 9.4.2.2.B corresponds to the 1st(last) sentence (beginning with "Where strong authentication") of the 2nd paragraph of the Implementation guidance of 9.4.2 in ISO/IEC

27017:2015.

9.4.3 9.4.3 corresponds to the part of 9.4.3 Control in ISO/IEC 27002:2013.

9.4.4 9.4.4 corresponds to the part of 9.4.4 Control in ISO/IEC 27002:2013.

9.4.5 9.4.5 corresponds to the part of 9.4.5 Control in ISO/IEC 27002:2013.

9.5.P Access control of cloud service customer data in shared virtual environment

Control Objective: To mitigate information security risks when using the shared virtual environment of cloud computing.

9.5.1.P 9.5.1.P corresponds to the part of CLD.9.5.1 Control in ISO/IEC 27017:2015 Annex A.

9.5.2.P 9.5.2.P corresponds to the part of CLD.9.5.2 Control in ISO/IEC 27017:2015 Annex A.

9.5.2.1.PB 9.5.2.1.PB corresponds to the 1st(last) sentence (beginning with "When configuring") of the 1st(last) paragraph of the Implementation guidance of CLD.9.5.2 in ISO/IEC 27017:2015 Annex A.

10 Cryptography

10.1 Cryptographic controls

Control Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

10.1.1 10.1.1 corresponds to the part of 10.1.1 Control in ISO/IEC 27002:2013.

10.1.1.9.PB The cloud service provider provides the cloud service customer with the capability to use cryptographic techniques to protect the information processed by the customer, or provides information about the environment in which the cryptographic techniques are used.

10.1.2 10.1.2 corresponds to the part of 10.1.2 Control in ISO/IEC 27002:2013.

10.1.2.20.PB The cloud service provider provides a cloud service customer with a function that allows said customer to manage cryptographic keys used to encrypt information managed by said customer, or provides information on how said customer manages cryptographic keys.

11 Physical and environmental security

11.1 Secure areas

Control Objective: To prevent unauthorized physical access, damage and interference to the organization’s information and information processing facilities.

11.1.1 11.1.1 corresponds to the part of 11.1.1 Control in ISO/IEC 27002:2013.

11.1.2 11.1.2 corresponds to the part of 11.1.2 Control in ISO/IEC 27002:2013.

11.1.3 11.1.3 corresponds to the part of 11.1.3 Control in ISO/IEC 27002:2013.

11.1.4 11.1.4 corresponds to the part of 11.1.4 Control in ISO/IEC 27002:2013.

11.1.5 11.1.5 corresponds to the part of 11.1.5 Control in ISO/IEC 27002:2013.

11.1.6 11.1.6 corresponds to the part of 11.1.6 Control in ISO/IEC 27002:2013.

11.2 Equipment

Control Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization’s operations.

11.2.1 11.2.1 corresponds to the part of 11.2.1 Control in ISO/IEC 27002:2013.
11.2.2 11.2.2 corresponds to the part of 11.2.2 Control in ISO/IEC 27002:2013.
11.2.3 11.2.3 corresponds to the part of 11.2.3 Control in ISO/IEC 27002:2013.
11.2.4 11.2.4 corresponds to the part of 11.2.4 Control in ISO/IEC 27002:2013.
11.2.5 11.2.5 corresponds to the part of 11.2.5 Control in ISO/IEC 27002:2013.
11.2.6 11.2.6 corresponds to the part of 11.2.6 Control in ISO/IEC 27002:2013.
11.2.7 11.2.7 corresponds to the part of 11.2.7 Control in ISO/IEC 27002:2013.
11.2.7.4.PB 11.2.7.4.PB corresponds to the 11.2. Implementation guidance for Cloud service provider in ISO/IEC 27017:2015.
11.2.8 11.2.8 corresponds to the part of 11.2.8 Control in ISO/IEC 27002:2013.
11.2.9 11.2.9 corresponds to the part of 11.2.9 Control in ISO/IEC 27002:2013.

12 Operations security

12.1 Operational procedures and responsibilities

Control Objective: To ensure correct and secure operations of information processing facilities.

