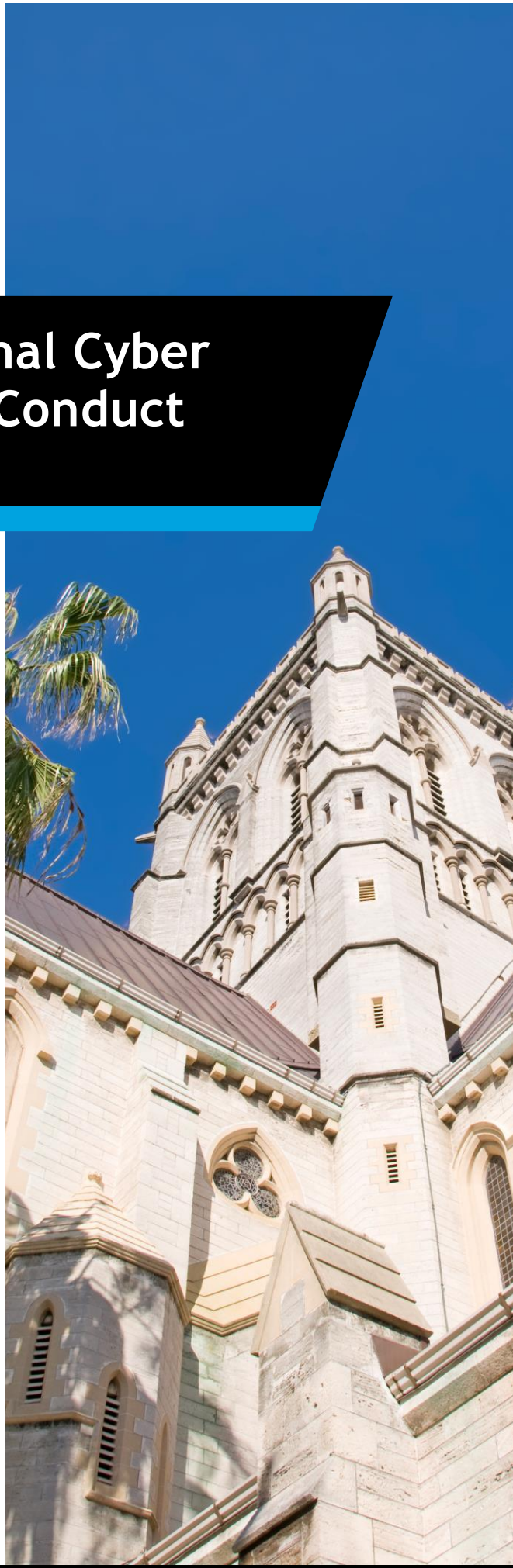
Insurance Sector Operational Cyber Risk Management Code of Conduct

October 2020



The Bermuda Monetary Authority (BMA) issued on 6 October 2020 the Insurance Sector Operational Cyber Risk Management Code of Conduct (Code) in its final form, together with the BMA's responses to the comments provided by the industry on a draft of the Code submitted for consultation in late 2019. The Code will come into force on 1 January 2021 to apply to all Bermuda registered Insurers, Insurance Managers, and Intermediaries (i.e. Agents, Brokers, Insurance Market Place Providers) (collectively referred herein as Regulated Entities). Regulated Entities have until 31 December 2021 to be in compliance with the Code.

The Code establishes duties, requirements, standards, procedures and principles to comply with in relation to operational cyber risk management. It complements the systems and operations risk component set forth in the Insurance Code of Conduct and the codes of conduct issued by the BMA applicable to Insurance Managers and Intermediaries (i.e. Insurance Manager Code of Conduct, Insurance Brokers and Insurance Agents Code of Conduct and Insurance Marketplace Provider Code of Conduct), by requiring Regulated Entities to manage and appropriately mitigate IT systems and operations risk by establishing a system of effective internal reporting and operational controls of their IT infrastructure.

Kennedys

BMA assessment based on proportionality principle

Failure to comply with the Code will be a factor taken into account by the BMA in determining whether Regulated Entities are meeting their obligation to conduct their business in a sound and prudent manner. The BMA will base its assessment of the technology risk programmes in place and the existence of sound and prudent business conduct on a proportionate basis having regard to the risk profile arising from the nature, scale, complexity of the business carry on by each Regulated Entity.

