# BERMUDA MONETARY AUTHORITY

## Insurance Sector Operational Cyber Risk Management

## Code of Conduct

## October 2020

# Table of Contents

# 1 Legislative Basis and Scope of Code

This document outlines the Bermuda Monetary Authority's (Authority or BMA) Insurance Sector Operational Cyber Risk Management Code of Conduct (the Code). This Code applies to all Bermuda registered Insurers, Insurance Managers, and Intermediaries (Agents, Brokers and Insurance Market Place Providers), collectively referred to as "registrants".

The Authority is issuing the Code pursuant to the powers under Section 2BA of the Act. The Code establishes duties, requirements, standards, procedures, and principles to be complied with in relation to operational cyber risk management. The Code should be read in conjunction with:

- Paragraph 5.1.5, item 37 of the Insurance Code of Conduct (2015)
- Paragraph 14 of the Insurance Manager Code of Conduct (2016)
- Paragraphs 13, 14, 29, 45 of the Insurance Brokers and Insurance Agents Code of Conduct (2020)

It must be noted that the Authority is not adopting a "one-size-fits-all" approach and expects cyber risk controls will be proportional to the nature, scale and complexity of the organisation. It is acknowledged some entities will use a third party to provide technology services and they may outsource their IT resources (for example, to an insurance manager). The Authority expects for the registrant to include a review of any services provided by third parties services as part of their overall assessment of cyber risk.

# 2 Introduction

Cyber incidents can cause significant financial losses and/or reputational impact to registrants as well as their clients. The confidentiality, integrity and availability of information, in all its forms, is critical to the daily operations of registrants.

The Code is designed to promote the stable and secure management of information technology systems of regulated entities. It is deliberately not exhaustive. Registrants must implement their own technology risk programmes, and determine what their top risks are and decide the appropriate risk response. Registrants must be able to evidence there is adequate board visibility and governance of cyber risk.

Failure to comply with provisions set out in the Code will be a factor taken into account by the Authority in determining whether a registrant is meeting its obligation to conduct its business in a sound and prudent manner.

# 3 Interpretation

Registrants should have regard to the following in interpreting the Code and how the Authority is likely to interpret compliance:

- "Shall" or "must" denotes that the standard is mandatory; the registrant must implement either what is prescribed in the Code, or a comparable or higher standard that Registrants can demonstrate yields similar protection levels (concerning its business model)
- "Should," while not mandatory, denotes a strong recommendation from the Authority; a registrant may depart from it where it has documented a valid reason
- "May" denotes options

- "Best practice" includes recognised standards such as those adopted by the National Institute of Standards and Technology (NIST) or the International Organisation for Standardization (ISO)

Note that the terms Cyber and Information Technology (IT) are considered interchangeable throughout this document.

# 4 Proportionality Principle

The Authority appreciates that registrants have varying risk profiles arising from the nature, scale and complexity of the business. In addition, registrants with higher risk profiles require more comprehensive governance and risk management frameworks to conduct business in a sound and prudent manner.

Accordingly, the Authority will assess the registrant's compliance with the Code in a proportionate manner relative to its nature, scale and complexity. These elements will be considered collectively, rather than individually (e.g., a registrant could be relatively small in scale but manage an extremely complex business; therefore, it would still be required to maintain a sophisticated risk management framework). In defining these elements:

- **Nature:** Includes the relationship between policyholders, clients and the registrant or characteristics of the services provided
- **Scale:** Includes size aspects, such as the volume of the business conducted or the size of the balance sheet in conjunction with materiality considerations (e.g., an assessment of the impact of a registrant's failure)
- **Complexity:** Includes items such as business processes, organisational structures and product design

In assessing the existence of sound and prudent business conduct, the Authority will have regard for both its prudential objectives and the appropriateness of each requirement specified in the Code, taking into account nature, scale and complexity. The proportionality principle, discussed above, is applicable to all sections of the Code, regardless of whether the principle is explicitly mentioned.

Limited purpose insurers, in particular, should be mindful of the proportionality principle in establishing a sound corporate governance, risk management and internal controls framework, and complying with provisions of the Code, and should be guided as discussed in this section in documenting their compliance with the Code.

