ISMS

Information Security Management Systems

Accreditation Criteria and Guidance for ISMS Certification Bodies
JIP-ISAC100E-3.1a

April 2, 2018

ISMS-AC
1-9-9 Roppongi, Minato-ku, Tokyo 106-0032 Japan
Tel.+81-3-5860-7570　　Fax.+81-3-5573-0564
URL　http://www.isms.jipdec.or.jp/

This document is translated into English by ISMS-AC.
The Japanese version shall be the authorized version.
In the event of any question as to the English version, comply with the original (Japanese) version.

ISMS-AC

General

This document specifies general requirements and guidance for a third-party body operating certification of Information Security Management Systems (ISMS) to be recognized as competent and reliable in the operation of ISMS certification.
ISO/IEC 27006: 2015 Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems, shall be applied as they are to the relevant clauses in this criteria and guidance unless otherwise specified.

Introduction

"Introduction" in ISO/IEC 27006: 2015 shall be referred to and applied.

1. Scope

"1. Scope" in ISO/IEC 27006: 2015 shall be applied.

2. Normative references

"2. Normative references" in ISO/IEC 27006: 2015 shall be applied.

3. Terms and definitions

"3. Terms and definitions" in ISO/IEC 27006: 2015 shall be applied.

4. Principles

"4. Principles" in ISO/IEC 27006: 2015 shall be applied.

5. General requirements

"5. General requirements" in ISO/IEC 27006: 2015 shall be applied.

6. Structural requirements

"6. Structural requirements" in ISO/IEC 27006: 2015 shall be applied.

7. Resource requirements

"7. Resource requirements" in ISO/IEC 27006: 2015 shall be applied.

8. Information requirements

"8. Information requirements" in ISO/IEC 27006: 2015 shall be applied.

9. Process requirements

"9. Process requirements" in ISO/IEC 27006: 2015 shall be applied.

10. Management system requirements for certification bodies

"10. Management system requirements for certification bodies" in ISO/IEC 27006: 2015 shall be applied.

Annex A

"Annex A" in ISO/IEC 27006: 2015 shall be applied.

Annex B

"Annex B" in ISO/IEC 27006: 2015 shall be applied.

Annex C

"Annex C" in ISO/IEC 27006: 2015 shall be applied.

Annex D

"Annex D" in ISO/IEC 27006: 2015 shall be applied.

Annex E (Normative)
Additional requirements and guidance for certification bodies Providing the ISMS Cloud Security Certification

E.1 Competence of personnel

In addition to the requirements in clause 7.1 of ISO/IEC 27006, auditors of the ISMS Cloud Security Certification shall have the following knowledge.

a) Cloud infrastructure / elemental technology (virtualization, etc.)
b) The requirements related to the ISMS Cloud Security Certification based on ISO/IEC 27017:2015 (JIP-ISMS517-1.0)
c) Relevant legal and regulatory requirements
d) Information security risks specific to cloud

E.2 Selecting audit team members for the ISMS Cloud Security Certification

In addition to the requirements in clause 7.2.1 IS 7.2 of ISO/IEC 27006, auditors of the ISMS Cloud Security Certification shall demonstrate their knowledge and skills specific to cloud security by CPD (Continuing Professional Development).

E.3 Certification documents

E.3.1 Certification documents

In addition to the requirements in clause 8.2.2 of ISO/IEC 27006, the following requirements apply.

E.3.1.1 Scope

Regarding the requirement in 8.2.2 f) of ISO/IEC 17021-1 (the scope of certification with respect to the type of activities, products and services as applicable at each site without being misleading or ambiguous), cloud services can be identified in the description of the scope in the certification document of the ISMS Cloud Security Certification and clearly stated in a non-misleading expression.

Note 1: When the name of the cloud service is not mentioned in the certification document, for example, it can be misunderstood as if all services are certified even though only a part of the multiple services provided by the organization is included in the scope. In order to prevent this, the cloud service name shall be clearly stated in the certification document of the ISMS Cloud Security Certification.

Note 2: The ISMS Cloud Security Certification is a management system certification for an organization, not a product or service.

