SmartSuite

Framework / Cybersecurity / Other

Guidelines on Cybersecurity for the Financial Sector (Financial Services Agency, October 4, 2024; revised July 4, 2025)

The FSA's Guidelines on Cybersecurity for the Financial Sector, applied from October 4, 2024, set fundamental and recommended cybersecurity measures for Japanese financial institutions.



What it is

The Guidelines on Cybersecurity for the Financial Sector are the supervisory guidelines of Japan's Financial Services Agency (FSA) that set out what the FSA expects every supervised financial institution to do about cybersecurity. They apply to banks, insurers, securities firms, payment, crypto-asset and other regulated businesses listed in section 1.4. The FSA issued them on October 4, 2024, after a public comment period from June 28 to July 29, 2024, and applied them from that day alongside amendments to its Comprehensive Guidelines for Supervision.

The Guidelines are not a statute. They sit beside the Comprehensive Guidelines for Supervision and the laws that require sound and appropriate operations, such as Article 12-2(2) of the Banking Act, Article 35-3 of the Financial Instruments and Exchange Act and Article 100-2-1(1) of the Insurance Business Act (section 1.1).

At a glance

PUBLISHER
Financial Services Agency (FSA), Government of Japan

TYPE
Guidance

VERSION
Guidelines on Cybersecurity for the Financial Sector, issued October 4, 2024, revised July 4, 2025

EFFECTIVE
October 4, 2024

DOMAIN
Cybersecurity

FAMILY
Other

REGION
Japan

INDUSTRY
Financial Services

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: fsa.go.jp/en/policy/cybersecurity/index.html

Why it matters

- **Executive accountability** Section 2.1.1 requires the board and senior management to set a basic cybersecurity policy, review the framework at least once a year, appoint a person such as a CISO to oversee cybersecurity, and receive a report at least once a year.
- **Two tiers of expectation** Every item is either a fundamental response measure or a recommended measure, so a regional bank and a major bank can see which expectations apply to each.
- **A defined supervisory scope** Section 1.4 lists the institutions covered, from major and regional banks to crypto-asset exchange service providers, prepaid payment instrument issuers and financial instruments exchanges.
- **Coverage of the whole group** Section 1.2.1 expects a consistent cybersecurity framework across a group, including overseas locations, adjusted for the scale of each subsidiary.

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

How SmartSuite supports JFSA Cybersecurity Guidance

Fundamental and Recommended Measures

Record each section 2 measure as a requirement, mark which tier the institution applies and link it to a policy, control and owner.

Annual Governance Cycle

Track the annual framework review, risk assessment and senior management report required by sections 2.1.1 and 2.2.2.2 with dates and approvals.

Cyber Risk Assessment

Register cyber risks with likelihood, impact, treatment plan and the vulnerability assessment and penetration test findings of section 2.2.4 in Cyber & IT Risk.

Incident and Recovery Records

Keep response plans, recovery time objectives, exercise results and post-incident corrective actions for the section 2.5 stages.

Third-Party Ledger

Maintain the third-party ledger, due diligence, contract clauses and monitoring that section 2.6(5) to (9) describe in Third Party Risk Management.

Supervisory Readiness

Assemble evidence and gaps by section for FSA inspections and monitoring, plus internal audit findings under section 2.1.5.

Common framework mappings

CIS Controls v8.1 | EU DORA | ISO 27001:2022 | MITRE ATT&CK | NIST CSF 2.0 | NIST 800-53 Rev.5 | SOC 2 | SWIFT CSCF

Official resources

JFSA Cybersecurity Guidance Overview

Describes the cybersecurity guidance framework for financial institutions by the Japan Financial Services Agency.

fsa.go.jp/en/policy/cybersecurity/index.html

JFSA Regulatory Implementation Guide

Provides detailed implementation guidance for financial institutions to comply with JFSA cybersecurity requirements.

fsa.go.jp/common/law/cybersecurity_guideline_en.pdf

Frequently asked questions

Who must follow the FSA Guidelines on Cybersecurity for the Financial Sector?

Section 1.4 applies the Guidelines to all financial institutions and related entities subject to the FSA's Comprehensive Guidelines for Supervision. The list includes major and regional banks, insurers, financial instruments business operators, money lending and funds transfer businesses, prepaid payment instrument issuers, crypto-asset exchange service providers, electronic payment service providers, market infrastructures and exchanges. They are supervisory guidelines, not a statute.

What is the difference between fundamental response measures and recommended measures?

Fundamental response measures are the baseline cyber hygiene actions every institution should take. Recommended measures are advanced practices for institutions whose incidents could affect local communities, the economy or the financial system, such as major banks and financial market infrastructures (section 1.1). The Guidelines add that they do not mandate uniform responses and that institutions apply a risk-based approach.

When did the Guidelines take effect, and have they changed?

The FSA issued the Guidelines on October 4, 2024, after public comment from June 28 to July 29, 2024, and applied them from that day. On July 4, 2025 it made a technical revision to reflect the reorganization of the Cabinet Cybersecurity Center into the National Cybersecurity Office on July 1, 2025, without a public comment procedure. The English text is a provisional translation.

What do the Guidelines say about multi-factor authentication, testing and backups?

Section 2.3.1(5) requires multi-factor authentication for remote access to critical systems. Section 2.2.4 requires regular vulnerability assessments and penetration tests and recommends regular threat-led penetration testing. Section 2.3.3(5) expects backup policies with isolation, integrity verification and recovery testing, and recommends tamper-resistant backups stored apart from the internal network because of ransomware.

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

What does section 2.6 expect for third-party risk?

Institutions manage cybersecurity risk across the full lifecycle of third-party relationships: a policy, a central oversight department, risk-based identification, a third-party ledger, due diligence before contracting, security requirements and audit rights in contracts or SLAs, continuous monitoring and an exit process (2.6(2) to (10)). Recommended measures add concentration risk, fourth parties and tested exit strategies for critical third parties.

License included / downloadable: Yes The Guidelines are published free by the Financial Services Agency in Japanese, with a provisional English translation for reference only; the platform links to the official pages.

Full framework page and mappings: smartsuite.com/frameworks/jfsa-cybersecurity-guidance-for-financial-institutions

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