Limited purpose insurers, should also ensure that they focus on the cyber risk of the insurer. Where systems are operated by fronting insurers or a parent company/organisation (who are data/system controllers), then these fronting insurers/parent companies may not be subject to the Code. To be clear, if the fronting insurer or the parent company is a registrant in Bermuda, then they must also comply with the Code. Limited purpose insurers may have a reliance on their insurance manager who may provide services which are subject to cyber risk. In these circumstances, the limited purpose insurer can rely on the insurance manager to confirm that the services provided are compliant with the Code.

# 5 SECTION I - IDENTIFICATION OF ASSETS AND RISKS

## 5.1 Board Level Governance of Cyber Risk

The board of directors and senior management team must have oversight of cyber risks. The board of directors must approve a cyber risk policy document at least on an annual basis. The cyber risk may be covered in a standalone cyber risk policy document or expressly set forth as a section in a broader risk policy document, e.g., the operational risk policy. Regular updates detailing the overall cyber risk status must be made available to the board and senior management team.

## 5.2 The Role of the Chief Information Security Officer (CISO)

The role of CISO must be allocated to the appropriately qualified member of staff or the outsourced resource. It should be noted, however, that if the role is outsourced, oversight responsibility remains with the Board.

The role of the CISO is to deliver the operational cyber risk management programme. The CISO role is expected to be of sufficient seniority to facilitate the delivery of the operational cyber risk management programme.

## 5.3 The Operational Cyber Risk Management Programme

The objectives of the cyber risk policy must be delivered by an operational cyber risk management programme. This must include:

- A risk assessment process to identify, evaluate, and manage cyber risks
- Data governance, classification controls and information security controls
- Detection, protection, response and recovery controls

The programme defines, documents and communicates policies, processes and procedures that direct the management of cyber risk.

## 5.4 The Three Lines of Defense (3LOD)

The Authority requires that cyber risk governance should follow a 3LOD model, namely: operational management, risk management and audit.

## 5.5 Risk Assessment Process:

The operational cyber risk management programme must include a risk assessment process which comprises of:

- Identification: the organisation understands the cyber risk to operations, assets and individuals
- Measurement: the organisation understands the potential impact and consequences of these risks
- Response: for each type of risk identified, a risk response must be decided; the risk response should be consistent with the criticality of the asset; and the level of risk tolerance
- Monitoring and reporting: a risk register should be maintained to monitor risks

The registrant's risk assessments must be documented and retained for at least five years in a manner that allows the reports to be provided to the Authority upon request.

## 5.6 IT Audit Plan

The third line of defence, IT audit, should provide the audit committee of the Board (or equivalent) an independent and objective assessment of the effectiveness of controls. An IT audit plan should be developed and approved by the audit committee of the board or its equivalent. Audits may be carried out by a qualified internal audit resource or by a qualified third-party company.

## 5.7 The Re-evaluation of Controls

The control environment should be continuously monitored and evaluated in order to:

- Identify control deficiencies and to initiate improvement actions
- Plan, organise and maintain standards for internal control assessment and assurance activities
- Evaluate whether the control environment is compliant with laws, regulations and contractual requirements

## 5.8 Cyber Insurance

One of the risk responses available is to transfer the risk to a third party. Registrants should consider the benefits of purchasing a cyber insurance policy which may be used to mitigate financial loss from a cyber incident. Registrants should review the adequacy of its cyber insurance coverage at least on an annual basis.

## 5.9 Identify Assets

An asset inventory should be put in place, detailing all information assets. The information must be classified in terms of its value, legal requirements, sensitivity and criticality to the organisation.

- All information assets should be owned by a designated part of the business
- Information owners are responsible for classifying information and information assets
- Classifications and associated protective controls for information should take account of business needs for sharing or restricting information and the business impacts associated with such needs
- An appropriate set of procedures for information labelling and handling should be developed and implemented

## 5.10 Managing Outsourcing and Third-Party Service Provider Cyber Risk

Where the registrant outsources functions either externally to third parties or internally to other affiliated entities, the registrant must ensure there is the oversight and clear accountability for all outsourced functions as if these functions were performed internally, and subject to the registrant’s own standards of governance and internal controls.

The registrant must also ensure the service agreement includes terms on compliance with jurisdictional laws and regulations, cooperation with the Authority, and access to data and records in a timely manner. The senior management team must understand the risks associated with IT outsourcing. It is important to note an organisation can never outsource responsibility for governance and risk.

