BERMUDA MONETARY AUTHORITY

Insurance Sector Operational Cyber Risk Management

Code of Conduct

December 2019

Contents

Consultation - Insurance Sector Operational Cyber Risk Management Code of Conduct

This document outlines the Bermuda Monetary Authority's (the Authority's) proposed Insurance Sector Operational Cyber Risk Management Code of Conduct (the Code).

The views of the insurance sector and other interested persons on the proposals set out in this document are invited.

Comments should be sent to policy@bma.bm no later than **31 January 2020**.

1 Legislative Basis and Scope of Code

This document outlines the Bermuda Monetary Authority's (the Authority) 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, 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 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 may outsource IT resources (for example, to an insurance manager). The Authority expects for the registrant to obtain confirmation from the service provider that they are in compliance with the requirements of the Code.

2 Introduction

Cyber risks can cause significant financial losses and/or reputational impact on 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 should 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 the Registrants can demonstrate yields similar protection levels (having regard for 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 would 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 carry out extremely complex business and, therefore, 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 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 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 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 annually. 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 Chief Information Security Officer (CISO) must be allocated to an appropriately qualified member of staff or outsourced resource. It should be noted, however, that if the role is outsourced, oversight responsibility remains with 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 delivery of the Operational Cyber Risk Management Programme.

5.3 The Operational Cyber Risk Management Programme

The Operational Cyber Risk Management Programme must include the three key functions below:

- A process to identify, evaluate and manage cyber risks
- Information security, data classification and data governance controls
- Detection, protection, response and recovery controls

Registrants shall define, communicate and document appropriate policies, processes and procedures that direct the overall organisational approach to securing systems and data that support delivery of essential business processes.

5.4 The Three Lines Of Defense (3LOD)

The Authority requires that cyber risk governance should utilise the 'Three Lines of Defense' (3LOD) in effective risk management and control – namely, operational management, risk management and internal audit. The best practice is that each line of defence is a separate role and resource but the rule of proportionality will be applied. Where multiple roles are completed by one resource, it is expected the associated work streams and tasks will be defined, actioned and reported under each of the 3LOD descriptions.

5.5 IT Audit Requirement

The third line of defence, IT audit, must provide the audit committee of the Board (or equivalent) an independent and objective assessment of the effectiveness of controls that are applied within the IT environment to manage risks. Independent audit can be carried out by a qualified internal audit function or a qualified third-party company.

A cyber risk audit plan must be developed and approved by the audit committee of the Board or equivalent. The audit frequency must be in line with the criticality and level of risk associated with the IT system or business process.

5.6 The Cyber Risk Process

Priorities, constraints, risk tolerances and assumptions should be established and used to support operational risk decisions. The risk appetite and tolerance level for each material risk area should also be established. The Operational Cyber Risk Management Programme should include the key risk processes listed below:

- **Risk Identification:**
  The organisation understands the cybersecurity risk to operations, assets and individuals
- **Risk Measurement:**
  The organisation understands the potential impact and consequences of these risks
- **Risk Response:**
  For each type of risk identified, a risk response must be decided; the risk response should be consistent with the criticality of the information system assets and the level of risk tolerance
- **Risk Monitoring and Reporting:**
  A risk register should be maintained to monitor risks; a monitoring process should enable continuous assessment and treatment of 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

5.7 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 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 in the event of a cyber incident. Registrants should review the adequacy of its cyber insurance coverage at least annually.

5.9 Identify Assets

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

- All information assets must 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 must 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 must 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 oversight and clear accountability for all outsourced functions, as if these functions were performed internally, and subject to the registrant's own standards on 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 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. Agreements should include service levels, availability, reliability, compliance, audit, security, contingency planning and disaster recovery.

The outsourcing agreement must also allow for regulators to have oversight of relevant outsourced functions. The registrant must request for outsourced service providers to implement security policies, procedures and controls that are at least as stringent as what is in place for its own operations.

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, 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:** 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
- **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 Business Continuity Management

A business continuity management process must be implemented to minimise the impact on the organisation and to recover from loss of service availability or information to an acceptable level. This process must identify the critical business processes and systems.

Events that can cause interruptions to business processes must be identified, along with the probability and impact of such interruptions, and any consequences for information security. Plans must be developed and tested to maintain or restore operations, and ensure the availability of systems and data as defined in the Business Continuity Plan (BCP).

Critical services should be listed against the business recovery requirements. This should include the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for each system. Registrants should review their BCP plans at least annually.

5.13 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 which do not follow formal IT standards. This can increase the risk of security incidents relating to data security or availability outages. Examples of end user applications include user developed spreadsheets and databases which are stored locally on user workstations.

5.14 Staff Vetting Process

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

5.15 The Security Review of New Projects and IT Systems

New projects and the implementation of new systems must be subject to a technology risk assessment to ensure that no new risks are introduced to the network by way of poor systems design, testing and implementation.

