SmartSuite

Framework / Risk Management / Other

MAS Technology Risk Management Guidelines (revised January 18, 2021)

The MAS Technology Risk Management Guidelines (January 18, 2021) set MAS's technology and cyber risk expectations for all Singapore financial institutions, backed by binding FSM-N notices.



What it is

The MAS Technology Risk Management Guidelines are the Monetary Authority of Singapore's statement of technology risk management principles and practices for every financial institution it regulates, issued in revised form on January 18, 2021. They are guidelines, not law: paragraph 2.3 says they provide general guidance and do not replace or override legislation, and paragraph 2.2 says the degree of observance is an area MAS considers when supervising an institution, which is why MAS expects FIs to observe them. The legally binding layer is the set of MAS Notices on Technology Risk Management, such as Notice FSM-N05 for banks, which took effect on May 10, 2024 under the Financial Services and Markets Act 2022.

At a glance

PUBLISHER Monetary Authority of Singapore (MAS)	TYPE Framework	VERSION Revised edition, January 18, 2021
EFFECTIVE January 18, 2021	DOMAIN Risk Management	FAMILY Other
REGION Singapore	INDUSTRY Financial Services	ADOPTION MODEL Voluntary
IMPLEMENTATION COMPLEXITY High		

Source: mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines

Why it matters

- **Supervisory expectations in writing** Fifteen chapters of expectations covering governance, the risk framework, development, operations, resilience, security, cyber operations and testing, online services and audit, read with MAS's legislation, notices and directions (paragraph 2.3).
- **Named accountable officers** Paragraph 3.1.3: a Chief Information Officer, Chief Technology Officer or Head of IT and a Chief Information Security Officer or Head of Information Security with the requisite expertise, appointments approved at least by the CEO; paragraph 3.1.2: board and senior management members who understand technology and cyber risk.
- **A binding layer with numbers** Notice FSM-N05 (banks) and its parallel notices for other FI classes: critical system identification, four-hour downtime cap per 12 months, four-hour RTO validated every 12 months, one-hour incident notification, 14-day root cause report, IT controls over customer information.

© 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports MAS TRM 2021

Guidelines Requirement Library

Load chapters 2 to 15 as requirements by paragraph (for example 3.1.3, 4.1.3, 8.1.2, 12.1, 13.2) with the control, owner and evidence that answers each, and the proportionality rationale under paragraph 2.2.

Technology Risk Register

Keep chapter 4 risks in Cyber & IT Risk with a named risk owner, assessment, treatment and monitoring, and report to the board or its delegated committee as paragraph 3.1.7 expects.

Third-Party Technology Oversight

Record pre-contract assessments and ongoing monitoring of third-party and cloud providers under paragraph 3.4 in Third Party Risk Management.

Critical Systems and Incident Clocks

Maintain the FSM-N05 critical system list, log unscheduled downtime against the four-hour annual cap, track the one-hour MAS notification and the 14-day root cause report through IT Service Management (ITSM) incidents.

Testing and Exercise Program

Schedule and evidence vulnerability assessments, penetration tests, cyber exercises and adversarial attack simulations under chapter 13, with remediation tracked to closure (13.6).

IT Audit and Board Reporting

Plan chapter 15 IT audits over the auditable areas, track findings and remediation in Internal Audit Management, and assemble the board's view of technology risk from the same records.

Common framework mappings

COBIT 2019 | EU DORA | FFIEC IT Handbook | ISO 27001:2022 | ISO 27002:2022 | NIST CSF 2.0 | NIST 800-53 Rev.5 | SWIFT CSCF

Official resources

Technology Risk Management Guidelines

Defines the MAS requirements for managing technology and cybersecurity risks in financial institutions.

mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf

Frequently asked questions

Are the MAS Technology Risk Management Guidelines legally binding?

No. Paragraph 2.3 says the Guidelines provide general guidance and do not replace or override legislation, and paragraph 2.2 says they are not a statement of the standard of care owed to customers. They still matter in supervision: paragraph 2.2 makes the degree of observance an area MAS considers, and MAS said on issuing them that it expects financial institutions to observe them. The binding requirements sit in the MAS Notices on Technology Risk Management, such as Notice FSM-N05 for banks.

Who do the Guidelines apply to?

All financial institutions regulated by MAS. MAS's page lists banks, merchant and wholesale banks, finance companies, card issuers and financial holding companies, insurers, reinsurers, insurance agents and brokers, capital markets intermediaries, fund managers, exchanges and depositories, payment system operators and payment institutions, money-changers, financial advisers and licensed trust companies. Paragraph 2.2 lets each institution apply them in proportion to the risk and complexity of its services.

Updated Oct 29, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What did the January 2021 revision expect of the board and senior management?

Chapter 3 expects board and senior management members with the knowledge to manage technology and cyber risk (3.1.2), the appointment of a Chief Information Officer, Chief Technology Officer or Head of IT and a Chief Information Security Officer or Head of Information Security with the requisite expertise, approved at least by the CEO (3.1.3), a technology risk management strategy (3.1.4), IT decisions within risk appetite (3.1.5) and a board-owned risk framework with a technology risk management function (3.1.7).

What does Notice FSM-N05 require of banks?

Notice FSM-N05, issued on May 9, 2024 under section 29(1) of the Financial Services and Markets Act 2022 and effective May 10, 2024, requires a bank to identify its critical systems; keep unscheduled downtime for each critical system to no more than four hours in any 12 months; set a recovery time objective of not more than four hours and validate it every 12 months; notify MAS within one hour of discovering a relevant incident; submit a root cause and impact analysis within 14 days; and implement IT controls protecting customer information. It replaced Notice 644, withdrawn the same day.

What testing do the Guidelines expect?

Chapter 13 expects vulnerability assessments (13.1), penetration testing with a combination of black-box and gray-box tests for online financial services and the option of a bug bounty program (13.2), cyber exercises (13.3), adversarial attack simulation exercises conducted under defined objectives, scope and rules of engagement (13.4), intelligence-based scenario design (13.5) and tracked remediation (13.6). Chapter 15 adds an IT audit that gives the board an independent opinion on the controls.

License included / downloadable: Yes The Guidelines and the MAS Notices on Technology Risk Management are published free as PDFs on the Monetary Authority of Singapore's website; the platform links to the official pages.

Full framework page and mappings: smartsuite.com/frameworks/singapore-mas-trm-2021-technology-risk-management-guidelines