12.1.1 12.1.1 corresponds to the part of 12.1.1 Control in ISO/IEC 27002:2013.
12.1.2 12.1.2 corresponds to the part of 12.1.2 Control in ISO/IEC 27002:2013.
12.1.2.11.PB The cloud service provider provides cloud service customers with information about changes in cloud services that can adversely affect the information security of cloud service customers.
12.1.3 12.1.3 corresponds to the part of 12.1.3 Control in ISO/IEC 27002:2013.
12.1.3.9.PB 12.1.3.9.PB corresponds to the 12.1. Implementation guidance for Cloud service provider in ISO/IEC 27017:2015.
12.1.4 12.1.4 corresponds to the part of 12.1.4 Control in ISO/IEC 27002:2013.
12.1.5.P 12.1.5.P corresponds to the part of CLD.12.1.5 Control in ISO/IEC 27017:2015 Annex A.
12.1.5.1.PB 12.1.5.1.PB corresponds to the 1st(last) sentence (beginning with "The cloud service") of the 1st(last) paragraph of the Implementation guidance of CLD.12.1.5 in ISO/IEC 27017:2015 Annex A.

12.2 Protection from malware

Control Objective: To ensure that information and information processing facilities are protected against malware.

12.2.1 12.2.1 corresponds to the part of 12.2.1 Control in ISO/IEC 27002:2013.

12.3 Backup

Control Objective: To protect against loss of data.

12.3.1 12.3.1 corresponds to the part of 12.3.1 Control in ISO/IEC 27002:2013.

12.4 Logging and monitoring

Control Objective: To record events and generate evidence.

12.4.1 12.4.1 corresponds to the part of 12.4.1 Control in ISO/IEC 27002:2013.
12.4.1.15.PB 12.4.1.15.PB corresponds to the 12.4.1 Implementation guidance for Cloud service provider in ISO/IEC 27017:2015.
12.4.2 12.4.2 corresponds to the part of 12.4.2 Control in ISO/IEC 27002:2013.

12.4.3 12.4.3 corresponds to the part of 12.4.3 Control in ISO/IEC 27002:2013.

12.4.4 12.4.4 corresponds to the part of 12.4.4 Control in ISO/IEC 27002:2013.

12.4.4.4.PB 12.4.4.4.PB corresponds to the 12.4. Implementation guidance for Cloud service provider in ISO/IEC 27017:2015.

12.4.5.P 12.4.5.P corresponds to the part of CLD.12.4.5 Control in ISO/IEC 27017:2015 Annex A.

12.5 Control of operational software

Control Objective: To ensure the integrity of operational systems.

12.5.1 12.5.1 corresponds to the part of 12.5.1 Control in ISO/IEC 27002:2013.

12.6 Technical vulnerability management

Control Objective: To prevent exploitation of technical vulnerabilities.

12.6.1 12.6.1 corresponds to the part of 12.6.1 Control in ISO/IEC 27002:2013.

12.6.1.18.PB 12.6.1.18.PB corresponds to the 12.6.1 Implementation guidance for Cloud service provider in ISO/IEC 27017:2015.

12.6.2 12.6.2 corresponds to the part of 12.6.2 Control in ISO/IEC 27002:2013.

12.7 Information systems audit considerations

Control Objective: To minimise the impact of audit activities on operational systems.

12.7.1 12.7.1 corresponds to the part of 12.7.1 Control in ISO/IEC 27002:2013.

13 Communications security

13.1 Network security management

Control Objective: To ensure the protection of information in networks and its supporting information processing facilities.

13.1.1 13.1.1 corresponds to the part of 13.1.1 Control in ISO/IEC 27002:2013.

13.1.2 13.1.2 corresponds to the part of 13.1.2 Control in ISO/IEC 27002:2013.

13.1.3 13.1.3 corresponds to the part of 13.1.3 Control in ISO/IEC 27002:2013.

13.1.4.P 13.1.4.P corresponds to the part of CLD.13.1.4 Control in ISO/IEC 27017:2015 Annex A.

13.2 Information transfer

Control Objective: To maintain the security of information transferred within an organization and with any external entity.

13.2.1 13.2.1 corresponds to the part of 13.2.1 Control in ISO/IEC 27002:2013.

13.2.2 13.2.2 corresponds to the part of 13.2.2 Control in ISO/IEC 27002:2013.

