Basic Regulations for Information system Security Management and Assessment Program (ISMAP)

June 3, 2020

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

Table of Contents

Chapter 1 General Rules

1.1 Purposes of the regulations

The regulations are to, based on the Basic framework of the Government Information system Security Management and Assessment Program for Cloud Services (established by Cyber Security Strategic Headquarters on January 30, 2020. Hereinafter referred to as “the decision of Strategic Headquarters”), determine the Information system Security Management and Assessment Program (hereinafter referred to as the “System”), which is operated by the Cabinet Secretariat (National Center of Incident Readiness and Strategy for Cybersecurity (NISC), IT Comprehensive Strategy Headquarters, National Strategy Office of Information and Communications Technology), Ministry of Internal Affairs and Communications, and Ministry of Economy Trade and Industry, as well as the basic matters of the System that should be observed by cloud service providers, assessors, ministries responsible for the System, ISMAP Steering Committee, procuring ministries, etc.

1.2 Purposes of the System

This System is to arrange the assessment and pre-registration of cloud services that meet the security requirements of the government, ensure the security level for cloud service procurement by the government, and contribute to the smooth introduction of cloud services.

1.3 Name of the System

The System is referred to as the “Information system Security Management and Assessment Program (ISMAP)”.

1.4 Definition of terms

1.4.1 Cloud service

Applying the definition in the “Basic Policy on the Use of Cloud Services in Governmental Information Systems” (established by the Liaison Meeting of the CIO of each Ministry on June 7, 2018), a “cloud service” means “a service which is offered via a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with services that allow for resources to be freely set and managed by users utilizing a provider-defined interface, and that also offers flexibility in adequately setting information security conditions.”

1.4.2 Cloud service provider

This refers to an operator that provides its own cloud service.

1.4.3 Assessor

In the System, this refers to a corporation which has completed registration in accordance with the

conditions set out in 4.3 and acts as the main party for conducting the assessment of cloud services.

1.4.4 Ministries responsible for the System

These are the ministries that operate the System, namely, the Cabinet Secretariat, Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry.

1.4.5 ISMAP Steering Committee

This refers to the highest organ of decision-making for the operation of this System consisting of experts, etc., and which is established under the responsible ministries based on the decision of Strategic Headquarters. In addition, an executive office to run the ISMAP Steering Committee shall be established within NISC.

1.4.6 ISMAP Operations Support Organization

This refers to the organization that was commissioned to handle administrative tasks related to the operations of the System by the ISMAP Steering Committee based on the provisions of 9.3.

1.4.7 Procuring ministries, etc.

In the System, this refers to government organizations, independent administrative corporations, and designated corporations (hereinafter referred to as the “Government Organizations, etc.”) which procure the cloud services.

1.4.8 Registration

This is the process by which the ISMAP Steering Committee confirms that an applying cloud service satisfies the System’s requirements defined in the provisions of Chapter 3, and then lists the cloud service on the ISMAP Cloud Service List stated in 1.4.12, or confirms that an applying assessor satisfies the System’s requirements defined in the provisions of Chapter 4, and then lists the company on the ISMAP Assessor List stated in 1.4.13.

1.4.9 Assessment

In the System, this refers to the information security assessment that is conducted by an assessor based on the standards, procedure, etc. defined for the System, to check the validity of the statement regarding the control of cloud service providers for the cloud service for which registration is requested by the operator. The assessment consists of two procedures; the design assessment and operational assessment.

1.4.10 Design assessment

This refers to the evaluation as to whether a cloud service provider has selected a control target and detailed control measures based on the ISMAP control criteria and has prepared the necessary

control measures at one point during the assessment period.

1.4.11 Operational assessment

This refers to the evaluation as to whether a cloud service provider has selected a control target and detailed control measures based on the ISMAP control criteria and the control measures that the operator has arranged are being operated effectively during the assessment period.

1.4.12 ISMAP Cloud Service List

This refers to a publicly available list of cloud services that were confirmed by the ISMAP Steering Committee, based on the provisions of Chapter 3 of this regulations, to have implemented security measures in accordance with the criteria required by the System.

1.4.13 ISMAP Assessor List

This refers to a publicly available list of corporations that were confirmed by the ISMAP Steering Committee, based on the provisions of Chapter 4 of this regulations, to have satisfied the requirements as an assessor mandated by the System.

Chapter 2 Structure of the System

2.1 Regulations for the System, etc.

Regulations for the System, etc. should be as follows: As a general rule, regulations, etc. should be published, however, the distribution of ISMAP standard assessment procedures shall be limited to assessors only.

The document that defines basic matters that should be observed by cloud service providers, procuring ministries, assessors, responsible ministries for the System and the ISMAP Steering Committee.

