Recommendations from BSA | The Software Alliance on ISMAP Reform

1) Obstacles to ISMAP Registration	**[Cost of ISMAP Registration, Number of Controls]** The high cost of obtaining and maintaining ISMAP certification (fees paid to external auditors, internal fees, etc.) has become an obstacle for cloud service providers ("CSPs"). While CSP management understands the importance of registering with ISMAP, the cost of certification makes them hesitant to make ISMAP a priority. Due to the annual audit requirement and the number of security controls to be audited, the annual cost for some CSPs can run up to 100 million Japanese yen, including the cost to hire a staff to work exclusively on ISMAP. Compared to government certification programs in other countries, ISMAP is highly expensive, with Federal Risk and Authorization Management Program (FedRAMP) in the United States coming close in cost to obtain and maintain in some cases (this includes not only fee for external auditing but also monitoring, cost to obtain and maintain respective certification). In some cases, the cost of paying to an external auditor alone can run up to four times the cost of Australia's The Infosec Registered Assessors Program (IRAP), with IRAP's auditing cycle set for two years and external auditing cost running half of ISMAP. In terms of the number of controls, ISMAP uses a checklist-based approach that specifies about three times as many security controls as FedRAMP - this could be improved by transitioning into more of a risk-based program. CSP's internal analysis found that more than 50% of ISMAP audited controls are compatible with SOC2 and ISO27000 series certification programs meaning that CSPs are required to perform a large number of duplicate audits to meet ISMAP requirements, and the discrepancy with rigorously developed international international standards is a significant lost

	opportunity, increasing the cost of security compliance without improving security outcomes. In addition, both IaaS providers with high unit costs and SaaS providers with low unit costs are spending similar amounts of costs. SaaS providers with low unit costs tend to have lower sales, making it harder for them to turn into business under this program. For this reason, some CSPs have SaaS products that cannot be added to the ISMAP Cloud Services List, and the initial cost of the application process discourages many small and medium-sized SaaS providers from applying. Given that reduced implementation costs and rapid development is important for governments that use SaaS, it is necessary to review ISMAP. In order to lower the barriers to entry for ISMAP, we urge that the cost of certification (fees paid to external auditors, internal costs, etc.) be lowered through a review of the number of controls, etc., taking into consideration other countries' systems and situation (please refer to attached comparison table).
2) Points and Issues that are Particularly Burdensome or Problematic During the Process of ISMAP	**[Number and Structure of Security Controls]** As mentioned in 1), the current structure of ISMAP security control is complex and the method of seeking CSPs to map the controls to control sets has resulted in burdensome exercise for CSPs. ISMAP requires a detailed descriptions on how functions and information are provided to customers, and there is a mix of mandatory and non-mandatory controls, up to 4 digits controls In the case the controls set by CSPs already meets ISMAP control criteria, the work of tying them together is required, even though ISMAP is essentially based on ISO. These optional controls have resulted in significant additional burden for CSPs and is unusual, as under other certification systems, all security controls are mandatory. Making controls optional creates additional work to confirm which controls need to be stated, requiring reasons to be explained if not stated. Even when selected, hundreds of controls need to be stated, and the sheer

	number of controls makes the certification challenging, in comparison to other major national cloud certification schemes for government procurement. We propose substantially reducing the number of controls, to remove additional work by CSPs of selecting non-mandatory controls. **[Audit Cycle]** As noted above, the single-year audit cycle has resulted in significant annual certification costs for CSPs. As such, we recommend that the audit cycle be changed to a triennial renewal frequency, and that the deadline for submission of audit report be extended to 6 months after completion of the audit, in order to implement a system that enables CSPs the flexibility to manage the global audit cycle. The current system requires the submission of audit report to be made within four months from the end of the audit, which does not enable sufficient time for CSPs to collect all the required evidence. The current ISMAP and ISMAP-LIU stipulate fixed audit periods, to be selected upon the first registration. The audit cycle is then established going forward and flexibility is not afforded to adjust the audit cycle afterwards. This rigid audit cycle will not allow CSPs undergoing changes in their global audit cycles to adjust accordingly and may create a gap in the ISMAP assessment process which could result in temporary revocation of their services from the ISMAP and ISMAP-LIU Cloud Service List. To resolve this, we encourage the relevant agencies to adopt a system similar to the bridge letter of System and Organization Controls (SOC) that covers the void between the most recent audit report's end date and the starting date of the next audit report. The bridge letter states that no material changes in the controls have taken place during the gap period and allows for the certification to be maintained during such circumstances. **[Registration Cycle]**

