SmartSuite

Framework / Cybersecurity / Other

BMA Operational Cyber Risk Management Code of Conduct

The BMA Cyber Code requires Bermuda insurers, banks, trust and investment firms to run a board-approved cyber risk program and report significant incidents within 72 hours.



What it is

The BMA Operational Cyber Risk Management Code of Conduct is a set of Bermuda Monetary Authority codes for the sectors the Authority regulates. It covers Bermuda insurers, insurance managers and intermediaries, banks, deposit companies, trust companies, corporate service providers, money service businesses, investment businesses and fund administration providers. Each of them must run a board-approved cyber risk program and tell the BMA about significant cyber incidents within 72 hours.

At a glance

PUBLISHER Bermuda Monetary Authority (BMA)	TYPE Framework	VERSION October 2020 (insurance); September 2022 (other sectors)
EFFECTIVE January 1, 2021 (insurance); March 15 and September 26, 2022	DOMAIN Cybersecurity	FAMILY Other
REGION Bermuda	INDUSTRY Financial Services	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: cdn.bma.bm/documents/2022-09-26-17-22-14-Operational-Cyber-Risk-Management-Code-of-Conduct.pdf

Why it matters

- **Board accountability** The board approves the cyber risk policy each year and receives regular updates on cyber risk status, so oversight cannot be delegated to IT.
- **A fixed incident clock** An officer must notify the BMA within 72 hours of determining or confirming a reportable cyber event, with an incident report due 14 days after notice.
- **Proportionate expectations** A small firm with complex activity still needs a sophisticated framework, because nature, scale and complexity are judged together.
- **Outsourcing stays your risk** A firm may outsource the CISO role or IT functions but never its responsibility for governance and risk (paragraph 27).

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports BMA Cyber Code

Cyber Risk Policy and CISO Accountability

Record the annual board approval of the cyber risk policy, the named CISO and the outsourced-resource oversight the Code requires (paragraphs 14 to 18).

Risk Register with Five-Year Retention

Track each risk through identification, measurement, response and monitoring, and keep the assessment history for the five-year minimum (paragraphs 20 and 21).

72-Hour Notice and 14-Day Report Tracking

Log each cyber reporting event with its determination time, notice date and incident report due date, using automations to notify owners as dates approach (paragraphs 43 and 44).

Outsourcing and Cloud Oversight

Keep each provider's service agreement terms, cloud risk assessment and responsible party in linked records (paragraphs 26 to 30).

Annual Testing and Training Evidence

Schedule the yearly tabletop exercise, staff training, penetration test and business continuity and disaster recovery test, and attach results and remediation items (paragraphs 39, 47, 56 and 66).

Board and Supervisor Reporting

Build dashboards of open risks, incident timelines and test status for the board and for BMA requests.

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

Which firms must follow the BMA Cyber Code, and which version applies?

The Code applies to firms the Bermuda Monetary Authority licenses or registers. Insurers, insurance managers and intermediaries follow the Insurance Sector Code (October 2020, in force January 1, 2021). Banks, deposit companies, corporate service providers, trust companies, money service businesses, investment businesses and fund administration providers follow the Code revised in September 2022. Digital asset businesses have a separate BMA code.

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

How quickly must a cyber incident be reported to the BMA?

An officer must notify the Authority within 72 hours from the time the firm determines or confirms a reportable cyber event, whichever is sooner. An incident report with the root cause, actions taken and any impact follows within 14 days of the initial notice (paragraph 43 of the September 2022 Code). Only events with significant adverse impact must be reported, and firms in doubt should consult the BMA.

What must the board do under the BMA Cyber Code?

The board and senior management must oversee cyber risk, and the board must approve a cyber risk policy at least annually. Regular updates on cyber risk status must reach the board, and the board stays responsible for outsourced activity, including an outsourced CISO (paragraphs 14 and 17).

How does proportionality work under the Code?

The BMA assesses compliance relative to the nature, scale and complexity of the business, considered together rather than separately. A small firm with a complex business is still expected to maintain a sophisticated risk management framework (paragraph 12).

How long must cyber records be kept?

Risk assessments must be documented and kept for at least five years, and incident investigation and response logs must be kept for a minimum of five years and be available to the BMA at any time (paragraphs 21 and 44).

License included / downloadable: Yes The Codes are published free by the Bermuda Monetary Authority at bma.bm and are included with the platform for reference.

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