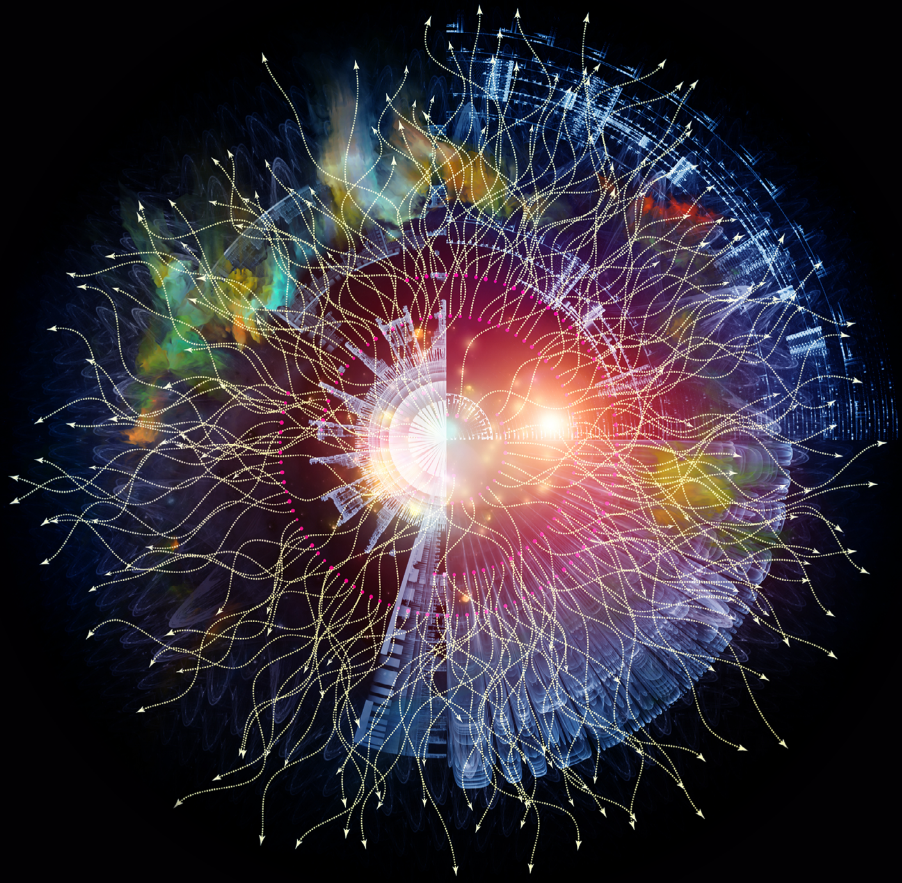
Deloitte.

BMA Insurance Sector Operational Cyber Risk Management Code of Conduct

July 2021



Bermuda Monetary Authority Insurance Sector Operational Cyber Risk Management Code of Conduct

Is your organisation ready?

Across the globe, and in Bermuda, cyber-attacks are increasing in frequency and sophistication. The Financial Services sector is a key target, and there are many well-publicized cybercrime cases involving Financial Institutions. Cybercriminals are becoming more sophisticated, and the cost of cybercrime is becoming increasingly intolerable. The stakeholders – including boards, regulators, investors, analysts, business partners, and customers – expect greater visibility into an organisation's cybersecurity risk management programme.

In light of the growing cyber threats to the insurance sector, the Bermuda Monetary Authority (BMA) published their Insurance Sector Operational Cyber Risk Management Code of Conduct on October 6, 2020. The Code came into force on 1 January 2021 and registrants are required to be in compliance by 31 December 2021.

