REQUEST FOR COMMENT RESPONSE

Proposed Amendments to the ISMAP Management Standards

17 October 2025

I. INTRODUCTION

CrowdStrike appreciates the opportunity to provide our comments to the draft Information System Security Management and Assessment Program ("ISMAP") Management Standards. We welcome the work done by the Government of Japan to modernize ISMAP. The proposed approach to align ISMAP more closely with current widely-adopted international standards, simplify the control set, introduce a risk-based precheck to reduce rework, clarify audit-period rules, and enable evidence reuse through inheritance from underlying ISMAP-certified services will improve security assurance for users of these cloud-based services, and reduce avoidable complexity.

CrowdStrike is an international cybersecurity company based in the United States, that helps protect businesses around the world from globally-distributed cyber threats. We have extensive experience helping organizations prevent data breaches with a range of cybersecurity products and services including cyber threat intelligence; proactive hunting, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace.

We support the revisions and respectfully offer some recommendations that from our perspective will strengthen consistency across auditors and providers while maintaining the security-outcomes and integrity of the ISMAP certification process.

II. BEST-PRACTICE PRINCIPLE

Alignment of local requirements to widely-adopted international standards is very helpful and promotes interoperability of security requirements between jurisdictions. The best practice for security certification schemes is to accept existing certifications from widely adopted international standards and accredited assessments (e.g., NIST SP 800-53 or ISO/IEC 27001, 27017, 27018) as sufficient where control intent/outcomes match the government's requirements. This is especially important for physical security components of ISMAP, where existing cloud providers leverage facilities that themselves are not SaaS entities but may be subject to additional, burdensome audits.

By taking this approach the ISMAP certification process would then only have to audit/assess any new or Japan-specific requirements beyond those already audited security standards (as a delta audit).

This reduces variance and duplication, while keeping assurance high, and speeds secure government agency adoption of advanced cloud-based technologies.

III. COMMENTS

There are a number of positive suggestions in the draft proposal that will greatly improve the efficiency of the process whilst maintaining the high security standards required by the Japanese Government. These points demonstrate a forward-thinking approach to modernizing the ISMAP framework.

- **Modernization and alignment.** The draft explicitly aligns its control set with updated widely-adopted international standards as a security baseline. This allows the Government of Japan to take advantage of international investments in security standard development, reduces unique interpretations, and can enable reuse of existing evidence.
- **Control reduction.** A smaller, clearer set of risk-based controls maintains a strong security posture that requires less audit overhead.
- **Pre-check to prevent rework.** A formal mechanism to validate scope and risk-based exclusions before audit is a practical way to increase efficiency into the ISMAP audit process.
- **Inheritance of controls.** Allowing providers to inherit evidence from ISMAP-listed services and infrastructure they are built on avoids duplicative testing and reflects the modern shared-responsibility security model.
- **Clarity around the frequency of evidence collection and audit-period.** Publishing example frequencies and tightening period rules (no gaps, clear expectations for subsequent events) promote predictable, continuous compliance.
- **Recognition of crypto-erase.** Explicit acceptance of cryptographic erasure brings ISMAP in line with modern cloud-native data-sanitization practices.

IV. RECOMMENDATIONS

CROWDSTRIKE

We respectfully recommend the following amendments to the proposed ISMAP process to deliver additional clarity, predictability and efficiency for all parties participating in the process.

1. State the document hierarchy plainly in the ISMAP process. That is the ISMAP standard document is mandatory, while the Guideline and Handbook are simply implementation aids that provide suggestions for equivalent controls permitted with justification.

   This stops “guidance creep” or mis-interpretations skewing the expectations of ISMAP auditors.

2. Provide a machine-readable version of the ISMAP control list (API/CSV with regions, scope notes, versions) as well as a machine-readable cross-walks (JSON/CSV) to convert from the old to new ISMAP controls, the Unified Standards, and NIST SP 800-53.

   This will provide faster scoping and inheritance verification for vendors, and help eliminate mis-interpretation of controls and migration errors as the new process is implemented.

3. Publish a table of changes (delta summaries) for any non-public sections (ie ISO 27017/27014).

   This will allow vendors implementing the new ISMAP process to update libraries confidently without copyrighted text.

4. Provide a range of concrete exclusion examples per control family in the supporting ISMAP documentation.

   This will guide auditors through the initial implementation of applying “risk-based exclusions” and can help it be more predictable over time.

5. Standardize the pre-check process with a framework and a minimum time to complete (e.g., 10 business days).

   This provides clear expectations for auditors and vendors, and fewer surprises.

6. Provide examples for change-log fields for individual control statements for continuous assessment and renewal processes.

This will improve the efficiency of the process and will mean faster renewals and less variance of change records between vendors.

7. Tighten the guidance on control-inheritance to help vendors communicate what is covered by an inherited control for an ISMAP-listed component of a product, and what residual responsibilities remain for the control objective.

   This will provide more consistent auditor expectations for the inheritance component of ISMAP audits.

8. Calibrate ISMAP Standard Audit Procedures documents to help auditors adopt common global practices (reasonable assurance, materiality, and risk-based sampling). Prioritize tests of operating effectiveness over prescriptive paperwork checks by explicitly requiring that minor documentation variances that do not affect security outcomes do not trigger findings.

   This will keep security strong while reducing variance, rework and unnecessary cost, helping Japanese government agencies move to trusted cloud faster.

9. Document audit-period rules with worked examples (renewals, shortened periods, subsequent events).

   This will allow for consistent planning and fewer late issues for vendors and auditors.

10. Clarify acceptable evidence for crypto-erase (e.g., key-destroy logs, approvals, verifier outputs, approved processes).

    This will set auditor expectations for the new control, and provide more consistent evidence across vendors and storage types.

11. Publish a bilingual glossary of key terms.

    This reduces translation ambiguity for multinational providers mapping ISO/SP controls.

We respectfully further recommend the following amendments to the proposed process to maintain the long-term consistency of the ISMAP certification.

12. Offer “delta-audit” renewals when individual control statements show no material control changes across periods.

This rewards continuous compliance by vendors throughout the process and reduces unnecessary audit duplication.

13. Synchronize the release and effective dates for the ISMAP Standard, Guideline, Handbook, and Standard Audit Procedures. Allow a 6-month transition for auditors and vendors to understand and adapt the new process.

    This will allow smoother adoption of the new process and avoids any mid-stream rework and confusion that could arise from staggered release of documentation.

14. Formalize shared-responsibility relationships for common cloud computing products (IaaS vs PaaS vs SaaS) with diagrams and sample evidence splits.

    As a longer-term goal this will better align expectations across vendors and auditors and lead to more consistency of audit documentation.

15. Model multi-region scope and inheritance with sample scope statements.

    This prevents potential disputes about regional boundaries and upstream evidence for multi-region, high-resilience deployments.

V. CONCLUSION

These recommendations keep the spirit of the reform intact while making it easier to implement consistently. If adopted, these recommendations would strengthen security by reducing variance, rework and unnecessary cost, which helps Japanese Government agencies migrate to trusted cloud-based services faster. CrowdStrike views these as key recommendations because they build on the existing draft: fewer controls but a higher bar (implement-by-default), an effective pre-check process, more effective audit processes, and explicit inheritance.

We appreciate the Japanese Government's leadership in modernizing ISMAP and would welcome further dialogue as the standards and procedures are further finalized.

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

Drew Bagley
VP & Counsel, Privacy and Cyber Policy

Brian Fletcher
Director, Public Policy APJ

Email: policy@crowdstrike.com

VI. ABOUT CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

Learn more: https://www.crowdstrike.com/.