ISMAP
Information Security Assessment Guidelines

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 Purpose of These Guidelines

These guidelines establish matters that shall be observed in order for the assessor to implement procedures and report the results of the assessment in this program in accordance with the Information Security Audit Criteria, these guidelines and ISMAP Standard Assessment Procedures (hereinafter referred to as "information security assessment criteria") with the intention of being used by the ISMAP Steering Committee as a reference to examine the registration of cloud services on the ISMAP Cloud Services List. These guidelines are applied based on Information Security Audit Criteria (Ministry of Economy, Trade and Industry Notification No. 114 of 2003), but the scope of compliance is limited to the advisory audit portion of the criteria.

1.2 Features of Assessment in This Program

Assessment in this program is conducted to confirm the status of design and operation of internal control over information security in accordance with the Control Criteria of ISMAP for the cloud services subjected to registration examination in the ISMAP Cloud Services List registration examination carried out by the ISMAP Steering Committee. The purpose of the assessment in this program is for the assessor to implement procedures in accordance with information security assessment criteria at the request of the cloud service provider and to report the results in a factual manner. The assessment report prepared by the assessment professional will be submitted by the cloud service provider to the ISMAP Steering Committee as an attachment to the application for service registration, and will be used as a reference when examining the registration to the ISMAP Cloud Service List.
For this reason, in the assessment in this program, the report of the assessment professional is limited to a factual report of the results of the implementation of the procedures and does not report or provide any assurance on the conclusions drawn from the results of the implementation of the procedures. The purpose of the assessment in this program is not to obtain sufficient and appropriate evidence on which to base its conclusions, which is different in nature from assurance engagement. Furthermore, in the assessment in this program, the assessment professional does not apply the concept of materiality or determine procedures based on risk assessment, does not evaluate the risk that users of the assessment report will draw improper conclusions based on the assessment professional’s report, and does not evaluate the sufficiency of the procedures performed or the evidence obtained.

1.3 Definition of Terms

For the purpose of these guidelines, the terms are defined as follows. For definitions other than those given in this section, the definitions of terms in the Basic Regulations for Information system Security Management and Assessment Program (ISMAP) (hereinafter referred to as "ISMAP Basic Regulations") shall be used.

1.3.1 Assessment in This Program

The assessment in this program is the engagement to be implemented at the request of the client, the cloud service provider in order for the cloud service provider to attach it when they apply for registration to the ISMAP Cloud Service List to be used as a reference for examination by the ISMAP Steering Committee. In the assessment in this program, the assessment professional implements procedures in accordance with the information security assessment criteria to assess the status of design and operation of internal control over information security for cloud services subject to registration examination based on the Control Criteria of ISMAP, and reports the results of the assessment based on fact.

1.3.2 ISMAP Assessor List

A public list of legal entities that have been identified by the ISMAP Steering Committee as meeting

the requirements under this Program as an assessor, as defined in the ISMAP Basic Regulations.

1.3.3 Assessor
As defined in the ISMAP Basic Regulations, an entity who mainly implements assessment in this program and has been registered on the ISMAP assessor list after being examined by the ISMAP Steering Committee and confirmed to meet the requirements of the ISMAP Registration Rules for Assessors.

1.3.4 Client
The client refers to a person who concludes an engagement letter with an assessment professional for the purpose of requesting an assessment in this Program and a cloud service provider as defined in the Basic Regulations.

1.3.5 Engagement Partner
Refers to a person belonging to an assessor who is in charge of the assessment in this program or a general partner in charge of implementing the assessment in this program, i.e., a person who is responsible for the engagement in question, its implementation, and the assessment report to be issued.

1.3.5 Chief Implementing Partner
Refers to a person on the engagement team who is responsible for the implementation of individual assessment.

1.3.6 Assessment Professional
A person on the engagement team who carries out an assessment in this program, and may be utilized including the Engagement Partner, the Chief Implementing Partner, or any other member of the engagement team.