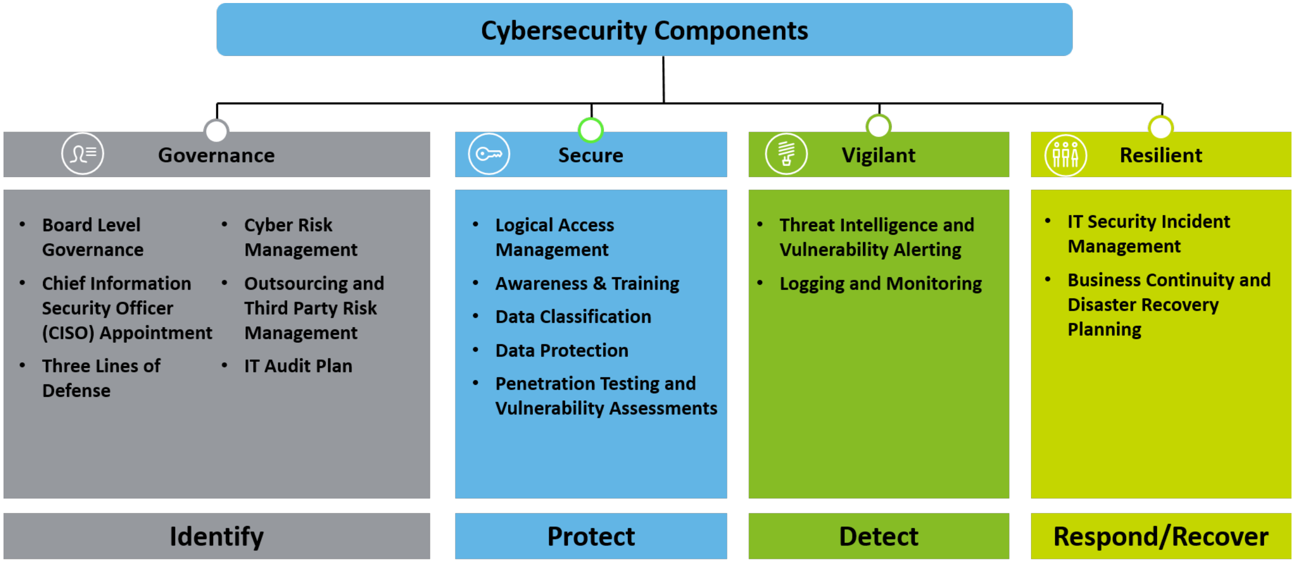
The ultimate goal of the Code is to ensure that insurance entities regulated by the BMA establish a robust cybersecurity program and comply with related requirements.

The Code prescribes specific requirements to ensure appropriate cybersecurity programs are in place.

Regulated entities should implement the Code in proportion to their cyber risk profile (nature, scale and complexity of their business), following an appropriate assessment of their cyber risks. Each entity is required to assess its particular risk profile and design a program that robustly addresses such risks.

Cybersecurity components

The BMA Code of Conduct emphasizes the importance for the regulated entities to ensure that robust cybersecurity measures are in place and that they can appropriately identify, protect, detect, respond to and recover from such cybersecurity-related threats, incidents and breaches. Broadly speaking, the requirements in the Code fall under the four main pillars - Governance. Secure. Vigilant. Resilient.(tm)



Cybersecurity Components

Governance
- Board Level Governance
- Chief Information Security Officer (CISO) Appointment
- Three Lines of Defense
- Cyber Risk Management
- Outsourcing and Third Party Risk Management
- IT Audit Plan

Identify

Secure
- Logical Access Management
- Awareness & Training
- Data Classification
- Data Protection
- Penetration Testing and Vulnerability Assessments

Protect

Vigilant
- Threat Intelligence and Vulnerability Alerting
- Logging and Monitoring

Detect

Resilient
- IT Security Incident Management
- Business Continuity and Disaster Recovery Planning

Respond/Recover

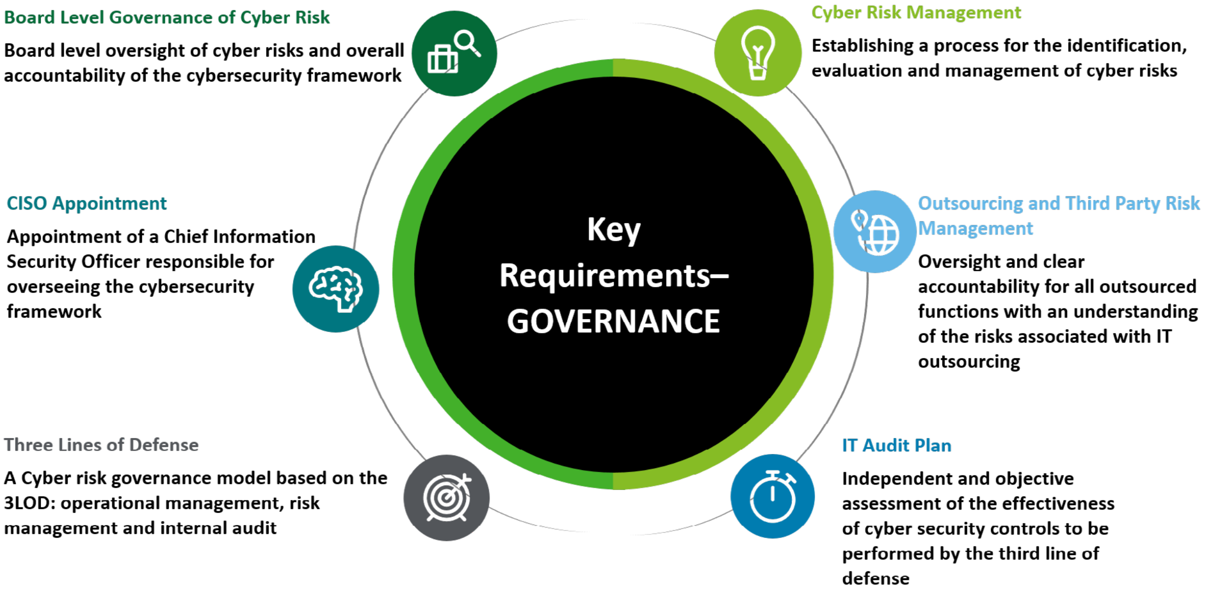
Identify, Protect, Detect, Respond to and Recover are the function areas of the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).

