

BMA Cyber Risk Management Code of Conduct

BMA Cyber Code sets cyber risk management and operational resilience requirements for Bermuda-regulated financial institutions.



What it is

The Bermuda BMA Cyber Risk Management Code of Conduct (BMA Cyber Code) is a regulatory framework that helps organizations strengthen cybersecurity defenses, manage technology risks, and ensure compliance with regulatory expectations. This Code is tailored for entities regulated by the Bermuda Monetary Authority (BMA) and establishes requirements for robust cyber risk management and operational resilience.

Published by the Bermuda Monetary Authority, the BMA Cyber Code applies to insurers, banks, investment firms, and other financial institutions under BMA supervision. The framework covers key areas such as cybersecurity controls, risk assessment, governance structures, incident response, and compliance oversight, aligning with global regulatory trends and industry best practices.

At a glance

PUBLISHER Bermuda Monetary Authority (BMA)	TYPE Framework	VERSION BMA Cyber Risk Management Code of Conduct
EFFECTIVE 2019	DOMAIN Cybersecurity	FAMILY Other
REGION Bermuda	INDUSTRY Financial Services	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: <https://www.bma.bm/documents-centre>

Why it matters

- **Strengthen cybersecurity governance** Enhance leadership oversight and accountability through clearly defined cyber risk management roles and responsibilities.
- **Promote regulatory compliance** Support alignment with evolving BMA requirements and global standards, reducing the risk of regulatory penalties or compliance gaps.
- **Enhance operational resilience** Reduce the likelihood of disruptions by implementing robust controls and continuity planning for critical business systems.
- **Improve incident response readiness** Enable consistent and timely detection, escalation, and response to cyber incidents, minimizing potential financial and reputational impact.

How SmartSuite supports BMA Cyber Code

Cyber Risk Management Framework

Structure cybersecurity policies, control domains, and governance aligned to BMA requirements.

Cyber Risk Assessments and Treatment

Track cyber risks, mitigation plans, and ongoing risk evaluations across systems.

Access and Authentication Control Management

Manage user access, authentication, and privileged account controls.

Security Monitoring and Incident Response

Monitor threats and manage incident detection, response, and escalation workflows.

Third-Party and Outsourcing Risk Oversight

Assess vendor cybersecurity posture and track third-party risk management activities.

Regulatory Reporting and Compliance Monitoring

Provide dashboards showing cyber risk posture, control coverage, and BMA compliance readiness.

Common framework mappings

CIS Controls v8.1

EU DORA

ISO 27001:2022

ISO 27002:2022

ISO 27017

ISO 27701

NIST CSF 2.0

SOC 2

Official resources

Bermuda BMA Cyber Risk Management Code of Conduct

Defines the requirements for cyber risk management for entities regulated by BMA.

bma.bm/documents-centre

BMA Guidance Notes on Cyber Risk

Provides insights into implementing and adhering to BMA's Cyber Code requirements.

bma.bm/documents-centre

BMA Regulatory Framework Overview

Outlines the regulatory framework governing financial institutions in Bermuda, including cyber risk.

bma.bm/documents-centre

Cyber Risk Management Statements of Principle and Guidance

Describes principles for cyber risk management and resilience under the BMA framework.

bma.bm/documents-centre

Frequently asked questions

What is the BMA Cyber Code used for?

The BMA Cyber Code is designed to strengthen the cybersecurity posture of organizations regulated by the Bermuda Monetary Authority. It sets clear expectations for cyber risk management, operational resilience, and effective oversight to protect the Bermuda financial sector from technology-related threats.

Is compliance with the BMA Cyber Code mandatory?

Yes, compliance with the BMA Cyber Code is mandatory for all financial services entities regulated by the Bermuda Monetary Authority, including insurers, banks, and investment firms. Failure to comply may result in regulatory enforcement actions and penalties.

Which organizations must comply with the BMA Cyber Code?

The BMA Cyber Code applies to all entities regulated by the Bermuda Monetary Authority, such as banks, insurance companies, investment businesses, and related financial institutions. Each entity must determine the applicability based on its regulatory license and activities.

What are the key requirements of the BMA Cyber Code?

Key requirements include establishing governance for cybersecurity, conducting regular risk assessments, implementing security controls, developing incident response plans, managing third-party risks, and maintaining evidence of continuous compliance. The Code also emphasizes oversight, monitoring, and reporting.

How should organizations implement the BMA Cyber Code?

Organizations should map BMA Cyber Code control families to internal policies, integrate cybersecurity controls into business operations, conduct regular risk and gap assessments, and establish incident response and remediation procedures. Continuous monitoring, documentation, and compliance testing are crucial for demonstrating adherence.

How does the BMA Cyber Code relate to other frameworks like ISO 27001 or NIST?

The BMA Cyber Code is aligned with global standards such as ISO 27001 and the NIST Cybersecurity Framework, sharing similar principles for governance, controls, and risk management. However, it contains Bermuda-specific regulatory requirements and reporting obligations tailored to local financial entities.

What ongoing activities are required to maintain BMA Cyber Code compliance?

Ongoing compliance requires regular reviews of cybersecurity controls, continuous risk assessments, prompt incident reporting, updates to governance documents, and periodic training for staff. Firms must also retain evidence for audits and keep policies and procedures up to date.

How would SmartSuite support the BMA Cyber Code?

SmartSuite streamlines BMA Cyber Code compliance by enabling organizations to track risks, manage cybersecurity controls, and collect evidence systematically. It offers configurable workflows for remediation, audit readiness tools, and compliance dashboards for reporting to internal and external stakeholders, facilitating continuous oversight and governance.

License included / downloadable: Yes The BMA Cyber Risk Management Code of Conduct is publicly available through the Bermuda Monetary Authority.

Full framework page and mappings: smartsuite.com/frameworks/bermuda-bma-cyber-risk-management-code-of-conduct