1.3.7 Engagement Team
A unit that is organized by the Engagement Partner under his or her own responsibility for the execution of engagement, which, in principle, consists of persons belonging to an assessor, including the Engagement Partner and the Chief Implementing Partner.

1.3.8 User of Results
Refers to the person who uses the assessment report prepared by the assessment professional, i.e. the client, the Ministries responsible for the System, the ISMAP Steering Committee, and the ISMAP Operations Support Organization.

1.3.9 Working Papers

A record of the procedures implemented by the assessment professional, evidence obtained, and matters identified in the course of operations.

1.3.10 Assessment Report
A report issued by an assessment professional as a result of implementing procedures in accordance with the information security assessment criteria on the status of design and operation of internal controls related to information security implemented by cloud service provider based on the Control Criteria of ISMAP.

1.3.11 ISMAP Standard Assessment Procedures
Refers to the standard procedures to be followed by the assessment professional in implementing the procedures of the assessment in this program. The ISMAP Standard Assessment Procedures

are structured to correspond to the detailed control measures.

1.4 Responsibility of the Client, Assessment Professional and the ISMAP Steering Committee for Assessment in this Program

1.4.1 Responsibility of the Client

With regard to the cloud services subject to declaration, i.e., the cloud services for which the client is applying for registration to the ISMAP Cloud Services List, the client is responsible for selecting the control objectives and detailed control measures in accordance with the Control Criteria of ISMAP, establishing the necessary controls, and declaring that they have been effectively operated those over the subjected period, based on the content of such services and the results of the security risk analysis.

1.4.2 Responsibility of the Assessment Professional

The assessment professional is responsible for implementing the assessment in this Program in accordance with information security assessment criteria and reporting the results to the client.
The assessment professional is responsible for implementing procedures for the controls which the client declares in accordance with ISMAP Standard Assessment Procedures, but is not responsible for reporting on the effectiveness of the relevant control objectives or the conclusions drawn from the results of the implementation of the procedures as a result.

1.4.3 Responsibility of the ISMAP Steering Committee

The ISMAP Steering Committee is responsible for receiving the application documents required for service registration, including the assessment report, from the client and for examining the registration of cloud services to the ISMAP Cloud Services List in accordance with the ISMAP Cloud Services Registration Rules.

Chapter 2 Independence, objectivity and professional ethics

2.1 The assessment professional shall comply with the independence, objectivity, and professional ethics requirements set forth in the Information Security Audit Criteria.

2.2 In addition to the preceding paragraph, the assessor[1] shall comply with the following matters regarding independence in appearance.

2.2.1 There shall be no equity relationship with the cloud service provider subject to the assessment in this program.

2.2.2 There shall be no conflict of interest with the cloud service provider subject to the assessment in this program[2].

[1] As set out in 1.3.3, an assessor is a legal entity registered on the ISMAP List of Assessors and does not include a group or network firm of such an entity.

[2] As the instances where there exists the conflict of interest, such a case, for example, is assumed that the assessor provides works, with regard to the cloud service subject to the assessment in this program, for development, maintenance, operation, design and introduction of the relevant cloud service.

Chapter 3 Quality Control

3.1 Quality Control

The assessor is responsible for ensuring the overall quality of the assessment in this program, which is implemented in accordance with the following quality control requirements.

3.1.1 Quality Control by the Quality Manager

In order to maintain and improve quality, a person responsible for quality control of assessment in this program in the organization shall be assigned, and the quality manager shall systematically control the quality of the assessment. However, this does not necessarily mean that the person in charge should be exclusively responsible for managing quality of engagement.

3.1.2 Ensuring quality based on the quality control manual

In order to maintain and improve quality, a manual for quality control, including the following items, shall be prepared and quality control shall be carried out based on the manual.

(1) Management of service providing process
(2) Management of output

3.1.3 Introduction of Procedures and Other Measures to Maintain and Improve Quality

In order to maintain and improve quality, the following procedures shall be carried out.

1. A person other than the person who was engaged in carrying out assessment in this program shall review the assessment plan and assessment report.

2. Persons engaged in assessment in this program shall be provided with any of the following education or training that contributes to ensuring the quality of assessment in this program.