Contractual terms and conditions must be defined, governing the roles, relationships, obligations and responsibilities of all contracting parties.

## 5.11 Cloud Computing

The use of cloud computing services must be risk-assessed. The risk profile of cloud computing must be assessed according to the type of cloud architecture, i.e. public cloud, private cloud, community cloud and hybrid cloud. A cloud risk assessment must include an analysis of security architecture and operations, as well as the following topics:

- **Governance and Enterprise Risk Management (ERM):** The ability of an organisation to govern and measure enterprise risk introduced by cloud computing, the ability to adequately assess the risk of a cloud provider, and the definition of roles and responsibilities
- **Legal issues:** Potential legal issues include protection requirements for information and computer systems, security breach disclosure laws, regulatory requirements, privacy requirements and international laws or regulations
- **Compliance and audit:** Maintaining and proving compliance when using cloud computing; evaluating how cloud computing affects compliance with internal security policies, as well as compliance requirements (regulatory, legislative and other)
- **Information governance:** Governing data that is placed in the cloud, i.e. the identification and control of data in the cloud, compensating controls that can be used to deal with the loss of physical control when moving data to the cloud

As part of the cloud risk assessment, a review of roles and responsibilities must be completed to define which party is responsible for operating and monitoring each cyber risk control.

### 5.12 End User Developed Systems (End User Computing)

The risk from any end user-developed systems should be assessed given that end users may develop systems that do not follow formal IT standards. This may increase the risk of security incidents relating to data security or availability outages.

### 5.13 Staff Vetting Process

The screening of staff is an important control used to minimise personnel risks. Registrants must implement a staff vetting process.

### 5.14 The Security Review of New Projects and IT Systems

New projects that involve data or systems classified as critical, must be subject to a technology risk assessment to identify and respond to any potential new risks introduced. Minor changes should be security reviewed as part of the standard change process.

# 6 SECTION II – DETECT AND PROTECT CONTROLS

### 6.1 IT Service Management

IT service management processes should be in place to assist in the management of stable and secure IT systems, services and operations and should include:

- Configuration management
- Change management
- Software release management
- Incident and problem management
- Performance and capacity management

### 6.2 Threat Intelligence and Vulnerability Alerting

Registrants should consider using threat intelligence and vulnerability alerting service to provide information about new cyber threats and vulnerabilities. This information can then be used to assist with threat response protective measures.

### 6.3 IT Incident Management

An IT incident occurs when there is an unexpected disruption to the standard delivery of IT services. An incident management process must be in place with the objective of restoring normal IT service following the incident and with minimal impact to business operations.

### 6.4 IT Security Incident Management

A formal IT security incident response process must be established. Consideration should be given to creating a Computer Security Incident Response Team (CSIRT). All employees, contractors and third-party users must be made aware of the procedure for reporting incidents.

A post-incident review should take place, this review should establish the root cause of the incident and conclude any remedial action required.

The IT incident management procedure should also define when a major incident becomes a crisis. Roles and responsibilities should be defined. Management of communications to internal and external stakeholders should also be clearly defined.

Scenario-based or "tabletop" response exercises should be held to prepare for any real incidents that may occur and test the processes in place. Registrants should consider contracting with an external organisation who specialise in security incident investigation and response so that their services are available in the event of a major security incident.

### 6.5 Notification of Cyber Reporting Events to the Authority

A cyber reporting event is defined as: "Any act that results in unauthorised access to, disruption or misuse of the electronic systems or information stored on such systems of a licensed undertaking, including any breach of security leading to the loss or unlawful destruction or unauthorised disclosure of or access to such systems or information", where -

(a) a cyber reporting event has the likelihood of adversely impacting policyholders or clients;

(b) an insurer has reached a view that there is a likelihood that loss of its system availability will have an adverse impact on its insurance business;

(c) an insurer has reached a view that there is a likelihood that the integrity of its information or data has been compromised and may have an adverse impact on its insurance business;

(d) an insurer has become aware that there is a likelihood that there has been unauthorised access to its information systems whereby such would have an adverse impact on its insurance business; or

(e) an event has occurred for which a notice is required to be provided to a regulatory body or government agency.