<Documents for Government Information system Security Management and Assessment Program for Cloud Services>	
“ISMAP Basic Regulations”	These regulations define the overall concept and structure of Government Information system Security Management and Assessment Program for Cloud Services. In other documents related to the System, this is referred as the “Basic Regulations”.

The document that defines basic matters that should be observed by ministries responsible for the System and the ISMAP Steering Committee.

<Documents related to the operations of the ISMAP Steering Committee>	
“Basic Policies Regarding the ISMAP Steering Committee”	It defines the basic matters concerning the composition of the ISMAP Steering Committee and the affairs under its jurisdiction, etc.
“ISMAP System Operation Regulations”	It defines the details for the operation of the System and the organization and procedures of the ISMAP Steering Committee.

The matters that shall be observed by responsible ministries, the ISMAP Steering Committee and cloud service providers that apply for registration.

<Documents related to the registration of cloud service>	
“ISMAP Cloud Service Registration Rules”	It defines the procedure and requirements related to cloud service registration for the System and the matters to be assessed regarding the application. (Hereinafter referred to as the “Service Registration Rules” of the regulations.)
“Requirements for Applicants”	Requirements for cloud service providers for the Government Information System.
“Control Criteria of ISMAP”	The criteria that become the subject of assessment as one of the requirements for cloud service security for the Government Information System (Hereinafter referred to as the “control criteria” of the regulations.)

The matters that shall be observed by responsible ministries, the ISMAP Steering Committee and assessors that apply for registration.

<Documents related to the registration of an assessor>	
“ISMAP Registration Rules for Assessors”	It defines the procedure and requirements related to the assessor registration for the System and the matters to be assessed regarding the application. (Hereinafter referred to as the “Registration Rules for Assessors” of the regulations.)
“Requirements for ISMAP assessor”	Requirements for the assessors that conduct an assessment of the System.

Matters that should be observed by assessors at the time of assessment.

<Documents related to the norms and procedure for assessment administrative tasks> (Hereinafter collectively referred to as the “assessment criteria”)>	
“Information Security Audit Criteria”	This refers to the “Information Security Audit Criteria” specified by Ministry of Economy, Trade and Industry. As

	the rules that shall be observed by assessors and assessment professionals at the time of assessing based on the System, they serve as the premise of the “ISMAP Information Security Assessment Guideline”.
“ISMAP Information Security Assessment Guideline”	This is the guideline that defines the detailed matters that should be observed by assessors and assessment professionals at the time of assessment based on the System.
“ISMAP Standard Assessment Procedure”	Document that defines the assessment standard procedures and methodologies related to the individual control measures defined by control criteria that should be observed by assessors and assessment professionals at the time of assessment based on the System.

2.2 Persons who constitute the System

The persons who constitute the System are cloud service providers, assessors, ministries responsible for the System, the ISMAP Steering Committee and procuring ministries.

2.3 Basic framework of the System

With the System, the ISMAP Steering Committee defines the requirements for cloud services and ISMAP control criteria, which serve as the standards for information security control and operations. Then, the ISMAP Steering Committee has an assessor assess if a cloud service application satisfies the requirements based on the ISMAP Cloud Service Registration Rules. It needs to be confirmed that the assessor conforms to the Requirements for ISMAP assessor, which are specified separately for the System. Upon receiving an application from a cloud service provider, the cloud service should be assessed, and it needs to be verified that it implements security measures based on the control criteria in accordance with the assessment criteria. When the registration of the cloud service is confirmed to be appropriate, it is listed on the ISMAP Cloud Service List. As a general rule, procuring ministries, etc. shall procure a service from the cloud services listed on the ISMAP Cloud Service List.

Chapter 3 Registration of Cloud Service

This chapter defines the basic matters including a series of requirements and procedures related to cloud service registration. Detailed matters regarding the requirements and procedures are specified in the ISMAP Cloud Service Registration Rules.

3.1 Application for registration

When a cloud service provider requests for its own cloud service to be registered in the System, it shall apply for registration through the ISMAP Steering Committee.

3.2 Assessment

A cloud service provider that requests registration under the System shall declare the compliance status of the control criteria prior to applying for registration. Then, it should select one of the assessors registered based on the provisions of Chapter 4 and undergo an assessment by the assessor. Moreover, regarding the compliance status with respect to the control criteria, an assessor shall conduct an assessment based on the assessment criteria, etc., prepare an Assessment Report for the results, and provide it to the cloud service provider.

3.3 Acceptance and examination of application

When a cloud service provider requests registration for its cloud service under the System, provided there is no specific deficiency in the application, the ISMAP Steering Committee shall accept the application and examine its appropriateness for registration. The ISMAP Steering Committee may request the cloud service provider and the assessor that conducts the assessment of the cloud service to provide the necessary information.