   (1) Engagement Partner and the Chief Implementing Partner

   A minimum of 20 hours of education or training per year (including training to maintain qualifications as well as on-the-job training, in-house training and self-study, in addition to education and training provided by the education service provider).

   (2) Assessment Professional

   A minimum of 5 hours of education or training per year (including training to maintain qualifications as well as on-the-job training, in-house training and self-study, in addition to education and training provided by the education service provider).

3. Procedures to protect the information of the client shall be established and implemented, and the effectiveness of these procedures shall be ensured by having an audit (internal or external) conducted by a person other than the one who was in charge of carrying out assessment in this program.

Chapter 4 Planning, Implementing and Reporting Assessment in This Program

4.1 Conclusion and Renewal of Engagement Letter

4.1.1 In order to avoid misunderstandings about assessment in this program, the assessment professional shall ensure that the client clearly understands the following points before entering

into an engagement letter with the client. The following items shall be included in the terms and conditions of the engagement letter.

1. Qualities of the assessment in this program

(1) The assessment in this program does not constitute assurance engagement[3], such as assurance-type audits or reviews, and therefore does not report on the conclusions drawn from the results of the implementation of the procedures, nor does it provide assurance.

(2) Responsibility of the client

> The client is responsible for determining the scope of the services to be declared and the duration of the procedure in the assessment in this program.

> Matters set forth in 4.6.2 are listed in the written representation and the client is responsible to comply with these.

> The client is responsible for selecting control targets and detailed control measures in accordance with the Control Criteria of ISMAP and developing necessary controls based on the content of the services to be declared and the results of the security risk analysis, as well as declaring that the control targets and detailed control measures have been effectively used over the period covered.

> The client is responsible for establishing a system for self-evaluation of the accuracy of the declaration and for conducting the evaluation.

> The client is responsible for interpreting the requirements of the Control Criteria of ISMAP.

> The client is aware that the assessment in this program complies with information security assessment criteria.

> There are restrictions on the distribution and use of assessment reports.

> The client has provided all information, interviews and opportunities for questions requested by the assessment professional.

> Whether any event has occurred during the period from the end of the period of the assessment subjected under the Program to the date of the written representation, if any, that may have materially changed the control and information security status of the cloud services subject to declaration (The client is responsible for the contents if this event occurs).

> Whether or not there is information about improper or illegal activities that may affect implementing the engagement (The client is responsible for the contents when this information exists).

(3) Responsibility of the assessment professional

> The assessment professional is responsible for conducting the assessment in this program in accordance with the objectives of the client's request to conduct the assessment in this program, and for reporting the results in accordance with the information security assessment criteria. However, the assessment professional shall not be responsible for

[3] Assurance engagement refers to work in which the person responsible for the subject matter reports information that expresses the results of an evaluation or measurement of the subject matter by means of certain criteria, or in which the assessment professional reports the conclusion of the results of a judgment made about the subject matter itself, based on evidence obtained by him or her in light of the criteria, in order to increase the degree of confidence of the intended users in the subject matter. (Opinion on the Conceptual Framework for Financial Information Assurance Engagement, Business Accounting Council, November 29, 2004)

determining the scope, duration and subject matter of these procedures.

> The assessment professional's report is only a factual report of the results of the implementation of the procedures, and does not report the conclusions drawn from the results of the implementation of the procedures, nor does it provide any assurance. The assessment professional does not apply the concept of materiality or determine procedures based on risk assessment in the assessment in this program, does not evaluate the risk of users of the assessment report drawing inappropriate conclusions based on the assessment professional 's report, and does not evaluate the sufficiency of the procedures implemented or the evidence obtained.

(4) Responsibility of the ISMAP Steering Committee

> The ISMAP Steering Committee is to confirm the application documents including the assessment report reported by the assessment professional, and to examine the registration of the cloud service to the ISMAP Cloud Services List in accordance with the ISMAP Cloud Service Registration Rules.