Only cyber reporting events resulting in significant adverse impact to the regulated entity's operations, their policyholders or clients, must be reported to the Authority.

When in doubt about whether an event is reportable, registrants should consult with the Authority for guidance. A Principal Representative (for insurers) and appropriate officer (for insurance managers and intermediaries) must notify the Authority within 72 hours from the time that there is either a determination or a confirmation of an event (whichever is sooner).

Following the initial notification, registrants are expected to keep the Authority regularly updated on progress throughout the remediation of the incident. An incident report containing details of the incident, the root-cause, actions taken to minimise impact and any actual adverse impact to the organisation must be prepared. This must be submitted within 14 days of the initial incident notification date. If root cause has not been confirmed then the report must still be submitted detailing information known to date. The Authority may then request further updates but this will be determined on a case by case basis.

Registrants are expected to maintain logs of all cybersecurity incidents together with details of actions taken to resolve them. Incident investigation and response logs (note this does not include actual system event logs) must be available for inspection upon the Authority's request at any time and kept for a minimum of five years.

### 6.6 Logical Access Management

Procedures must be in place to manage the allocation of access rights to information systems and services. Employees, third parties and customers using IT systems must be authorised to do so through an approved process to ensure the access and level of privilege is appropriate to their role.

Roles and areas of responsibility should be segregated as much as possible to minimise opportunities for misuse, abuse of privileges and unauthorised or unintentional modification. Access to systems and data should only be granted to individuals confirmed as having a requirement. An audit log of all logical access changes should be maintained.

### 6.7 Awareness and Training

Staff cyber risk awareness training must be completed at least annually. Staff responsible for cyber risk and cybersecurity should also have the relevant skills and training to carry out their role.

### 6.8 Data Classification and Security

Information should be classified and protected in a manner commensurate with its sensitivity, value and criticality. If personal or otherwise sensitive information is used for testing purposes, all sensitive details and content should be removed or anonymised.

### 6.9 Data Loss Prevention (DLP)

Registrants must perform an assessment of their Data Loss Prevention (DLP) control requirements. Typically, this assessment would reference the level of data classification, potential unauthorised data egress points and appropriate mitigating controls.

### 6.10 Data Protection and Governance

Registrants must perform an assessment of their compliance against applicable data protection requirements. Where Personally Identifiable Information (PII) is processed, this must be in accordance with data protection/privacy laws relevant to each jurisdiction of operation.

Data governance controls should be documented to define how data assets are formally managed throughout the enterprise. These should include: data quality, handling, security and retention. Storage limitation should also be defined, along with setting limits as to how long data is to be stored i.e. to prevent unnecessary storage.

### 6.11 Mobile Computing

Mobile computing services to include Bring Your Own Device (BYOD) services, must be subject to a risk assessment and then secured with appropriate controls.

### 6.12 Protection against Malicious Code

Controls to detect and block malicious code (or suitable mitigating controls) must be deployed at both the endpoint (i.e. desktop and mobile devices), as well as the network level. Malicious code includes computer viruses, ransomware, spyware, network worms, Trojan horses and backdoors.

### 6.13 Securing Nonpublic Data

Data classified as nonpublic must be protected by an appropriate level of security. The Authority requires that nonpublic data (including Personally Identifiable Information - PII), is protected by encryption at rest and when transmitted over public networks. Where encryption is not feasible, mitigating controls may be used, by exception.

### 6.14 Data Backup Management

Registrants should define a data backup strategy which references the classification level of data. Registrants should carry out periodic testing to ensure that backups can be restored.

### 6.15 Penetration Testing and Vulnerability Assessments

Registrants must assess their risk and determine a suitable security testing programme. The following should be considered as a minimum baseline:

- Regular penetration testing of internet-facing services by an independent and qualified testing company
- A security assessment for any new internet-facing services, or changes to existing services to determine if they need to be penetration tested before they go live
- Internal vulnerability scanning
- External vulnerability scanning
- Baseline standards to document secure configuration baselines of all network devices

### 6.16 Patch Management

Registrants must have patch management procedures that define the identification, categorisation and prioritisation of security patches. Registrants must pay close attention to a vendor’s end of support date as patches may no longer be available after this date.

### 6.17 Data Deletion/Sanitisation Policy

Data deletion and sanitisation of all media types that are used by the business should be documented and communicated to the appropriate staff.