3.4 Decision on registration

For the applying cloud service, the ISMAP Steering Committee shall approve the registration when it has determined that it is appropriate based on the examination.

3.5 Renewal of registration

Effective period of registration prescribed in 3.4 is from the day after the last day of the assessment period covered by the registration to 16 months later. Cloud service providers should apply for the renewal of registration by the end of the effective period. The registration shall remain effective after the expiration of the effective period until such time the ISMAP Steering Committee decides whether the renewal of registration can be approved.

Regarding the series of requirements and procedures related to the renewal of the registration, the provisions of this Chapter apply.

3.6 Announcement/Publication and use of the list

When the ISMAP Steering Committee approves the registration of a cloud service based on 3.4, it shall promptly list the cloud service on the ISMAP Cloud Service List to publicize it. When it accepts a renewal of the registration of the cloud service based on 3.5, it should update the necessary information. The ISMAP Cloud Service List should include the name of the cloud service to be registered, the effective period of the registration and other required information as defined in the ISMAP Cloud Service Registration Rules.

3.7 Report

Cloud service providers shall immediately send a summary report to the ISMAP Steering Committee when there is an information security incident which could have a significant impact on users of its own registered service.

3.8 Notification

A cloud service provider shall, with respect to the service registered, report to the ISMAP Steering Committee without delay when there are changes to the information described in the ISMAP Cloud Service List, or when there are significant control changes or there are circumstances that could result in such changes during the registration period.

Chapter 4 Registration of Assessor

This chapter defines the basic matters including a series of requirements and procedures related to assessor registration. Detailed matters regarding the requirements and procedures are specified in the ISMAP Registration Rules for Assessors.

4.1 Application for registration

A company that makes a request for an assessor to be registered in the System shall submit an application for registration to the ISMAP Steering Committee. (A company that requests registration based on the regulations is hereinafter referred to as an “Applicant”.)

4.2 Acceptance and examination of application

When an applicant submits an application, provided there is no specific deficiency in the application, the ISMAP Steering Committee shall accept the application and examine the appropriateness of registration. For the examination, the ISMAP Steering Committee may request the applicant to provide the necessary information.

4.3 Decision on registration

For an application for registration based on the provisions of 4.1, the ISMAP Steering Committee shall approve the registration of an applicant when it has determined that the application is appropriate.

4.4 Renewal of registration

The effective period of a registration which has been approved based on 4.3 shall be two years from the date the application for registration was made. Assessors should apply for renewal of registration by the end of the effective period. The registration shall remain effective after the expiration of the effective period until such time the ISMAP Steering Committee decides whether the renewal of registration can be approved.

Regarding the series of requirements and procedures related to the renewal of the registration, the provisions of this Chapter apply.

4.5 Announcement/Publication and use of the list

When the ISMAP Steering Committee approves the registration of an assessor based on 4.3, it shall promptly list the institution on the ISMAP Assessor List to publicize it. When it accepts the renewal of the registration based on 4.4, it should update necessary information. The ISMAP Assessor List should include the name of the assessor to be registered, the effective period of the registration and other required information as defined by the Assessor Registration Rules.

4.6 Report

An assessor shall report the status of compliance with the Requirements for ISMAP assessor to the ISMAP Steering Committee after 12 months have elapsed from the date of application for registration or the date for renewal of the registration.

4.7 Notification

An assessor shall promptly notify the ISMAP Steering Committee when there are any changes in the information after the application for registration has been submitted.

Chapter 5 Monitoring, Re-assessment, Suspension, and Cancellation of Registration, Etc.

5.1 Monitoring

Based on the ISMAP Cloud Service Registration Rules/ISMAP Registration Rules for Assessors, the ISMAP Steering Committee may investigate a cloud service registered on the ISMAP Cloud Service List or assessors registered on the ISMAP Assessor List as required, for such reasons as the status of compliance with the System.

5.2 Re-assessment

For a registered cloud service, based on the content of the application specified in 3.8 and the monitoring results stipulated in 5.1, the ISMAP Steering Committee may request the cloud service provider to have re-assessment conducted by an assessor in accordance with ISMAP Cloud Service Registration Rules.

5.3 Reapplication

Regarding registered cloud service providers and assessors, the ISMAP Steering Committee may request a cloud service provider or an assessor to apply for registration again as required in

accordance with ISMAP Cloud Service Registration Rules/ISMAP Registration Rules for Assessors. For re-examination and reregistration after reapplication, the provisions of 4.2 and 4.3 are applied, respectively.

5.4 Temporary suspension or revocation of registration

Based on the results of monitoring, re-examination or re-assessment, the ISMAP Steering Committee may temporarily suspend or revoke the registration of a cloud service which was on the ISMAP Cloud Service List or an assessor which was on the ISMAP Assessor List, in accordance with the ISMAP Cloud Service Registration Rules/ISMAP Registration Rules for Assessors. When the cloud service provider or assessor fails to comply with a request from the ISMAP Steering Committee based on this System without justifiable grounds, similar measures may be taken.