13.2.3 13.2.3 corresponds to the part of 13.2.3 Control in ISO/IEC 27002:2013.

13.2.4 13.2.4 corresponds to the part of 13.2.4 Control in ISO/IEC 27002:2013.

14 System acquisition, development and maintenance

14.1 Security requirements of information systems

Control Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

14.1.1 14.1.1 corresponds to the part of 14.1.1 Control in ISO/IEC 27002:2013.
14.1.2 14.1.2 corresponds to the part of 14.1.2 Control in ISO/IEC 27002:2013.
14.1.3 14.1.3 corresponds to the part of 14.1.3 Control in ISO/IEC 27002:2013.

14.2 Security in development and support processes
Control Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.
14.2.1 14.2.1 corresponds to the part of 14.2.1 Control in ISO/IEC 27002:2013.
14.2.1.13.PB 14.2.1.13.PB corresponds to the 14.2.1 Implementation guidance for Cloud service provider in ISO/IEC 27017:2015.
14.2.2 14.2.2 corresponds to the part of 14.2.2 Control in ISO/IEC 27002:2013.
14.2.3 14.2.3 corresponds to the part of 14.2.3 Control in ISO/IEC 27002:2013.
14.2.4 14.2.4 corresponds to the part of 14.2.4 Control in ISO/IEC 27002:2013.
14.2.5 14.2.5 corresponds to the part of 14.2.5 Control in ISO/IEC 27002:2013.
14.2.6 14.2.6 corresponds to the part of 14.2.6 Control in ISO/IEC 27002:2013.
14.2.7 14.2.7 corresponds to the part of 14.2.7 Control in ISO/IEC 27002:2013.
14.2.8 14.2.8 corresponds to the part of 14.2.8 Control in ISO/IEC 27002:2013.
14.2.9 14.2.9 corresponds to the part of 14.2.9 Control in ISO/IEC 27002:2013.

14.3 Test data
Control Objective: To ensure the protection of data used for testing.
14.3.1 14.3.1 corresponds to the part of 14.3.1 Control in ISO/IEC 27002:2013.

15 Supplier relationships
15.1 Information security in supplier relationships
Control Objective: To ensure protection of the organization’s assets that is accessible by suppliers.
15.1.1 15.1.1 corresponds to the part of 15.1.1 Control in ISO/IEC 27002:2013.
15.1.1.14.B 15.1.1.14.B corresponds to the m) part of 15.1.1 Implementation guidance in ISO/IEC 27002:2013.
15.1.1.16.B The cloud service provider evaluates the risk of information handled in the service provided by the cloud service provider being accessed or processed without the cloud service customer's intention as a result of the application of laws and regulations other than domestic laws to the information handled. Based on this evaluations, the cloud service provider selects an external contractor and, if necessary, specify the location where the information handled by the cloud service customer is handled and the governing law and jurisdiction as stipulated in the contract.
15.1.2 15.1.2 corresponds to the part of 15.1.2 Control in ISO/IEC 27002:2013.
15.1.2.18.PB The cloud service provider defines, as part of the agreement, appropriate information security measures to be implemented by the cloud service provider to avoid misunderstandings between the cloud service provider and cloud service customers.
15.1.3 15.1.3 corresponds to the part of 15.1.3 Control in ISO/IEC 27002:2013.

15.2 Supplier service delivery management
Control Objective: To maintain an agreed level of information security and service delivery in

line with supplier agreements.

15.2.1 15.2.1 corresponds to the part of 15.2.1 Control in ISO/IEC 27002:2013.

15.2.2 15.2.2 corresponds to the part of 15.2.2 Control in ISO/IEC 27002:2013.

16 Information security incident management

16.1 Management of information security incidents and improvements

Control Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

16.1.1 16.1.1 corresponds to the part of 16.1.1 Control in ISO/IEC 27002:2013.

16.1.2 16.1.2 corresponds to the part of 16.1.2 Control in ISO/IEC 27002:2013.

16.1.3 16.1.3 corresponds to the part of 16.1.3 Control in ISO/IEC 27002:2013.

16.1.4 16.1.4 corresponds to the part of 16.1.4 Control in ISO/IEC 27002:2013.

16.1.5 16.1.5 corresponds to the part of 16.1.5 Control in ISO/IEC 27002:2013.

