BSA Comments on the Draft of Various Standards for Information System Security Management and Assessment Program (ISMAP)

April 24, 2020

BSA | The Software Alliance (**BSA**)[1] appreciates the opportunity to submit the following opinions to the National Center for Incident Readiness and Strategy for Cybersecurity **(NISC)**, National Strategy Office of IT, Ministry of Economy, Trade and Industry (**METI**), and Ministry of Internal Affairs and Communications (**MIC**) regarding the Draft of Various Standards for Information System Security Management and Assessment Program (**ISMAP**).

General Comments

BSA's members are at the forefront of innovative technologies, products, and services, including cloud computing and related services that drive the global information economy and improve our daily lives. Cloud computing is and will continue to be one of the most important technologies, particularly in this time of global crisis, supporting governments around the world to maintain vital, trusted functions to meet critical needs and to enable remote working. Relevant regulations and policies, therefore, should support the growth of secure cloud services. BSA also recognizes the importance of prioritizing cybersecurity in government procurement processes including those for cloud services.

In this regard, we are appreciative of the ongoing effort by the Government of Japan to facilitate government-wide adoption of secure cloud services and for providing relevant stakeholders the opportunity to discuss the development of ISMAP. BSA provided comments on the draft Interim Summary[2] and subsequent draft Report[3] from the Committee on Security Assessment of Cloud Service in April and December 2019. We were grateful to see many of our earlier comments taken into consideration in the draft of various standards of ISMAP.

Cybersecurity policy solutions are most effective when they are risk based, adaptable, and outcome oriented. Although ISMAP is still in development, we see it meeting much of that requirement. We would like to offer the below comments to further contribute to your efforts.

[1] BSA's members include: Adobe, Amazon Web Services, Atlassian, Autodesk, AVEVA, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

[2] https://www.bsa.org/files/policy-filings/04162019bsasecurityassessmentcloudservice.pdf

[3] https://www.bsa.org/files/policy-filings/en12252019bsaseccloudservice.pdf

Specific Comments Regarding the Guideline

[ISMAP Management Standards (Security Controls)]
Chapter 2/ 2.2 Content to be written in statements / 2.2.5. Period Subject to Audit

[ISMAP Information Security Audit Guidelines]
Chapter 4 / 4.5 Use of the evidence of other certification/audit system

Section 2.2.5 of Security Controls states that audits will be required every year for all security measures of cloud service registered in the Cloud Service List. While we are encouraged that the ISMAP Information Security Guidelines acknowledge that evidence collected for existing certification/audit system and internal auditing can be reused to conduct standard audit procedures, the associated upfront investment could still become a barrier for innovative cloud service providers (**CSPs**). Audit processes are not only expensive, but also pull security personnel away from their responsibilities to instead fulfill audit requirements; for that reason, many leading global certification processes require audits once every two or three years without compromising security. We therefore recommend the government to continue exploring ways to minimize unnecessary burdens on CSPs by simplifying the process.

We recommend that ISMAP impose a less frequent auditing schedule. Depending on the complexity of the cloud service, ISO 27000-like audit processes can be lengthy activities and are usually current for three years, although that may be shortened for major system changes. Yearly audits could mean CSPs having to conduct back-to-back audit processes holding them in a constant state of audit. We are also concerned that yearly audits would place an increased burden on the procurement agency to renew the associated contracts yearly. In addition, the registration system for general open tenders at public offices sets three years as the valid period. We recommend changing the period of audit to once every three years, reducing the audit overhead for all stakeholders and bringing the requirement in line with the general open tender requirement.

We also recommend tailoring the requirements for security controls depending on the different cloud computing models, which range from Infrastructure-as-a-Service (**IaaS**), Platform-as-a-Service (**PaaS**), and Software-as-a-Service (**SaaS**). These models differ from one another in various ways, including in the relationship between the CSP and the cloud service customer (**CSC**) and the nature of allocating shared responsibility.

BSA is concerned that, as written, ISMAP will overload limited cloud auditing resources in Japan. IT audits and certifications for cloud services require highly specialized skills with a limited pool of skilled staff able to effectively perform them globally. This has proven to be an issue with similar schemes around the world, particularly in the first few years of operation, where many cloud services are being certified for the first time under the new requirements. The limited global pool of auditors has also meant a high price for capable staff. While this argues for establishing reasonable expectations and costs on CSPs and the government agencies implementing the ISMAP, it also underscores the global need to build a highly skilled workforce to defend the most critical systems.

We recommend the ISMAP appropriately take into account these factors to better identify and narrow essential security controls to make better use of limited resources for the CSPs, the auditors, and the government agencies involved.

In order to implement an expeditious process for auditors and CSPs, it will also be helpful to have additional guidance and Q&A developed for ISMAP Management Standards (Security Controls) in the coming months. This will assist CSPs to accurately interpret the listed security control requirements before the implementation phase begins and better streamline the initial certification activities. We also recommend that the government develop a process for training and skilling an IT audit and certification workforce for cloud services in Japan, in parallel to the ISMAP development process.