Governance

Regulated entities are required to identify and manage cyber risks to organisational systems, assets, data, and capabilities. They also need to ensure management involvement and sponsorship of a business-aligned cybersecurity program. A cybersecurity program that is designed with security, vigilance, and resilience in mind, guided by a clear strategy and supported by strong governance measures will be well placed to meet the regulatory requirements.

The Code highlights the importance of the Governing Body in overseeing cybersecurity and cyber–resilience and also carrying out periodic reviews of the effectiveness of the cybersecurity framework and cyber–resilience.

Key Requirements



Key Requirements– GOVERNANCE

Board Level Governance of Cyber Risk
Board level oversight of cyber risks and overall accountability of the cybersecurity framework

Cyber Risk Management
Establishing a process for the identification, evaluation and management of cyber risks

CISO Appointment
Appointment of a Chief Information Security Officer responsible for overseeing the cybersecurity framework

Outsourcing and Third Party Risk Management
Oversight and clear accountability for all outsourced functions with an understanding of the risks associated with IT outsourcing

Three Lines of Defense
A Cyber risk governance model based on the 3LOD: operational management, risk management and internal audit

IT Audit Plan
Independent and objective assessment of the effectiveness of cyber security controls to be performed by the third line of defense

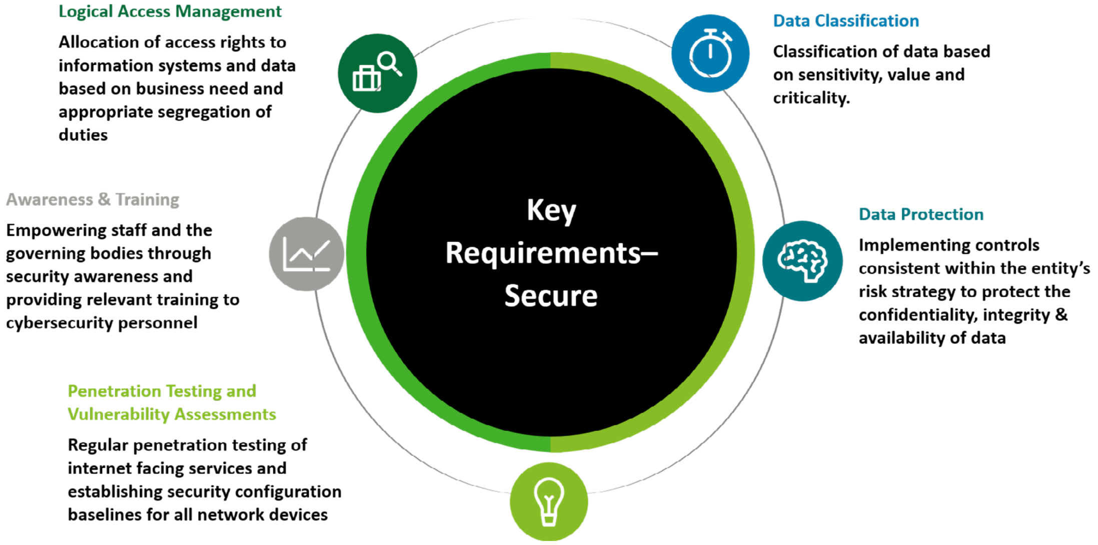
Secure

Regulated entities are required to establish and implement effective mechanisms around information assets, systems, and data and balance the need to reduce cyber risk while enabling productivity, business growth, and cost optimisation objectives.

Regulated entities must demonstrate that data protection is part of their strategy and cybersecurity framework, and will soon also need to take into consideration the provisions of the Bermuda Personal Information Protection Act and the guidance issued by the Office of the Privacy Commissioner.

A comprehensive cybersecurity training and awareness program must be established and endorsed by the governing body and/or senior management.

Key Requirements



Key Requirements– Secure

Logical Access Management

Allocation of access rights to information systems and data based on business need and appropriate segregation of duties

Data Classification

Classification of data based on sensitivity, value and criticality.