16.1.6 16.1.6 corresponds to the part of 16.1.6 Control in ISO/IEC 27002:2013.

16.1.7 16.1.7 corresponds to the part of 16.1.7 Control in ISO/IEC 27002:2013.

16.1.7.13.PB 16.1.7.13.PB corresponds to the 16.1.7 Implementation guidance for Cloud service provider in ISO/IEC 27017:2015.

17 Information security aspects of business continuity management

17.1 Information security continuity

Control Objective: Information security continuity should be embedded in the organization's business continuity management systems.

17.1.1 17.1.1 corresponds to the part of 17.1.1 Control in ISO/IEC 27002:2013.

17.1.2 17.1.2 corresponds to the part of 17.1.2 Control in ISO/IEC 27002:2013.

17.1.3 17.1.3 corresponds to the part of 17.1.3 Control in ISO/IEC 27002:2013.

17.2 Redundancies

Control Objective: To ensure availability of information processing facilities.

17.2.1 17.2.1 corresponds to the part of 17.2.1 Control in ISO/IEC 27002:2013.

18 Compliance

18.1 Compliance with legal and contractual requirements

Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

18.1.1 18.1.1 corresponds to the part of 18.1.1 Control in ISO/IEC 27002:2013.

18.1.2 18.1.2 corresponds to the part of 18.1.2 Control in ISO/IEC 27002:2013.

18.1.2.13.PB 18.1.2.13.PB corresponds to the 18.1.2 Implementation guidance for Cloud service provider in ISO/IEC 27017:2015.

18.1.3 18.1.3 corresponds to the part of 18.1.3 Control in ISO/IEC 27002:2013.

18.1.3.13.PB 18.1.3.13.PB corresponds to the 18.1.3 Implementation guidance for Cloud service provider in ISO/IEC 27017:2015.

18.1.4 18.1.4 corresponds to the part of 18.1.4 Control in ISO/IEC 27002:2013.

18.1.5 18.1.5 corresponds to the part of 18.1.5 Control in ISO/IEC 27002:2013.

18.1.5.7.PB 18.1.5.7.PB corresponds to the 18.1. Implementation guidance for Cloud service provider in ISO/IEC 27017:2015.

18.2 Information security reviews

Control Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

18.2.1 18.2.1 corresponds to the part of 18.2.1 Control in ISO/IEC 27002:2013.

18.2.2 18.2.2 corresponds to the part of 18.2.2 Control in ISO/IEC 27002:2013.

18.2.3 18.2.3 corresponds to the part of 18.2.3 Control in ISO/IEC 27002:2013.

(Appendix 1) Points to be noted in the selection of detailed controls and their implementation

A cloud service provider who applies for registration to the ISMAP Cloud Service List need to select detailed controls in accordance with the Control Criteria of ISMAP, and effectively implement the established control. At that time, the cloud service provider especially takes sufficient measures for the critical areas to reduce the risks that can seriously affect the information security of the cloud service and lead to serious incidents, and tries to reduce the risks that can lead to serious incidents.

The above critical areas include the following four areas.

1. Access management (privilege management, ID management, physical security, etc.)
2. Management related to system development and changes (development management, change management)
3. System operation management (vulnerability management, cryptographic processing, media disposal, fault management, system operation monitoring, network management, ensuring redundancy, etc.)
4. Outsourcer management (related to 1. to 3.)

(Reference 1) Approach to references to each standard

As prescribed in Chapter 1, this Control Criteria was created based on international standards, referring to the Common Standards for Information Security Measures for Government Agencies and Related Agencies (FY 2018 version) (below "Common Standards") and NIST SP800-53 rev.4 (below, "SP800-53"). This section describes this approach to referring to these standards.

The reference to JIS Q 27014:2015 (ISO/IEC 27014:2013) in the governance criteria is based on the following approach.

- General, outline, and principles are not subject to assessment, but are positioned as reference information when conducting an assessment.
- Process control objectives are also be positioned as explanations of detailed controls.

In addition, the following changes have been made from JIS Q 27014:2015 (ISO/IEC 27014:2013) in order to make the content easier to understand.

