Insurance Sector Operational Cyber Risk Management Code of Conduct

On October 6, 2020, the Bermuda Monetary Authority (the BMA or the Authority) released it's Insurance Sector Operational Cyber Risk Management Code of Conduct (the Code). The Code comes into force on January 1, 2021, and registrants are required to comply by December 31 2021.

The Code includes a series of minimum (i.e., mandatory) and recommended standards, structured across the following pillars of a cybersecurity program:

- **Identification of assets and risks (including governance and risk assessment);**
- **Detect and protect controls; and**
- **Response and recovery controls.**

We recommend that organisations initiate, in short order, a formal process to evaluate their current cyber risk programs' conformance with the requirements of the Code. In executing this evaluation we recommend (as with the development of a cybersecurity program) that organisations take a holistic (as opposed to siloed) approach, affording entities the agility needed to align and adjust their cyber-programs to other new regulations (such as PIPA/GDPR) and the continued evolution of cyber threats. For those entities with less mature cybersecurity programs we also recommend that the Code be reviewed alongside consideration of recognised frameworks (such frameworks include: NIST Cybersecurity Framework, Cobit, and ISO 27001).

pwc

Proportionality Principle:

As with other regulatory areas, the BMA will assess a registrant's cyber risk management program and its compliance with the Code in a manner proportionate to the registrant's cyber risk profile (including consideration of the nature, scale and complexity of its business). As such, as organizations must evaluate their current programs against the requirements of the Code, we recommend that this assessment start with ensuring that the organization's cyber risk assessment is sufficiently robust and appropriately documented. Such an assessment will also support an organization's need to clearly detail operational cyber risk in the Commercial Insurer / Group Self Solvency Assessment (CISSA/GSSA).

Overview of the Standards:

The following provides a high level overview of the standards detailed within the Code:

Identification of assets and risks

- **Governance** –standards pertaining to Board oversight, appointment of the role of chief information security officer, program structure, staff vetting, managing outsourcing / third party providers, and cyber insurance.
- **Risk Assessment** –standards pertaining to the assessment process, identification of assets, cloud computing, business continuity management, system development, and end user-developed systems.
- **Audit & Monitoring** –standards pertaining to conducting independent and objective IT audits, security review of New Projects and IT system, and the ongoing monitoring and evaluation of controls.

Detect and protect controls

- **Threat and Vulnerability Intelligence** –standards pertaining to penetration and vulnerability assessments and alerting services.
- **IT and Security Incident Management** –standards pertaining to roles, responsibilities, response / escalation procedures and exercises, and management of internal and external stakeholders.
- **Data** –standards pertaining to the assessment and classification of data, data loss prevention and protection requirements, securing non-public information, use of cryptography, and data back up.
- **Specific control requirements** –standards pertaining to network security management, security and logical access management, malicious code detection, mobile computing, user awareness and training, patch management, cryptography, DDOS defense, and logging and monitoring.
- **BMA Notification** –requirement to notify the BMA within 72 hours from the time that there is a determination or confirmation of a cyber event.

Response and recovery controls

- **Business continuity and disaster recovery planning** – standards pertaining to the development, implementation, communication and testing of such plans.

Focus Areas & Challenges

While the BMA, based on their 2018 review, recognized a general improvement in the sector's resilience to cyberattacks, they also noted the following areas requiring further improvement:

- Board approval of Operational Cyber Risk Strategy/Policy;
- Third-Party Operational Cyber Risk Management Assessment;
- Data Classification and Data Loss Prevention (DLP) controls;
- Testing of Business Continuity Planning (BCP) and Disaster Recovery (DR);
- Scenario rehearsal "table top testing" of the Security Incident Response Plan; and
- Monitoring of anomalous network activity.

Smaller and/or less mature entities face further challenges primarily due to constraints of appropriately skilled resources impacting the level of time that can be dedicated to managing cybersecurity risks. However, it is for this same reason that smaller companies often suffer increased consequences of, and find it more difficult to recover from, cybersecurity incidents.

How can PwC help

PwC's cybersecurity and privacy practice can help you assess, build and manage your cybersecurity capabilities while enabling effective incident response to a myriad of potential threats.

Our local cybersecurity and privacy practice consists of professionals with significant business and technical experience who can help you address your cybersecurity and privacy risks, ranging from supporting your risk assessment process, developing and assessing policies and procedures including the response and recovery process, designing, implementing and assessing controls, and conducting efficient and effective independent IT audits.

We also leverage the power of our global network of member firms to provide organisations with deeper, broader and timely expertise on evolving cybersecurity and privacy challenges.

Contact us

Matt Britten
Partner
+1 441 299 7265
matthew.britten@pwc.com

Chris Mills
Director
+1 441 299 7162
christopher.mills@pwc.com

Tapiwa Maringazuva
Senior Manager
+1 441 299 7284
tapiwa.maringazuva@pwc.com