Business Software Alliance

October 17, 2025

BSA COMMENTS ON THE AMENDMENT OF ISMAP CONTROL CRITERIA

The Business Software Alliance (**BSA**)[1] appreciates the opportunity to submit comments to the National Cybersecurity Office (**NCO**), Digital Agency, Ministry of Internal Affairs and Communications (**MIC**), and Ministry of Economy, Trade and Industry (**METI**) regarding the draft amendment of Control Criteria of Information Security Management and Assessment Program (**ISMAP**) (**draft Proposal**).

BSA is the global trade association of the enterprise software industry. Our members are at the forefront of developing innovative technologies, including cloud computing services that support governments worldwide in delivering secure, reliable and citizen-centric digital services.

We commend the Government of Japan for its continued efforts to promote the adoption of secure cloud services across government agencies and for engaging stakeholders in the reform of ISMAP. As the Government works to improve the program, we hope the following recommendations will help address challenges and facilitate broader cloud adoption in the public sector.

Promote Clear Understanding of the Amended Detailed Controls

We welcome the proposed reduction in the number of detailed controls from 1,163 items to 322 items. This streamlining is a positive step toward improving clarity and operational efficiency. However, the shift to high-level descriptions and the general requirement for cloud service providers (CSPs) to implement — as a general rule — all detailed controls introduce ambiguity. The draft proposal states that detailed controls can be excluded "if determination is made that reasonable application of such controls is impossible or unnecessary based on risk analysis." The proposal further states that Guidelines will be developed in the future, which provides reasoning and examples for excluding control objectives and detailed controls, and outlines the approaches and examples for selecting from the Handbook[2] CSP's own security measures to implement detailed controls.

---

[1] BSA's members include: Adobe, Alteryx, Amazon Web Services, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Cohesity, Dassault Systemes, Databricks, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Workday, Zendesk, and Zoom Communications Inc.

[2] The Handbook（手引き）presents reference information on how detailed controls can be implemented, presented in reference document 1-2, here: https://public-comment.e-gov.go.jp/pcm/download?seqNo=0000299113

Given the limited precedent for risk-based assessments in ISMAP, it is essential to establish clear operational standards in both the Guidelines and the actual examination process. For instance, it remains unclear whether previously listed control items—now omitted or consolidated—will continue to be considered during assessments. The current proposal shifts previous items into the Handbook, which seems to indicate that the detailed control items still need to be satisfied as audit criteria which, if so, would result in requiring the same audit workload.[3] We understand that the purpose of the amendment this time is to reduce the burden on businesses. We urge the Government to further amend the draft Proposal to specify that the items listed in the Handbook are for reference and not mandatory obligations requiring auditing, in line with the intent of this amendment. Further, we request clear handling guidelines for submitting evidence samples for audits stated in ISMAP Standard Audit Procedures[4]. Clarifying these points will help ensure consistent implementation and avoid confusion.

We recommend that government agencies, examining bodies, CSPs, and audit firms (assessors) engage in intensive discussions with relevant stakeholders including BSA member companies, prior to implementation. These discussions should aim to:

- Establish mechanisms for sharing insights to support appropriate risk assessments.
- Strengthen the capabilities of examining bodies.
- Help CSPs build internal structures aligned with operational standards.
- Create mechanisms for continuous improvement.

It is also important to clarify in the Guidelines that the examples provided are illustrative—not prescriptive—and that CSPs and their customers may flexibly select appropriate security controls tailored to their specific objectives.

---

[3] The draft Appendix 3 presents the proposed detailed controls which have been reduced:
https://public-comment.e-gov.go.jp/pcm/download?seqNo=0000299112

and the draft Reference 2 document (参考２) presents the detailed controls that are currently described as four-digit number ((X.X.X.X) in the Control Criteria which has been shifted to the Handbook:
https://public-comment.e-gov.go.jp/pcm/download?seqNo=0000299113

However, it is not clear how the items described in the Handbook will be considered. If the items described in the Handbook are required to be audited, the operational burden will not decrease, and in fact, if items other than ".B" in the current Control Criteria will be required, it will increase the items subject to audit.

[4] ISMAP Standard Audit Procedures (ISMAP 標準監査手続)
https://www.ismap.go.jp/csm?id=kb_article_view&sys_kb_id=ae5a275d2b8cb610f0bbfd69fe91bfaa

With the four digital number detailed controls shifting to the Handbook, it is not clear how the random sampling required to assess operation status will be considered. It will be helpful to understand whether the coverage of random sampling should be presented in accordance with the detailed controls in draft Appendix 3 or with items described in the Handbook presented in Reference 2 document.

Further, given that the evaluation framework for AI services under ISMAP has not been determined, we encourage ensuring the statement requirements for AI services and sub-services to be developed in the future are based on the reality of how AI is used.

While the timeline for releasing the Guidelines and related ISMAP documents is still under discussion, we request that a general timeline be presented, including the expected start date for applying the amended Control Criteria. To allow time for stakeholder engagement and internal preparation, we recommend providing a sufficient grace period from the release of the finalized Handbook and Guidelines to the start of application.

Avoid Mandating a Framework for Prior Confirmation

The draft proposes a framework for prior confirmation of the appropriateness of controls intended to be implemented. While this framework could be helpful if used voluntarily, making it mandatory would risk imposing excessive burdens on both examining bodies and CSPs, increasing costs and prolonging the examination process. We therefore request that the framework be explicitly stated as voluntary.

Actively Utilize Internationally Recognized Standards

The "Regulatory Reform Implementation Plan" (**Plan**)[5] released from the Cabinet Office in June 2025 clearly states that "if other certification systems are obtained, utilize the relevant certification systems to reduce audit items, etc. to alleviate the audit burden." We applaud the Cabinet Office's recognition of the utility of existing certifications, which help ensure services meet their user's risk management needs while increasing competition and helping government agencies keep pace with private sector innovation. During the recent briefing, it was noted that this point may be reflected in the auditing framework. To ensure the implementation of the Plan, we urge the Government to conduct thorough discussions with relevant stakeholders on ways to reuse the evidence obtained by CSPs such as ISO 27000 series and SOC 2 certifications. Recognizing these certifications and eliminating duplicative procedures would reduce burdens on both the Government and CSPs.

To enhance cloud security globally, BSA recommends like-minded countries pursue mutual recognition of applicable portions of each other's certifications — for example, between Japan's ISMAP and US FedRAMP. Such an approach would improve cybersecurity and resilience broadly, foster deeper international collaboration, and provide government agencies with access to the best and most secure services.

Conclusion

We thank the Government for considering our recommendations and welcome the opportunity to contribute to future discussions on ISMAP reform. Please feel free to contact us should you have any questions or wish to discuss our feedback in more detail.

---

[5] https://www8.cao.go.jp/kisei-kaikaku/kisei/publication/program/250613/01_program.pdf