E.3.1.2 Cloud service providers and cloud service customers

Since the ISMS Cloud Security Certification is applicable to a cloud service provider and a cloud service customer, it shall be clearly stated in the certification document (ISO/IEC 17021-1 clause 8.2.2 certification document) that the organization is certified as a cloud service provider or a cloud service customer, or as both of them.

E.3.1.3 Other information required by standards used in certification and/or other normative documents

Since the applicable standard for the ISMS Cloud Security Certification is ISO/IEC 27001 and JIP-ISMS517, it shall be stated in the certification document that the organization conforms to JIP-ISMS517. In addition, ISO/IEC 27001 which is the basis of the ISMS Cloud Security Certification shall be clearly identified in the certification document.

E.3.1.4 Expiration date of ISMS Cloud Security Certification

The expiration date of the ISMS Cloud Security Certification shall not exceed the expiration date of the base ISO/IEC 27001 certification.

When ISO / IEC 27017 is mentioned in the certification document, it shall be clearly stated that ISO / IEC 27017 is a guideline.

An example of description (a case where an organization is certified as both a cloud service provider and a cloud service customer)

> The organization is found to comply with JIP-ISMS517-1.0 as a cloud service provider and cloud service customer in line with the guidelines in ISO/IEC 27017:2015.

E.4 Audit time

In addition to the requirements in clause 9.1.4.1 IS 9.1.4 in ISO/IEC 27006, additional audit time for the ISMS Cloud Security Certification shall be calculated.

Note 1: The additional audit time for the ISMS Cloud Security Certification is based on the ISO/IEC 27001 audit time for the scope of the ISMS Cloud Security

Certification.

Note 2: Annex F (Informative) provides additional guidance for the formula to calculate the audit time.

E.5 Suspension, withdrawal and reduction of certification

If the ISO/IEC 27001 certification which is the basis of the ISMS Cloud Security Certification is suspended, withdrawn or reduced, the ISMS Cloud Security Certification shall also be suspended, withdrawn or reduced.

Annex F (Informative)
Calculation method of audit time for ISMS Cloud Security Certification

F.1 General

The audit time for the ISMS Cloud Security Certification is calculated by taking into account the requirements for the ISMS Cloud Security Certification (JIP-ISMS517), the types of the organization (cloud service provider and/or customer), types of cloud services, system configuration and the number of service users.

This annex provides additional guidance for the formula to calculate the audit time for the ISMS Cloud Security Certification in addition to the audit time for ISO/IEC 27001. Table F.1 shows examples of the classification of factors that can be used as the basis for calculating the audit time when extending to the ISMS Cloud Security Certification together with the ISO/IEC 27001 surveillance audit or recertification audit.

The additional audit time for extending to the ISMS Cloud Security Certification is based on the audit time for the initial audit of ISO/IEC 27001.

When the ISMS Cloud Security Certification audit is carried out independently, one auditor-day should be added in addition to the audit time in Table F.1.

After the extension to the ISMS Cloud Security Certification, the audit time shown in Table F.1 shall be added to the audit time of surveillance or recertification audit of ISO/IEC 27001 for the scope of the ISMS Cloud Security Certification.

Table F.1 The examples for the classification of factors to calculate audit time
(a case where the extension to the ISMS Cloud Security Certification is conducted with ISO/IEC 27001 surveillance or recertification audit)

	Factors to increase the audit time related to the controls in ISO/IEC 27017	Factors to increase the audit time related to the types of cloud services	Additional audit time*
Cloud service provider	40/114 = 40%	$+\alpha$	40% $+\alpha$
Cloud service customer	40/114 = 40%	$+\alpha$	40% $+\alpha$

Cloud service provider and customer	80/114 = 70%	+ α	70% + α

*"Additional audit time" here means the audit time for the ISMS Cloud Security Certification to be added to the audit time for ISO/IEC 27001.

If the ISMS Cloud Security Certification is extended at the time of ISO/IEC 27001 surveillance audit or recertification audit, the audit is not necessary to be conducted in an equivalent manner as the initial audit (Stage 1 + Stage 2) because the ISMS Cloud Security Certification is an extension to ISO/IEC 27001 certification.