Awareness & Training

Empowering staff and the governing bodies through security awareness and providing relevant training to cybersecurity personnel

Data Protection

Implementing controls consistent within the entity's risk strategy to protect the confidentiality, integrity & availability of data

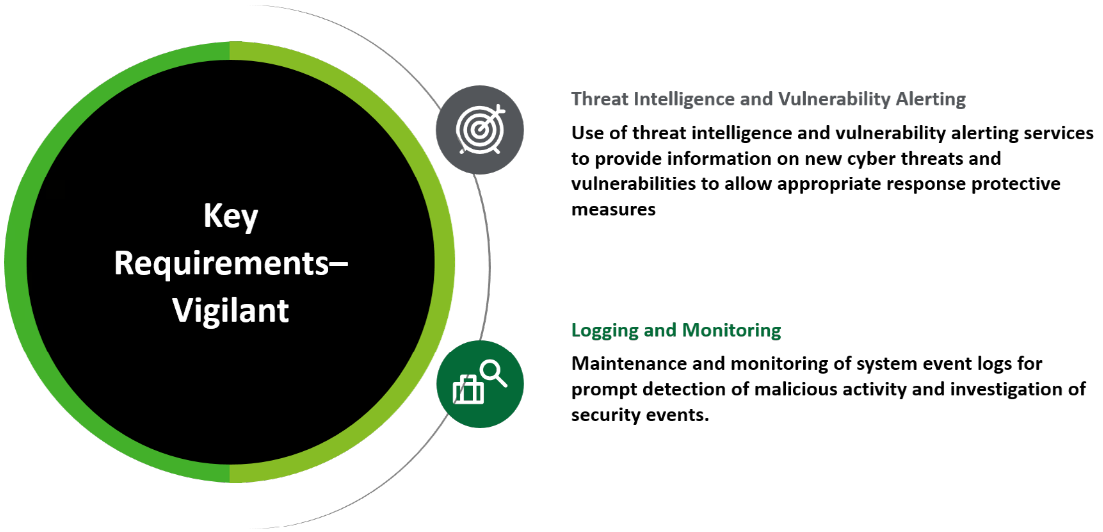
Penetration Testing and Vulnerability Assessments

Regular penetration testing of internet facing services and establishing security configuration baselines for all network devices

Vigilant

Regulated entities will need to develop and implement mechanisms and systems to proactively detect and manage cyber threats and respond more effectively to cyber incidents such as Denial of Service (DoS) attacks, Data Leakages, Insider Attacks, etc. from internal and external forces.

Regulated entities must implement monitoring/surveillance and detection techniques and systems that allow real-time monitoring and detection of threats (e.g., Firewalls, Web Application Firewalls (WAFs), Network Behaviour Analysis, etc.).



Key Requirements– Vigilant

Threat Intelligence and Vulnerability Alerting

Use of threat intelligence and vulnerability alerting services to provide information on new cyber threats and vulnerabilities to allow appropriate response protective measures

Logging and Monitoring

Maintenance and monitoring of system event logs for prompt detection of malicious activity and investigation of security events.

Resilient

Cyber threats are continually evolving and increasing in volume, intensity, and complexity. It has become more likely that an attack can penetrate an entity's defenses and controls. When this happens, regulated entities must respond fast, thoroughly, and decisively.

Regulated entities must notify the BMA of a cyber event resulting in signficant adverse impact to the regulated entity's operations, their policyholders or clients no later than 72 hours following the determination or confirmation of an event.

Key Requirements

Key Requirements– Resilient

IT Security Incident Management

Development of an appropriate IT incident management process with the objective of restoring normal IT services following a cyber event with minimal impact to business operations

Business Continuity and Disaster Recovery Planning

Annual testing of the business continuity and disaster recovery plans that are based on a documented business impact analysis.

We are here to help!

Every entity is at a different place when it comes to the maturity of its cybersecurity risk management program. Besides, the nature and magnitude of cyber risks are continuously evolving, and so are the practices for staying ahead of these threats. That's why it's essential to understand where you stand today by proactively performing a compliance readiness assessment and addressing the gaps.

Brett Henshilwood
Partner, Risk Advisory
brett.henshilwood@deloitte.com
+1 441 534 1395

Thelma Gombedza
Manager, Risk Advisory
thelma.gombedza@deloitte.com
+ 1 441 299 1880

BMA Sources:

BMA Insurance Sector Operational Cyber Risk Management | Code of Conduct

www.deloitte.com/bm/cyberrisk

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Ltd. is an affiliate of DCB Holding Ltd., a member firm of Deloitte Touche Tohmatsu Limited.Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the "Deloitte organization") serves four out of five Fortune Global 500 ® companies. Learn how Deloitte's approximately 330,000 people make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms or their related entities(collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.