Cyber Risk Governance

The Code provides that the governance of cyber risk is under the responsibility and oversight of the board of directors of the Regulated Entity (Board). The Board is required to approve a cyber risk policy document at least annually. The oversight of cyber risk by the Board and the senior management (Cyber Risk Governance) must be documented and subject to regular updates. The Cyber Risk Governance should use the "three lines of defence" model that provides a simple and effective way to improve communications on risk management and control by clarifying essential roles and duties in organisations. Pursuant to the three lines of defence model, organizations' overall risk and control structure shall be organised among three lines involved in the effective risk management of Regulated Entities:

- **Operational management function** provided by the executive management of the Regulated Entity which has ownership, responsibility and accountability for assessing, controlling and mitigating risks.
- **Risk management function** held by the chief information security officer (CISO) (as more detailed below).
- **Internal audit function** that provides independent assurance carried out by the audit committee of the Board (or equivalent) delivering an independent and objective assessment of the effectiveness of the IT risk management and control.

The Board must appoint a senior executive as CISO, whose role is to oversee and implement the operational cyber risk management programme (Programme). The CISO function may be outsourced under the oversight of the Board as if this function was performed internally and subject to the Regulated Entity's own standards on governance and internal controls.

The Programme must comprise the following three functions:

- Process to identify, evaluate and manage cyber risks, including:
  - Risk identification consisting in Regulated Entities' assets inventory, third party service provider risks, use of cloud computing, strength of security safeguards, and evaluation of any existing or potential threats to security.
  - Risk measurement including determination of assess value/sensitivity, impact on policyholders, significance to operational viability.
- Controls relating to information security and data classification including limitation of the access to system and data to employees or third parties with demonstrated business need, safeguarding data proportional to their sensitivity, value and criticality.
- Controls relating to risk detection, and response and recovery, including implementation of business continuity management which must identify the critical business processes and system, events that can cause interruptions of the business and develop a business continuity plan to maintain or restore operations which shall be tested annually.

IT management controls

Regulated Entities are required under the Code to implement an IT service management framework (IT Framework) to assist in the management of stable and secure IT systems, services and operations/ detection and protection of data/systems, covering:

- Configuration management
- Change management
- Software release management
- Incident and problem management
- Performance and capacity management
- Data classification and security
- Specific mobile computing controls
- Protection against malicious code
- Encryption of non-public information
- Data backup management
- Patch management

- Data deletion/sanitisation Policy
- Network security management
- Risk analysis of the threat and impact form a distributed Denial of Service Defense
- Secure application development
- Use of cryptography
- Crisis management.

As part of the IT Framework, Regulated Entities must perform internal assessments of (i) their risk and determine a suitable security testing programme, (ii) their compliance with data protection law and regulations applicable to each jurisdiction of operation (such as the Bermuda Personal Information Protection Act 2016 and the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (i.e. GDPR)) and (iii) their compliance with the applicable data loss prevention requirements. The staff of Regulated Entities must receive annual training proportionate to their responsibility in the cyber risk and security management process and the sensitivity of the data they have access to.

IT security incident

Regulated Entities are required to develop and implement a formal IT security incident reporting procedure including an incident response, internal escalation procedure and external communication plan which will be triggered when an IT incident occurs leading to an unexpected disruption to the standard delivery of IT services.

Regulated Entities through their principal representative or appropriate officer must report material cyber risk events to the BMA within 72 hours of becoming aware that such events have occurred or may potentially occur. Material cyber risk events are IT security incidents:

- Having a significant adverse impact on policyholders or clients, or a significant loss of system availability;
- Where integrity of the information system or data is severely compromised;
- Causing a breach of confidentiality of the information system; or
- For which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body.

Business continuity and recovery controls

Policies and procedures must be in place and tested at least annually to implement effective and coordinated business continuity planning and disaster recovery planning.

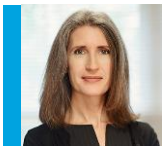
Further information

To find out more about our services and expertise, and key contacts, go to: kennedyslaw.com

Key contacts

Nick Miles
Partner
t + 1 441 278 7164
nick.miles@kennedyslaw.com

Nicolas Champ
Senior Associate
t + 1 441 278 7162
nicolas.champ@kennedyslaw.com



Ciara Brady
Senior Associate
t + 1 441 278 7169
ciara.brady@kennedyslaw.com

Mark Chudleigh
Partner
t + 1 441 278 7160
mark.chudleigh@kennedyslaw.com