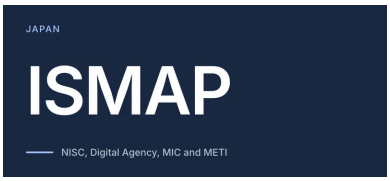
SmartSuite

Framework / Cloud Security / Other

ISMAP (Japan)

ISMAP is Japan's government program that audits and registers cloud services so agencies can procure them; run by NCO, the Digital Agency, MIC and METI.



What it is

ISMAP (Information system Security Management and Assessment Program, in Japanese the Security Evaluation Scheme for Government Information Systems) is the Japanese government's program for evaluating and registering cloud services against the government's security requirements, so that national agencies can procure from a list of pre-assessed services. It is not a statute: the Cyber Security Strategic Headquarters decided its basic framework on 30 January 2020, operation began in June 2020, and the first Cloud Service List was published in March 2021. Government agencies generally procure from the ISMAP lists, so a cloud provider that wants to sell to them seeks registration.

At a glance

PUBLISHER
Government of Japan: National Cybersecurity Office (Cabinet Secretariat), Digital Agency, MIC and METI; operation support by IPA

TYPE
Framework

VERSION
ISMAP Control Standards of June 3, 2020, last revised August 1, 2024; ISMAP-LIU from November 1, 2022; revision released for public comment September 2025

EFFECTIVE
June 2020 (operation began); first Cloud Service List March 2021

DOMAIN
Cloud Security

FAMILY
Other

REGION
Japan

INDUSTRY
Government & Public Sector

ADOPTION MODEL
Industry Requirement

IMPLEMENTATION COMPLEXITY
High

Source: cyber.go.jp/policy/group/general/ismap.html

Why it matters

- **A route into government procurement** Registered services appear on the public ISMAP lists, and agencies in principle buy from those lists; an agency does not have to check the provider's controls itself.
- **An audited assertion, not a self-assessment** The provider asserts compliance with the Control Standards (Standards 2.2) and a registered audit body examines design (design evaluation) and operation (operating effectiveness evaluation).
- **Continuing obligations** Registered providers must promptly report incidents with a serious impact on users (Basic Regulation 3.7) and notify material control changes (3.8).
- **Public transparency** The list shows the service name, scope, audit period and which control objectives apply, so agencies see what the registration covers.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports ISMAP

Assertion Scope Register

Record the cloud service name, scope, region and the underlying services used, with owners, as the written statement of Standards 2.2 requires.

Control Objective and Detailed Control Selection

Hold governance, management and control criteria with the B and PB controls marked, and record the reason for every excluded objective or unselected detailed control.

Audit Period and Registration Calendar

Track the audit period (maximum one year, no gaps), the three-month minimum for shorter periods and the expiry set at one year and four months after the period ends.

Findings and Improvement Plans

Log audit findings with owners, the improvement plan and the deadline, which IPA's review expects within two months of the report date for minor findings.

Incident and Change Notifications

Run a record for incidents with a serious impact on users (Basic Regulation 3.7) and material control changes (3.8) with notice dates and responsible people.

Underlying Service Oversight

Track each underlying cloud service in Third Party Risk Management and whether it is on an ISMAP list, as Standards 2.2.2 requires for services outside the assertion.

Common framework mappings

CSA STAR | FedRAMP Rev. 5 | ISO 27001:2022 | ISO 27017 | ISO 27018 | ISO 27701 | NIST CSF 2.0 | NIST 800-53 Rev.5

Official resources

ISMAP Overview

Provides a detailed explanation of the ISMAP framework and its significance for cloud services.

ismap.go.jp/csm?id=ismap_en

ISMAP Security Control Requirements

Defines the mandatory security controls required for compliance with ISMAP.

ismap.go.jp/en/info/documents/control-guidelines.pdf

ISMAP Assessment Guide

Outlines the process and criteria for conducting assessments under the ISMAP framework.

ismap.go.jp/en/info/documents/assessment-guide.pdf

ISMAP Implementation Guidance

Offers official guidance on implementing ISMAP requirements for cloud services.

ismap.go.jp/en/info/documents/implementation-guidelines.pdf

Frequently asked questions

What is ISMAP and who runs it?

ISMAP, the Information system Security Management and Assessment Program, is the Japanese government's program for evaluating and registering cloud services that meet its security requirements. The National Cybersecurity Office, the Digital Agency, MIC and METI are responsible for it, a Steering Committee decides registrations, and IPA is the operation support agency (Basic Regulation 1.4 and 9.3).

Is ISMAP registration mandatory for cloud providers?

It is not a law, and registration is not mandatory for providers in general. Procuring government agencies are expected, in principle, to buy from the ISMAP lists (Basic Regulation 2.3), so a provider that wants to sell cloud services to national agencies needs a registered service. A registration is a decision of the Steering Committee, not an ISO-style certificate.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How does a cloud service get registered?

The provider states its compliance with the ISMAP Control Standards, selects a registered audit body, and receives the audit report (Basic Regulation 3.2). It applies to the Steering Committee, which reviews the application with IPA's technical review and, if appropriate, registers the service on the list (3.3 to 3.6). Registration is valid to one year and four months after the end of the audited period (3.5).

What is ISMAP-LIU?

ISMAP for Low-Impact Use (ISMAP-LIU) is a track within ISMAP for SaaS services used for low-risk work and information. It has its own registration rule and list, and it has been in operation since 1 November 2022 (Basic Regulation 1.3 and 1.4.13).

What standards do the ISMAP Control Standards use, and are they changing?

They build on the 2016 cloud information security control standards, which follow JIS Q 27001:2014, JIS Q 27002:2014 and JIS Q 27017:2016, with JIS Q 27014:2015 for governance, and reference the government's common standards and NIST SP 800-53 Rev. 4. The last revision was on 1 August 2024. A draft revision reflecting the revised JIS Q 27001 and 27002 and NIST SP 800-53 Rev. 5 went to public comment from 18 September to 17 October 2025.

License included / downloadable: Yes The ISMAP rules, Control Standards and lists are published free by the Japanese government on the ISMAP portal; controls taken from JIS Q 27017 and JIS Q 27014 are not published for copyright reasons. The platform links to the government's page.

Full framework page and mappings: smartsuite.com/frameworks/japan-ismap-information-system-security-management-assessment-program