### 6.18 Network Security Management

Network segregation must be used effectively to create zones of enhanced security within a network. Any service accessing the internet must first be routed through a Demilitarised Zone (DMZ). This is a physical or logical subnetwork that separates an organisation's external-facing services to an untrusted network.

Network security tools should be used to detect network intrusions and to provide alerts when an intrusion occurs. Examples of a network intrusion detection tool include a network Intrusion Detection System/Intrusion Protection System (IDS/IPS).

### 6.19 Distributed Denial of Service Defense (DDOS Defense)

Registrants should ensure they have conducted a risk assessment of DDOS attacks and then deploy the appropriate defences. The review should assess the following:

- Inherent risk from a DDOS attack to business services
- Detection controls: how quickly an attack could be detected
- Mitigation controls: how effectively traffic can be dropped/cleaned

### 6.20 Secure Application Development

Where application development takes place, a Secure Development Lifecycle (SDLC) should document secure development practices, examples include:

- The testing of application modules using source code review, exception testing and compliance review to identify insecure coding practices and system vulnerabilities
- The use of separate environments for unit, integration and user acceptance testing
- The separation of development and testing environments from the production environment

### 6.21 Logging and Monitoring

Registrants must complete an assessment of their logging and monitoring requirements. The following controls should be considered as part of this review:

- System event logs must be retained and stored in accordance with business and regulatory requirements, taking into account system criticality
- Where logs contain personal data, they must be treated in accordance with the relevant privacy law requirements
- All security logs must be protected from unauthorised access, disclosure, modification or destruction
- Anomalous activity must be detected and investigated in order to understand the potential risk to the network
- Security events must be monitored to facilitate the prompt detection of malicious activity
- Data that allows for the complete and accurate reconstruction of all financial transactions and accounting must be maintained

### 6.22 Use of Cryptography

Registrants should evaluate cryptographic implementations, and ensure that only cryptographic modules based on authoritative standards, and reputable protocols are installed. The strength of cryptography depends not only on the algorithm and key size but also on implementation. Testing should be conducted before any cryptographic services go into production to identify any security issues.

# 7 SECTION III – RESPONSE AND RECOVERY CONTROLS

### 7.1 Business Continuity and Disaster Recovery Planning

Registrants must implement effective Business Continuity Planning (BCP) and Disaster Recovery (DR) policies and procedures to include:

- Regular documented business impact analysis exercises to determine the criticality of business process, recovery criticality and the likely impact resulting from different disaster scenarios
- BCP and DR plans must be tested at least annually. These tests must be documented and any issues identified and tracked for remediation

# 8 Implementation

The Code comes into force on 1 January 2021 and registrants are required to be in compliance by 31 December 2021.

# 9 Definitions:

- **Business Continuity Planning (BCP)**
  The process of creating systems of prevention and recovery to deal with potential threats to a registrant.
- **Bring Your Own Device (BYOD)**
  Bring your own device refers to employees using their personal devices to connect to their organisational networks and access work-related systems.
- **Chief Information Security Officer (CISO)**
  This means the senior executive, by whatever title called, appointed by the registrant to oversee and implement its Cyber Risk Programme and enforce its cyber risk policies.
- **Computer Security Incident Response Team (CSIRT)**
  A Computer Security Incident Response Team is an organisation that investigates, manages and responds to computer security incidents.
- **Distributed Denial Of Service (DDOS)**
  DDOS is a type of Denial of Service (DOS) attack where multiple compromised systems are used to attack a target.
- **Data Loss Prevention (DLP)**
  DLP is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network.
- **Demilitarised Zone (DMZ)**
  A DMZ or demilitarised zone (sometimes referred to as a perimeter network or screened subnet) is a physical or logical subnetwork that contains and exposes an organisation's external-facing services to an untrusted network, usually a larger network such as the Internet.
- **Information Asset**
  An asset is any data, device or other component of the environment that supports information-related activities.
- **Mobile Devices**
  Refers to any portable device, i.e. a cellphone, smartphone, tablet or laptop device.
- **Personally Identifiable Information (PII)**
  PII is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymising anonymous data can be considered PII.
- **Secure Development Lifecycle (SDLC)**
  A document outlining secure application development practices