	Currently, the ISMAP administrators accept ISMAP 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 the CSP the business opportunity and the procuring agencies the benefits of the cloud services in question. Continuous registration throughout the year will enable ISMAP to incorporate rapidly evolving cloud technology more quickly. **[Reuse of Evidence of Other Certifications]** The limited sampling methodology for operational status audits makes it difficult to reuse evidence of other certifications, as auditors are voluntary designating evidence (samples). As such, there are many cases in which it is not possible to reuse the evidence of other certifications due to designations differing from evidence submitted in other certifications. For this reason, the assumption at the time of audit planning (that the program allows for reuse of the evidence of other certifications) is broken, resulting in a significant number of man-hours spent on preparing evidence. We recommend that reuse of other certifications (especially sampling methods for audit of operational status) be made possible, and that audit firms recognize this. **[Lack of Resources on ISMAP Administrator]** One of the factors prolonging the process is the lack of experience in cloud auditing by the ISMAP administrators who are the point of contact for the initial application. As a result, there are cases where it takes up to six months from the time of application to approval. Renewals are also subject to the same inquiries as initial applications, creating a difficult situation for CSPs, putting them in a situation in which the renewal process does not proceed easily with the next audit period beginning. **[Documents to be Submitted]**

	ISMAP requires many of its submission forms to be written and submitted by CSPs. Accredited auditors that are more familiar with the application process should be able to fill these forms out for the applicants to simplify the process. For example, the information required on Form 1 is information that the audit firm will eventually include in the audit report and can be considered that CSPs do not need to provide information by themselves. If other information that will eventually be included in the audit report is also required by the CSP, we recommend that this be omitted from the CSPs' submission. **[Additional Requirements Not in the ISMAP process]** There are cases in which the applicant is requested to fulfill requirements that are not included in the written requirements for ISMAP, thus creating an audit process that is not part of the formal ISMAP process. In some cases, CSPs and auditors have been asked by the ISMAP Steering Committee not to proceed with the audit or even preparation work, such as pre-assessments, which has caused months of delays in CSPs ISMAP registration schedule.
3) Views on Constraints of External Audit Organizations and Bottleneck in Communication Between CSPs and Audit Organizations	**[Registered Auditing Firm]** The limited number of auditing firms registered for ISMAP prolongs the time it takes to obtain ISMAP. CSPs may have to wait six months or more due to the lack of resources at the audit firm, or due to audit firm not being able to undertake the audit due to the nature of the solutions provided by the CSP or the complexity of the involved task. The capacity of the five registered audit firms is insufficient to meet the demand for CSPs who wish to obtain ISMAP certification. In addition, in cases where the audit firm is a partner of the services provided by the CSP, the audit may not be undertaken due to a conflict of interest. Given the difficulty for CSPs to request ISMAP audits at the time and cost desired by CSPs, as described above, we urge expanding the resources of audit firms and to also consider broadening the scope of audit organizations to include more than just audit firms. Further, current ISMAP requires

	auditors to be Japanese nationals. Considering the global network of accounting and auditing firms and the English speaking ability of auditors, the burden of auditing overseas controls is high. We recommend that an organization that can facilitate overseas audits be added to the registered auditing organization.
4) Improvements That Should be Made in the Operations After Cloud Service Registration (change procedures, incident response, Operation of ISMAP Steering Committee, etc.)	**[Addition of New Service]** When a new service is added to an existing ISMAP-registered platform of the same CSP, there have been cases in which the use of the service had to be abandoned simply because the specific service is not registered (not listed in the ISMAP statement). We encourage to clearly state that new services on the same platform can be introduced at the discretion of the procuring ministry, so that even if a service is not listed in the statement, if it is on the registered platform, the risk will be low and that it can be introduced after a risk assessment by the procuring ministry. We recommend that this point be notified or clearly guided, as even for services that are scheduled to proceed to ISMAP registration in the future, there is a tendency for procuring ministries to perceive the lack of written statement as a risk and that the service cannot be used without ISMAP registration. **[Local Point of Contact].** Under the current ISMAP, it is necessary to designate local contact person in Japan. However, since many global operators do not have a contact person in Japan who is familiar with the security framework, we recommend allowing flexibility in designating a contact person, such as allowing a non-Japanese contact person located outside of Japan to be a point of contact and be able to have interactions in English. **[Contact Point to Provide Operational Feedback After Registration]** Although the IPA is the contact point for inquiries during the operation period, we recommend that a contact point be

