SmartSuite

Framework / Operational Resilience / Other

HKMA C-RAF v1.0

HKMA C-RAF is a mandatory framework for Hong Kong banks to assess and strengthen cyber resilience and incident response.

HONG KONG MONETARY AUTHORITY
香港金融管理局

What it is

The HKMA Cyber Resilience Assessment Framework (C-RAF) is a cybersecurity and risk management framework that assists authorized institutions in assessing and enhancing their cyber resilience capabilities. Its primary purpose is to strengthen organizational ability to prevent, detect, respond to, and recover from cyber threats within the Hong Kong banking sector.

Issued by the Hong Kong Monetary Authority (HKMA), the C-RAF is mandatory for banks and other authorized financial institutions operating in Hong Kong. The framework covers cybersecurity controls, risk management practices, governance structures, incident response, and operational resilience, aligning local expectations with international standards and regulatory requirements.

At a glance

PUBLISHER Hong Kong Monetary Authority (HKMA)	TYPE Assessment / Maturity Model	VERSION HKMA Cyber Resilience Assessment Framework
EFFECTIVE 2017	DOMAIN Operational Resilience	FAMILY Other
REGION Hong Kong	INDUSTRY Financial Services	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech/research-and-applications/cybersecurity-fortification-initiative-cfi/

Why it matters

- **Strengthen cybersecurity governance** Establish clear accountability and oversight for cybersecurity risk management through defined roles and systematic evaluation processes.
- **Enhance regulatory alignment** Support compliance with HKMA requirements and facilitate adherence to recognized international cybersecurity standards and frameworks.
- **Promote operational resilience** Improve the organization's ability to withstand, respond to, and recover from cybersecurity incidents impacting critical banking operations.
- **Improve threat detection and response** Bolster incident management capabilities and enable timely detection, escalation, and containment of cyber threats and breaches.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports HKMA C-RAF

Inherent Risk and Maturity Assessments

Run assessments, capture scoring, and attach supporting evidence.

Gap Remediation Roadmap and Ownership

Turn gaps into a prioritized roadmap with owners and milestones.

Testing and Exercise Cadence

Schedule resilience testing and record outcomes and improvement actions.

Monitoring and Incident Response Workflows

Track telemetry coverage, incident timelines, and corrective actions.

Provider Dependency and Contingency Planning

Manage provider dependencies, monitoring, and contingency planning evidence.

Leadership Reporting Dashboards

Report maturity, gaps, and progress trends for governance.

Common framework mappings

EU DORA | FFIEC CAT | ISO 27001:2022 | ISO 27002:2022 | NIST CSF 2.0 | NIST 800-53 Rev.5 | SOC 2 | SWIFT CSCF

Official resources

Cyber Resilience Assessment Framework (C-RAF) Overview

Describes the HKMA's framework for assessing cyber resilience in financial institutions.

hkma.gov.hk/eng/key-functions/international-financial-centre/fintech/research-and-applications/cybersecurity-fortification-initiative-cfi

C-RAF Assessment Process Guidelines

Outlines the process and requirements for conducting assessments under the C-RAF.

hkma.gov.hk/eng/key-functions/international-financial-centre/fintech/research-and-applications/cybersecurity-fortification-initiative-cfi

Cybersecurity Fortification Initiative (CFI)

Provides an overview of the initiative aimed at enhancing cybersecurity for HK financial institutions.

hkma.gov.hk/eng/key-functions/international-financial-centre/fintech/research-and-applications/cybersecurity-fortification-initiative-cfi

Frequently asked questions

What is the HKMA Cyber Resilience Assessment Framework (C-RAF) used for?

The HKMA C-RAF is a structured framework designed to help banks and authorized financial institutions in Hong Kong assess, strengthen, and demonstrate their cyber resilience. It is used to identify gaps in cyber risk management, improve security controls, and enhance the ability to prevent, detect, and recover from cyber threats.

Is HKMA C-RAF mandatory for banks in Hong Kong?

Yes, implementation of the HKMA C-RAF is mandatory for all authorized institutions regulated by the Hong Kong Monetary Authority. Organizations are required to regularly conduct cyber resilience assessments and report outcomes to the HKMA as part of ongoing regulatory compliance.

Which organizations are in scope for HKMA C-RAF requirements?

All licensed banks, restricted license banks, and deposit-taking companies operating in Hong Kong fall under the scope of C-RAF. The framework applies to both local and international banking operations managed within Hong Kong's jurisdiction.

 © 2026 SmartSuite Inc. All rights reserved.

What key controls or artifacts are required by HKMA C-RAF?

The C-RAF requires organizations to implement and document cybersecurity controls around governance, risk management, incident response, and operational resilience. Essential artifacts include completed risk assessments, gap analyses, incident response plans, control documentation, and evidence of periodic testing and reviews.

How does an organization implement HKMA C-RAF?

Implementation involves mapping current security controls to C-RAF requirements, conducting risk and maturity assessments, and performing scenario-based exercises. Organizations should document gaps, create remediation plans, and routinely update governance documentation and incident response procedures to align with regulatory expectations.

How does HKMA C-RAF relate to other cybersecurity frameworks?

HKMA C-RAF aligns with international standards such as the NIST Cybersecurity Framework, incorporating similar control families and maturity models. This alignment helps ensure that institutions maintain compliance with both local regulatory requirements and global cybersecurity best practices.

What are the ongoing compliance and reporting requirements for C-RAF?

Institutions must conduct periodic cyber resilience reviews, monitor control effectiveness, and update risk assessments in line with C-RAF's maturity model. Results and remediation actions should be documented, reviewed by governance bodies, and reported to the HKMA as required.

How would SmartSuite support HKMA C-RAF?

SmartSuite can support HKMA C-RAF compliance by enabling organizations to manage cyber risk in a centralized platform, track and maintain security controls, and store audit-ready evidence. It facilitates risk register maintenance, automates compliance workflows, and generates configurable reports for governance and regulatory reporting, ensuring audit readiness and streamlined oversight.

License included / downloadable: Yes The Cyber Resilience Assessment Framework is published by the Hong Kong Monetary Authority and is publicly available through official HKMA resources.

Full framework page and mappings: smartsuite.com/frameworks/hkma-c-raf-cyber-resilience-assessment-framework