Chapter 6 Rights of Registered Cloud Service Provider and Assessor

6.1 Rights of registered cloud service provider

A registered cloud service provider has the right to state that its service is a cloud service which was registered with the System for the procurement of a cloud service used in the information system of the government.

6.2 Rights of registered assessor

A registered assessor has the right to conduct an assessment of the System based on a request from a cloud service provider that wishes to be registered with the System.

Chapter 7 Scope of Responsibility of System Participants

7.1 ISMAP Steering Committee

For the operation of the System, the ISMAP Steering Committee is responsible for operating the System in compliance with the basic framework of the System stipulated in the decision of Strategic Headquarters, and reviewing the System to check if it is flexible enough to facilitate smooth operation of the System.

For registration of a cloud service, registration of an assessor and the establishment, revision, and abolition etc. of the rules of the System, the ISMAP Steering Committee is fully accountable for decision-making.

7.2 Ministries responsible for the System

For the operation of the System, regarding the commission of administration tasks stipulated in 9.3,

ministries responsible for the System should properly supervise an ISMAP Operations Support Organization and support them so they can process tasks effectively. In addition, to facilitate smooth operation of the System, it is responsible for coordinating with the ISMAP Steering Committee and procuring ministries, etc. and providing information, etc.

7.3 Cloud service provider

Cloud service providers are responsible for complying with the regulations and rules of the System, and regarding items required by the provisions of the System, faithfully executing the matters specified in the application for the registration. In addition, they are obliged to extend necessary cooperation as requested by the ISMAP Steering Committee

7.4 Assessor

Assessors are responsible for complying with the regulations and rules of the System regarding the registration of an assessor, and faithfully conducting assessments in accordance with the assessment criteria, etc.

7.5 Procuring ministries, etc.

Procuring ministries, etc. are responsible for understanding the purpose of the System and assuring the security of the entire information system that they procure.

Chapter 8 Operations Conducted by ISMAP Steering Committee

The ISMAP Steering Committee conducts the matters stipulated in Chapters 3 to 5 and the following:

8.1 Arrangement of regulations, etc.

The ISMAP Steering Committee shall establish, revise, and abolish the regulations stipulated in 2.1 except “Basic Policies Regarding the ISMAP Steering Committee” and “Information Security Audit Criteria”, as well as interpreting these regulations as required.

8.2 Issuance and announcement/publication of guidance

The ISMAP Steering Committee shall use its website, etc. to announce/publicize the guidance for the regulations and rules of the System.

Chapter 9 Others

9.1 Confidentiality

Persons who are members of the ISMAP Steering Committee, ministries responsible for the System,

ISMAP Operations Support Organization, and contractors shall prevent unauthorized persons from accessing confidential information during the operation of the System, as this may compromise the confidentiality of the information.

9.2 Prohibited matters

Persons who are members of the ISMAP Steering Committee, ministries responsible for the System, ISMAP Operations Support Organization, and contractors shall not do the following:

(1) Obtain profit that could affect the results of assessment, examination, and registration.
(2) Provide consulting services to persons who apply a request for assessment, examination, and registration.

9.3 Commission of administration tasks

In accordance with the ISMAP System Operation Regulations, the ISMAP Steering Committee shall commission the administration tasks for the operation of the System to an ISMAP Operations Support Organization, Information-technology Promotion Agency, Japan (hereinafter referred to as “IPA”). IPA shall process commissioned administration tasks as an ISMAP Operations Support Organization under the supervision of the ministries responsible for the System.

9.4 Establishment of additional rules, etc.

In addition to the items specified in the regulations, the ISMAP Steering Committee shall define the matters required for the operation of the System which are not stipulated in the ISMAP System Operation Regulations and documents stated in 2.1.

9.5 Consideration for the decisions made by the Cyber Security Measure Promotion Council and the Liaison Meeting of the Chief Information Officer (CIO) of Each Ministry

For the execution of the provisions contained in Chapters 3 and 4 of the regulations, the matters to be considered required for the System that were determined by the Cyber Security Measure Promotion Council and the Liaison Meeting of the Chief Information Officer (CIO) of Each Ministry shall be noted.

Supplementary provisions (Enacted on June 3, 2020)
(Effective period)
1. These Regulations will come into effect on June 3, 2020.

(Special cases at the time the System is started)
2. For a certain period after enforcement of the System has started, independent administrative

corporations and designated corporations shall not be recognized as procuring ministries, etc.

3. The assessment for a cloud service that had applied for registration within 12 months after the enforcement of the regulations shall conduct the design assessment only.