2. Purpose of the client's request for assessment in this program
3. Cloud services subjected to the assessment in this program
4. Assessment in this program shall be conducted in accordance with information security assessment criteria.
5. The scope, period, and scope of procedures to be implemented, etc.
6. The expected format and content of the assessment report
7. Restrictions on distribution and use of assessment reports
8. Other matters deemed necessary

4.1.2 The assessment professional shall not enter into a new or renewal of the engagement letter for assessment in this program agreement if any of the following circumstances occurs.

> When the client is not aware of his or her responsibility for the status of design and operation of internal control over information security in accordance with the purpose of this program and the Control Criteria of ISMAP.

> When it is clear that the terms and conditions of the contract set out in 4.1.1 cannot be complied with.

> When it is not possible to restrict the use of the assessment report to the persons specified in 1.3.8 due to laws and regulations or other circumstances.

> When, as a result of an inquiry to the ISMAP Operations Support Organization, it is found to be difficult to carry out the examination within the time frame set out in the ISMAP Cloud Services Registration Rules, Section 6 Examination.

4.2 Organization of the Engagement Team

4.2.1 The Engagement Partner shall organize the engagement team to meet the requirements for engagement teams set forth in the Requirements for ISMAP assessor.

4.2.2 The Engagement Partner shall supervise the engagement team to ensure that they perform their work in accordance with information security assessment criteria.

4.3 Planning

4.3.1 The assessment professional shall develop a plan for effective and efficient implementation of the assessment in this program.

4.4 Implementing Procedures

4.4.1 With respect to the status of design and operation of internal controls over information security at the cloud service provider, the assessment professional shall implement procedures in accordance with the following items.

1 Procedures to be implemented
In addition to these guidelines, procedures shall be carried out in accordance with the Information Security Audit Criteria and ISMAP Standard Assessment Procedures.

2 The scope of the declaration subject to the procedures

> The procedures involve a design assessment and operational assessment of the client's controls that correspond to all of the detailed control measures described in Section (4) Covered Controls and Corporate Control Details of 1. Scope and Duration of the Declaration in the declaration.

> When the client excludes control targets or detailed control measures, the assessment professional shall confirm that the reason for the exclusion of control targets is described in the declaration and its annex, and the reason for the exclusion of detailed control measures is described in the annex. However, the assessment professional does not evaluate the validity of any of the reasons for exclusion.

3 Assessment period in this program
A period of time, not less than three months and not more than one year, to be specified by the client.

4.5 Use of Evidence from Other Certification and Audit Systems

The assessment professional implements their own procedures in accordance with ISMAP Standard Assessment Procedures. Therefore, in principle, the results of other certification/audit systems and internal audits, etc., or their reports may not be used as they are. However, if the assessment professional considers it appropriate to use them when implementing ISMAP Standard Assessment Procedures, the evidence collected from other certification/audit systems and internal audits may be used.

4.6 Written Representation

4.6.1 Prior to issuing an assessment report, the assessment professional shall obtain from the client a written representation of the materials and other explanations provided by the client during the implementation period.

4.6.2 The assessment professional shall ensure that the following items are included in the written representation.

> The fact that the client is responsible for selecting control objectives and detailed control measures in accordance with the Control Criteria of ISMAP, establishing the necessary controls, and declaring that they are being effectively used over the period of the cloud service subject to declaration, based on the content of the service and the results of the security risk analysis.

> The fact that the client shall be responsible for establishing a system for evaluating the accuracy of the declarations and implementing the evaluation.

> The fact that the client is responsible for interpreting the requirements of the Control Criteria of ISMAP.

> The fact that the client is aware that the assessment in this program is in accordance with information security assessment criteria.

> The fact that there are restrictions on the distribution and use of assessment reports.

> The fact that the client has provided all information, interviews and opportunities for questions requested by the assessment professional.

> Whether any event has occurred since the end of the assessment period in this program to the date of the written representation that could cause a material change in the control and information security status of the cloud service subject to declaration(If any event occurs, detailed information shall be provided).

> The existence of information on fraudulent or illegal activities that may affect the conduct of engagement (If this information exists, detailed information shall be provided).