- Unification of subject to the governing body
- Replacement of "executive management" with "administrator"
- Reorganization of closely related content as embodiment of a single criteria

The common standards stipulate the items that government agencies, etc. should comply with. These items can be achieved only when a cloud service customer takes additional measures in addition to the measures that should be taken by a cloud service provider, and it is not appropriate to require the items in the common standards of a cloud service provider as is. For this reason, in accordance with the purpose of the government common standards, and taking into consideration the matters that cloud service providers should perform as the main entity, after reading the items as standard criteria, the matters deemed to be required of a cloud service provider were added and some additions were made from the perspective of whether or not the matters would hinder a cloud service customer from meeting the uniform criteria if a cloud service provider does not implement them.

In addition, most of the criteria used as reference including the common standards are implemented by customers of on-premise information systems, and were not developed assuming a cloud service providers as the implementer. From this perspective, they were replaced with the following three controls patterns.

- Controls pattern 1: Cloud service providers should implement the relevant controls by themselves
- Controls pattern 2: For government agencies to implement the relevant controls , cloud service providers should provide functions.
- Controls pattern 3: For government agencies to enable to implement the relevant controls , cloud service providers should provide information.

SP800-53 was used as a reference in considering the criteria because it has been in operation for a long time among overseas standards and has been updated multiple times. At this time, because it targets cloud services, the level was set assuming the handling of confidential 2 information, which is most frequently handled by the government, and from the viewpoint of the correspondence with international standards, the items that are considered moderate requirements in FedRAMP but are not addressed in ISO/IEC 27001 were narrowed down and added, and some contents were added.

(Reference 2) Points to note regarding attached tables

Attached table 2. Management criteria

- Controls marked as "changed" in the "Type of change" column indicate that the controls in the Cloud Information Security Management Standard have been partially changed.

Attached table 3. Controls criteria

- Type of change column legend

  Changed: A control that has been partially changed of the controls in the Cloud Information Security Management Standard.

  Addition: A control that does not exist in the controls of the Cloud Information Security Management Standard, but is added in this Control Criteria.

  Missing: A control for cloud service customers in the Control Criteria of the Cloud Information Security Management Standard, and deleted in this Control Criteria which is implemented by cloud service providers.

Attached table 4. Mapping (control criteria vs. common standards),
Attached table 5. Mapping (common standards vs. control criteria)

- This mapping shows the items that are related at the control objectives level, based on the detailed controls, in order to provide a reference for the relationship with other criteria. However, it only shows the items that are closely related and does not show that the mapped items have a necessary and sufficient relationship with each other.
- In addition, in Attached table 5, because this criteria is a control criteria in which the cloud service provider is the implementation entity as specified in 1.2, the mapping of the Part 4 of the common standards in this mapping is done assuming that the cloud service provider is the entruster.

Attached table 6. Mapping (control criteria vs. SP800-53),
Attached table 7. Mapping (SP800-53 vs. control criteria)

- This mapping shows the items that are related at the control objectives level, based on the detailed controls, in order to provide a reference for the relationship with other criteria. However, it only shows the items that are closely related and does not show that the mapped items have a necessary and sufficient relationship with each other.
- Note that there are additional controls that have been added to the correspondence shown in SP800-53 in the process of developing this Control Criteria.

Attached table 8. Examples of frequency of implementation of individual controls

- In principle, individual controls are implemented at a frequency determined by the cloud service provider based on the service contents and the results of security risk analysis, etc. However, this table is provided as a reference for determining the frequency.

Attached table 8:Examples of frequency of implementation of individual controls

No.	Main assessment target	Examples of frequency of implementation
1	Regulations, etc.	At least once a year
2	Basis documents, records, etc. (1) Items for which sample tests are not conducted (Design document, specification document, procedure document, etc.)	At least once a year, or whenever a change occurs
3	Basis documents, records, etc. (2) Items for which sample tests are not conducted (Application forms, approval records, system logs, ledgers, etc.)	As needed (once a day, once a week, once a month, once a quarter, etc., depending on the nature of the control)
4	Basis settings, etc. (Parameters, status, commands, etc.)	At least once a year, or whenever a change occurs
5	Facilities, buildings, etc.	At least once a year (same as No. 3 above for review of access logs to facilities, etc.)

*Items subject to assessment procedures for individual controls. Details are defined in the ISMAP Standard Assessment Procedure.