Recommendations from BSA | The Software Alliance on the Review of Information system Security Management and Assessment Program (ISMAP)

December 7, 2021

BSA | The Software Alliance (**BSA**)[1] welcomes the ongoing efforts of the National center for Incident readiness and Strategy for Cybersecurity (NISC), the Ministry of Economy, Trade and Industry (METI), the Ministry of Internal Affairs and Communications (MIC), and the Digital Agency (**relevant agencies**) to improve the "Information system Security Management and Assessment Program" (**ISMAP**), designed to assess the security of cloud services that may be used by the public sector with the goal of promoting cloud service adoption across government agencies.

General Comments

BSA is the leading advocate for the global software industry before governments and in the international marketplace. Our members lead the world in offering cutting-edge cloud computing technologies and services that can help governments be more nimble, productive, and innovative while also improving network security and system availability. Based on the experiences gained, we provide the below recommendations to support the government's goal of realizing smooth adoption of cloud services.

Observations and Recommendations

We strongly recommend the relevant agencies take the below points into consideration when reviewing and refining the ISMAP. The current ISMAP imposes significant compliance burdens and costs on cloud service providers (**CSPs**) wishing to register with the ISMAP Cloud Service List, likely straining the limited government resources needed to implement the system.

- **Recognize the shared responsibility model of cloud services.**[2] For the successful deployment of secure cloud computing systems, it is critical that cloud users and procurers understand that they have responsibility to minimize security risks by effectively training employees, developing secure applications in the cloud environment by using tools and implementing measures supplied by CSPs as necessary. Clearly incorporating the principle of shared responsibility in the ISMAP will ensure that CSPs and their customers recognize their different responsibilities for cloud operations when establishing and maintaining security controls. It will also help clarify which entity is

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

[2] https://cloudsecurityalliance.org/blog/2020/08/26/shared-responsibility-model-explained/

responsible for the aspects of the environment over which they have control and are responsible, and not for those over which they have no visibility. This clarity will avoid imposing security requirements or obligations on CSPs over customer data and systems to which they do not have access, and which can consequently have counter-productive outcomes for security and privacy if they are subject to inappropriate obligations.

- **Make the ISMAP more flexible and implementable**. The ISMAP may be improved by better taking into account the distinctive requirements of different types of cloud services (SaaS, IaaS, PaaS) and defining essential security controls tailored to manage the risks most relevant to these respective services as well as the environments and organizations in which they are deployed.

- **Reduce repetitive auditing process.** Exempting the application of security controls that are duplicative with internationally recognized standards for which certifications have already been received would streamline auditing processes, freeing up resources to focus on a more limited set of specific controls. Many CSPs already are certified for internationally recognized standards (e.g., the ISMS-JISQ/ISO 27000 series) by internationally accredited certification bodies. Recognizing such certifications and eliminating repetitive procedures and requirements to reuse evidence already provided during prior certifications will contribute to alleviating the burden of all stakeholders involved, including the Government of Japan. This will also facilitate more companies in Japan obtaining ISMS/ISO certification, opening up greater international business opportunities for such companies and increasing competition to provide better and more cost effective solutions to the government of Japan.

- **Recognize third party, internationally accredited certifications and audit results**. Eliminating the need to duplicate evidence of compliance with relevant ISMAP controls and requirements would also reduce the need for on-site audits which are often impractical, repetitive, and expose the data centers to unnecessary physical security risks by requiring access to the site by otherwise unauthorized personnel.

- **Establish more specific audit guidelines and map them to internationally recognized standards**. Discrepancies in the interpretation of security controls amongst ISMAP administrators, auditors, and CSPs imposes inefficiencies, additional costs, and delays. In some cases, CSPs that have undergone audits have experienced repeated requests from ISMAP administrator to re-audit because of difference in the interpretation of security controls by ISMAP administrators and auditors.

- **Increase the number of auditing firms registered under ISMAP.** The limited number of accepted auditing firms has resulted in a lack of resources to fulfill current and future demands for audit procedures required under ISMAP. Increasing the number of registered auditing firms from the four currently registered will alleviate bottlenecks and promote fair competition among auditing firms, providing CSPs with a wider variety of choice and potentially driving efficiencies in the auditing market. In parallel, developing and appropriately resourcing a process for training an IT audit and certification workforce for cloud services will be important to make ISMAP sustainable.

- **Establish a less frequent auditing schedule**. In contrast to the ISMAPs requirement to conduct audits on an annual basis, international cloud security best practices generally require audits once every three years. A less frequent audit schedule will reduce unnecessary costs to CSPs and the Government of Japan alike. Yearly audits could result in CSPs conducting effectively back-to-back audit processes, holding them in a constant state of audit, unnecessarily distracting security staff and diverting other important resources, and placing an increased burden on procuring agencies that will be required to renew the associated contracts yearly.

- **Accept applications for ISMAP certification and registration throughout the year**. Currently, the ISMAP administrators accept applications from companies seeking ISMAP certification and registration on a quarterly basis, which may cause three-month delays or more for CSPs seeking ISMAP certification. Such delays can preclude companies from bidding for valuable procurement opportunities, denying both the company the business opportunity and the procuring agencies from benefiting from the benefits of the cloud services in question. Continuous application and registration throughout the year will enable ISMAP to incorporate more quickly rapidly evolving cloud technology.

These recommendations are consistent with Japan's Cybersecurity Strategy,[3] which states that "the government will implement initiatives to visualize the safety of cloud services using ISMAP and other means. These efforts will target a wide range of stakeholders in both public and private sectors and promote increased use of cloud services that ensure a certain level of security. As many cloud services are provided by foreign companies, Japan will work to advance global collaboration as well."[4] Prioritizing the above improvements to the ISMAP and allowing for greater recognition of international security certifications will lead to greater proliferation of security-assured cloud services in Japan.

Conclusion

BSA looks forward to the opportunity to discuss how BSA and our members that have global operations can work closely together with relevant agencies to implement the above recommendations and expand options for government procurement and generate value for government investment in services provided by the private sector.

[3] Cybersecurity Strategy, The Government of Japan, September 28, 2021 at https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2021-en.pdf.

[4] Ibid, pp. 24-25