4.7 Reporting

4.7.1 The assessment professional shall prepare an assessment report in accordance with Form 1 set forth in Appendix 1. The assessment report shall include all of the following.

> Title

> Destination

> Date

> Assessor name

> Name, signature and seal of the Engagement Partner

> The purpose of the client's request for the procedures

> Cloud services subject to assessment in this program

> A statement that the assessment in this program implemented by the assessment professional complies with information security assessment criteria.

> Responsibilities of the client, assessment professional, and the ISMAP Steering Committee. The statement regarding the responsibilities of the ISMAP Steering Committee shall not be changed from the wording of the form.

> Outline of the engagement performed (subjected scope, period and subject of procedures, etc.)

> The procedures and results of the implementation of the procedures carried out by the assessment professional

> The fact that item numbers of the control objectives or detailed control measures and the reason for the exclusion are stated in the declaration, when the client has excluded any control objectives or detailed control measures. The fact that the assessment professional is not responsible for assessing the validity of the reason for the exclusion.

> If any of the ISMAP Standard Assessment Procedures could not be implemented, the procedures and the reasons for not being able to be implemented.

> The findings[4]. The fact that the assessment professional shall be responsible for reporting the findings in accordance with the facts, but shall not evaluate the findings to determine the sufficiency and relevance of the evidence obtained. It also states that the assessment professional will not make a determination based on its interpretation of any requirement of the Control Criteria of ISMAP or make a determination of materiality as to whether a particular fact constitutes as findings.

> The fact that assessment in this program does not constitute assurance engagement such as assurance-type audits or reviews, and therefore does not report on the conclusions drawn from the implementation of the procedures or provide assurance.

> The fact that distribution and use of the assessment report is restricted to clients, Ministries responsible for the System, ISMAP Steering Committee and ISMAP Operations Support Organizations only and it shall not be used for any other purpose except to the extent necessary for examination and monitoring as defined in the ISMAP registration rules for assessors, in addition to service registration examination.

4.7.2 The assessment report shall be prepared in Japanese.

4.7.3 The date of the assessment report shall not be dated prior to the date on which the engagement is completed by the assessment professional.

4.7.4 The date of the assessment report shall be, in principle, within a maximum of three months from the end of the assessment period in this program as stated in the declaration.

4.7.5 The assessment report shall describe in detail the scope, duration and subject matter of the procedures carried out in accordance with ISMAP Standard Assessment Procedures, so that users of the results can understand the procedures which were implemented.

4.7.6 The assessment professional shall state the results of implementing the procedure in a factual and objective manner, and shall not use ambiguous language or express opinions.

4.7.7 The Engagement Partner shall attach to the assessment report documentation demonstrating that the engagement team that performed the engagement in accordance with Attachment 2 of Form 1 meets the Requirements for ISMAP assessor.

4.8 Working Papers

4.8.1 The assessment professional shall document the results of the procedures performed and related materials in the working papers.

4.8.2 In preparing the working papers, they shall be kept in an orderly manner so that the process leading to the results of implementation can be understood.

4.8.3The working papers should include, for example, the following

> Compliance with the provisions on independence, objectivity and professional ethics set forth in the Information Security Audit Criteria

> A decision on the conclusion or renewal of a new engagement letter with the client

> Scope and duration subject to engagement implemented and scope of procedures, etc.

> The results of the procedures implemented and the evidence obtained

---

[4] Findings refer to the following results of procedures implemented by the assessment professional.
・As a result of implementing procedures for design assessment, there are no rules and regulations related to internal control.
・As a result of implementing procedures for design assessment, there is no evidence related to internal controls.
・As a result of implementing procedures for operational assessment, deviations in internal control were found in the selected sample.

> Other matters identified in the course of engagement

> The person who implemented the procedures, the date of its completion as well as the person who reviewed it, the date of the review and the scope of the review

4.8.4 The working papers shall be retained appropriately after the completion of the assessment in this program until the end of its retention period.

Form 1: Assessment report