SmartSuite

Framework / Risk Management / Other

HKMA Supervisory Policy Manual (SPM) — TRM

HKMA TRM sets standards for managing technology and cybersecurity risks to ensure operational resilience in Hong Kong's authorized financial institutions.

What it is

The HKMA Supervisory Policy Manual — Technology Risk Management (TRM) is a regulatory framework that sets out standards and guidelines for managing technology and cybersecurity risks within authorized institutions in Hong Kong. It aims to ensure robust risk management practices to safeguard information assets and maintain operational resilience in the banking sector.

Published by the Hong Kong Monetary Authority (HKMA), the TRM framework applies to banks and other authorized financial institutions operating in Hong Kong. It addresses key areas such as information security, cybersecurity controls, system integrity, outsourcing risk, incident response, and technology governance, with a focus on compliance, risk management, and resilience against emerging threats.

At a glance

PUBLISHER Hong Kong Monetary Authority (HKMA)	TYPE Guidance	VERSION HKMA Supervisory Policy Manual — Technology Risk Management Modules
EFFECTIVE 2017	DOMAIN Risk Management	FAMILY Other
REGION Hong Kong	INDUSTRY Financial Services	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: https://brdr.hkma.gov.hk/eng/spm

Why it matters

- **Strengthen technology risk governance** Promote consistent risk management practices and leadership oversight to ensure accountability for technology-related decisions across the institution.
- **Enhance regulatory compliance** Align technology controls and reporting with HKMA expectations, reducing the likelihood of compliance breaches and associated penalties.
- **Improve operational resilience** Minimize service disruptions and maintain essential banking operations even during technology failures or cyber incidents.
- **Increase audit readiness** Document risk management activities and controls to support efficient regulatory audits and facilitate timely compliance reviews.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports HKMA TRM

Governance and Accountability Hub

Track roles, policies, oversight, and recurring reporting for technology risk.

Risk Assessments and Treatment Plans

Run periodic assessments and manage mitigations with approvals and evidence.

Outsourcing and Vendor Oversight

Track due diligence, contract safeguards, and ongoing monitoring evidence.

Monitoring and Incident Response Workflows

Capture telemetry proof, incident timelines, and post-incident improvements.

Resilience Planning and Testing

Manage recovery plans, exercises, results, and corrective actions.

Supervisory Readiness Reporting

Report posture, gaps, and evidence coverage for supervisory expectations.

Common framework mappings

CIS Controls v8.1 | EU DORA | ISO 27001:2022 | ISO 27002:2022 | MITRE ATT&CK | NIST CSF 2.0 | NIST 800-53 Rev.5 | SOC 2

Official resources

HKMA Supervisory Policy Manual TRM Guidelines

Provides comprehensive guidelines for managing technology risks in authorized institutions.

brdr.hkma.gov.hk/eng/doc-ldg/spm/current/TM-G-1

HKMA Information Security Controls

Describes the required security controls and measures for information systems in banks.

brdr.hkma.gov.hk/eng/doc-ldg/spm/current/TM-G-1

HKMA Incident Management Guidelines

Outlines procedures for managing and reporting cybersecurity incidents in financial institutions.

brdr.hkma.gov.hk/eng/doc-ldg/spm/current/TM-G-1

HKMA Outsourcing Guidelines

Defines requirements for managing risks associated with outsourcing financial services.

brdr.hkma.gov.hk/eng/doc-ldg/spm/current/SA-2

Frequently asked questions

What is the HKMA TRM framework used for?

The HKMA Supervisory Policy Manual — Technology Risk Management (TRM) is designed to establish standards and guidelines for managing technology and cybersecurity risks in authorized financial institutions in Hong Kong. It aims to protect information assets, ensure operational resilience, and support regulatory oversight in the banking sector.

Is compliance with the HKMA TRM mandatory?

Yes, compliance with the HKMA TRM framework is mandatory for all authorized institutions regulated by the Hong Kong Monetary Authority. Organizations are expected to demonstrate adherence through regular assessments, governance practices, and documentation of implemented controls.

Which organizations does the HKMA TRM framework apply to?

The HKMA TRM applies to all authorized institutions operating under the Hong Kong Monetary Authority, including banks and stored value facility licensees. The scope covers their operations, technology systems, outsourced services, and all supporting digital infrastructure relevant to Hong Kong operations.

What key controls or artifacts are required by the HKMA TRM?

Required controls include risk assessments, information security policies, system integrity checks, incident management procedures, outsourcing risk frameworks, and documented governance structures. Institutions must also establish regular monitoring, reporting mechanisms, and evidence of compliance activities.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How should organizations implement the HKMA TRM framework?

Implementation begins with conducting a technology risk assessment and mapping existing controls to HKMA supervisory requirements. Institutions should then formalize risk management policies, deploy security controls, create incident response plans, and integrate TRM requirements into overall governance and compliance programs.

How does the HKMA TRM relate to other global cybersecurity frameworks?

The HKMA TRM is aligned with leading international cybersecurity standards such as ISO 27001, NIST, and local regulatory guidance. It complements these by providing sector-specific requirements that address Hong Kong's regulatory landscape, ensuring both global best practice alignment and local compliance.

What are the ongoing compliance requirements for the HKMA TRM?

Institutions must conduct periodic technology risk assessments, maintain up-to-date security controls, provide incident reports, and undergo supervisory reviews as required by the HKMA. Ongoing training, regular audits, and continuous monitoring are also critical for sustaining compliance.

How would SmartSuite support HKMA TRM?

SmartSuite enables institutions to operationalize HKMA TRM through centralized risk registers, mapped control libraries, and automated policy governance workflows. It supports robust evidence collection, compliance tracking, audit readiness, and comprehensive reporting dashboards to monitor and improve risk management posture and meet regulatory obligations.

License included / downloadable: Yes The HKMA Supervisory Policy Manual and Technology Risk Management guidance are publicly available through the Hong Kong Monetary Authority.

Full framework page and mappings: smartsuite.com/frameworks/hkma-supervisory-policy-manual-technology-risk-management-trm