	established to receive requests for improvement of the system, as there is no contact point for feedback on the program design.
5) Any Other Opinions or Requests Regarding the Direction of Improvement of the System or the System in General	**[Alignment of ISMAP with the Economic Security Promotion Act]** We request that the government clarify the position of ISMAP in relation to the Economic Security Promotion Act, which is currently under consideration by the government. If ISMAP is related to the requirements introduced by the Economic Security Promotion Act, we recommend that announcement on the direction of the ISMAP be made as soon as possible, as it will affect CSPs' products and marketing strategies. **[ISMAP-LIU]** With regards to ISMAP LIU launched this fall, we recommend the establishment a forum of registered CSPs to share information with the operators of ISMAP, facilitating communication between the system administrators (IPA), the ISMAP Steering Committee, and CSPs, leading to overall improvement of the system. Specifically, with ISMAP-LIU, it will be beneficial to have discussion on clarifying the covered operations in a transparent manner, speeding up the pre-screening of cloud services not included in the list of covered operations, reduction of the number of impact assessment results obtained from government agencies, sharing the implementation status of educational activities (study sessions, etc.) for each government agency, and sharing the current ISMAP-LIIU adopted by each ministry and agency.

認証制度名称	運営組織国籍	再監査頻度	管理基準数	報告書対応言語	ISO相互認証	評価方法	参照
ISMAP	日本	１年毎	1,157	日本語	しない	監査法人	https://www.ismap.go.jp/csm
FedRAMP	米国	１年毎３分の１監査	325 (中), 421 (高)	英語	しない	監査法人	https://www.fedramp.gov/
BSI C5	ドイツ	１年毎	121	英語、ドイツ語	する	監査法人	https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html
ENS	スペイン	２年毎	73	スペイン語	する	監査法人	https://www.ccn.cni.es/index.php/es/esquema-nacional-de-seguridad-ens/esquema-nacional-de-seguridad
CSPN	フランス	３年毎	該当なし	英語、フランス語	しない	第三者評価 ＋ANS	https://www.ssi.gouv.fr/administration/produits-certifies/cspn/
AgID	イタリア	２年毎	20	イタリア語	しない	自己評価	https://cloud.italia.it/
Cyber Essentials	英国	１年毎	89	英語	しない	自己評価	https://www.ncsc.gov.uk/cyberessentials/overview
Cyber Essentials +	英国	１年毎	89	英語	しない	監査法人	https://www.ncsc.gov.uk/cyberessentials/overview
IRAP	オーストラリア	２年毎	837	英語	他の承認に使った	監査法人	https://www.cyber.gov.au/acsc/view-all-content/programs/irap
ISO 27001	国際	１年毎の維持審査	93 (Annex A 規格)	英語	する	監査法人	https://www.iso.org/standard/82875.html
Common Criteria	国際	５年間有効	トによって異なる	英語	しない	監査法人（認定テ	https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/IT-Sicherheiskriterien/CommonCriteria/commoncriteria_node.html

Certification Nam	Country	Frequency of Aud	Number of Contro	Submission langu	Recognition of ISO	Verification meth	Reference
ISMAP	Japan	Annual	1,157	Japanese	No	External audit	https://www.ismap.go.jp/csm
FedRAMP	US	1/3 assessed annu	edium), 421 (High)	English	No	External audit	https://www.fedramp.gov/
BSI C5	Germany	Annual	121	English, German	Yes	External audit	https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html
ENS	Spain	Biennial	73	Spanish	Yes	External audit	https://www.ccn.cni.es/index.php/es/esquema-nacional-de-seguridad-ens/esquema-nacional-de-seguridad
CSPN	France	Triennial	N/A	English, French (re	No	Third party evaluat	https://www.ssi.gouv.fr/administration/produits-certifies/cspn/
AgID	Italy	Biennial	20	Italian	No	Self-assessment	https://cloud.italia.it/
Cyber Essentials	UK	Annual	89	English	No	Self-assessment	https://www.ncsc.gov.uk/cyberessentials/overview
Cyber Essentials +	UK	Annual	89	English	No	External audit	https://www.ncsc.gov.uk/cyberessentials/overview
IRAP	Australia	Biennial	837	English	Can re-use evidence u	External audit	https://www.cyber.gov.au/acsc/view-all-content/programs/irap
ISO 27001	International	Annual verification	93 Annex A Control	English	Yes	External audit	https://www.iso.org/standard/82875.html
Common Criteria	International	Five year life-span	g on security target	English	No	External audit (cert	https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/IT-Sicherheiskriterien/CommonCriteria/commoncriteria_node.html