[ISMAP Cloud Service Registration Rules]
Chapter 8 Service Registration Validity Period

Similar to concerns expressed above, Section 8.1 states that registrants must apply for renewal within one year and four months from the day following the end of the last registration audit. As noted above, we recommend ISMAP service registration be set to three years.

Chapter 4 Application for Service Registration / 4.2, Chapter 5 Acceptance of Applications / 5.4 (1), Chapter 6 Assessment / 6.1 (4)

These sections set a time period in which applicants must submit the application, respond to any queries, and make improvement on minor findings found during the assessment phase. The period is currently set to one or two months. This period does not provide sufficient preparation time for applicants to fully complete these actions. As such, we recommend the period be changed to three months.

[ISMAP Management Standards (Security Controls)]
Chapter 4 Management criteria

Section 4.2 correctly states that it is very important to exchange information between the CSC and the CSP on information security risks. BSA agrees with the Government of Japan that exchanging information with CSPs on information risks is essential to good cybersecurity outcomes. We note ISO 27005:2018 as an applicable international standard.

BSA recommends that the government of Japan develop a formal mechanism to exchange all information and intelligence with CSPs on information security risks to government networks collected by the private and public sectors. This will be essential for a CSP to appropriately assess and apply security controls to best protect government data and services.

Chapter 6 Organization for Information Security
6.3.P Relationship between the cloud service user organization and the cloud service provider

While ISMAP takes a uniform approach to ensuring an adequate security level for cloud service procurement by the government, it is also important that ISMAP stakeholders recognize that the services of government agencies vary widely and security controls for services are generally covered in individual cloud computing service level agreements (**Cloud SLAs**). Our understanding is that ISMAP covers the core, fundamental security controls and other extended security controls will be agreed between the procuring agency and the CSP under the Cloud SLA, including the elaboration of the shared responsibility between the parties. We recommend again that this point be clarified among stakeholders involved in ISMAP.

[ISMAP Cloud Service Registration Rules]
Chapter 9 Report on Information Security Incidents

Under section 9.1, CSPs are required to report security incidents related to its registered cloud service. Implementation of this would be greatly assisted by defining what security incidents need to be reported to the ISMAP Steering Committee. BSA recognizes the importance of this control as an essential communication device in the event of a major security incident that puts government services or data at risk. There is a risk that if the threshold for reporting is set too low, the committee will be overwhelmed by insignificant security events that had been resolved without impact to the government. We recommend that only security incidents that are unresolved or critical, have resulted in data loss or have resulted in a measurable impact be reported to the committee. Furthermore, we recommend that incidents relating to personal information to be aligned with the data breach reporting requirements set under Act on the Protection of Personal Information.

Finally, as the form for this reporting is not attached to the proposed draft, we recommend providing clarification in the Registration Rules on the information that will be required for this reporting.

Chapter 15 Raising Registration Objections

Chapter 15 of the ISMAP Cloud Service Registration Rules states that the applicant or registrant may appeal to the ISMAP Steering Committee using a designated form if there are objections to the actions taken against service registration. Such adverse actions subject to appeal may include denial of registration of a certain cloud service by the ISMAP Steering Committee. As the designated forms are not included in the current draft Rules, it is not clear what information should be provided. We recommend including a clear description of the information required to appeal decisions in this section of the Registration Rules.

Table 1 How to Submit Application Form, Form 1-14

Table 1 states that applicants should submit their application by post. In accordance with the government of Japan’s ‘digital first’ principle, we recommend that applications be submitted online.

Also, as the form 1-14 is not attached to the proposed draft, in order to fully evaluate the items and information required for registration it will be helpful to have the actual forms disclosed to ISMAP stakeholders.

[Basic Regulations for Information System Security Management and Assessment Program (ISMAP)]
Chapter 9 Others

Section 9.1 states that ISMAP Steering Committee members will prevent access to confidential information by unauthorized people. It is not clear, however, how this is proposed to be done and whether this confidentiality will be guaranteed through a separate and specific non-disclosure agreement (NDA). If an NDA will be included in the process of ISMAP, it would be helpful to have it presented to ISMAP stakeholders for comment.

Chapter 1 Definition of terms / 1.4.5 ISMAP Steering Committee

We would also appreciate having clarity on the members that will consist ISMAP Steering Committee and how the future discussions will be shared amongst ISMAP stakeholders, including disclosure of the minutes to provide transparency in the process.

Conclusion

BSA hopes the above comments will be useful as you finalize the various standards of ISMAP. We will be happy to continue supporting the government of Japan in your efforts to promote the greater adoption of secure and effective cloud computing solutions for the public sector. Please let us know if you have any questions or would like to discuss these comments in more detail.