6 SECTION II – DETECT AND PROTECT CONTROLS

6.1 IT Service Management Controls

An IT Service Management framework should be in place to assist in the management of stable and secure IT systems, services and operations. IT Service Management should comprise the governance structure, processes and procedures for the following:

- 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 a threat intelligence service to provide information about cyber threats that have, will or are currently targeting the insurance sector or relevant geographic locations. This information can then be used to assist with threat response protective measures.

Registrants should consider using a vulnerability alerting service to inform the organisation of the latest vulnerabilities relevant to its systems.

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 as quickly as possible following the incident and with minimal impact to business operations. To facilitate this, a major incident team should be set up comprising of staff with the necessary technical and operational skills.

6.4 IT Security Incident Management

A formal IT security incident reporting procedure must be established, together with an incident response and escalation procedure. Consideration should be given to setting up 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 communication plan must be in place to manage communication to internal and external stakeholders, including regulatory authorities and third-party vendors. A post-incident review should be completed for incidents resulting in a high level of risk or impact. This review should establish the root cause of the incident and conclude any remedial action required to reduce the likelihood of the incident recurring.

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 also 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 Risk Reporting Events to the Authority

Material cyber risk reporting events must be reported to the Authority. As a guide, material cyber risk events are considered to be:

- any significant adverse impact to policyholders or clients (significant would be any breach of their data or any widespread outage of IT services)
- a significant loss of system availability (for example – an outage of a system identified as critical that has resulted in a significant impact to normal operations)
- integrity of the information system or data being severely compromised (for example - a system configuration or data file has been changed by a malicious attacker)
- a breach of confidentiality of the information system or in relation to any other data as a result (for example - a malicious code execution that has resulted in unauthorised access to a system or data)
- an event for which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body

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 manager and intermediaries) must notify the Authority of an event within 72 hours from the time there is either a suspicion or a

confirmation of a material event (whichever is sooner). This can be the CISO, CTO, COO or other appropriate senior officer.

Following initial notification, registrants are expected to provide an incident report containing details of root-cause and any impact to the organisation. This must be submitted within 14 days of the initial incident notification date. Registrants are expected to maintain logs of all cybersecurity incidents together with details of actions taken to resolve them. Incident logs must be available for inspection upon the Authority's request at any time.

6.6 Logical Access Management

Formal procedures must be in place to control 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 must be segregated to minimise opportunities for misuse, abuse of privileges and unauthorised or unintentional modification. Access to systems and data must only be granted to individuals with a demonstrated business need. Separation of duties must be enforced where possible. Controls must be in place to ensure identification, authorisation and authentication of the individual. An audit log of all access changes should be maintained.

6.7 Awareness and Training

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

6.8 Data Classification and Security

Information must be classified and protected in a manner commensurate with its sensitivity, value and criticality. Information must be used only for the business purposes expressly authorised by management.

Test data should not be used in a production system. If personal or otherwise sensitive information is used for testing purposes, all sensitive details and content should be removed or anonymised before use.

6.9 Data Loss Prevention (DLP)

Registrants must perform an assessment of their Data Loss Prevention (DLP) requirements. DLP controls should be considered at both the endpoint (i.e. desktop and mobile device) as well as the network layer (i.e. firewall, internet and email filter). DLP should also manage the use of internet data sharing services such as cloud-based internet storage sites and web-based email.

6.10 Data Protection

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. A data protection policy must be defined and implemented. The data protection policy should define data retention requirements. Storage limitation should also be defined, setting limits to how long data is to be stored (i.e. to prevent the unnecessary storage of PII).

6.11 Mobile Computing

Security controls must be implemented to protect Mobile Devices accessing group information or networks. Access to group information via personally owned devices, commonly known as Bring Your Own Device (BYOD), 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 – see definition in Appendix), as well as the network level. Malicious code includes computer viruses, ransomware, spyware, network worms, trojan horses and backdoors.

6.13 Encryption of Nonpublic Information

Data classified as nonpublic (it is expected that this includes Personally Identifiable Information (PII)) must be protected by an appropriate level of security. Encryption controls should be used to encrypt this data at rest and when transmitted over public networks.

6.14 Data Backup Management

Registrants should define a data backup strategy. This must reference the classification level of data. Registrants must carry out periodic testing to ensure that backups can be restored. The testing must also determine if the backups meet requirements defined by the BCP.

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; it should be noted that a risk assessment should be completed of any new internet-facing services, or changes to existing services to confirm if they need to be penetration tested before they go live
- Internal vulnerability scanning
- External vulnerability scanning
- Baseline standards should be in place to document secure configuration baselines of all network devices

6.16 Patch Management

Registrants must have patch management procedures which define the identification, categorisation and prioritisation of security patches. Registrants must pay close attention to a vendor's end of support date. It is common for vendors to cease the provision of system updates, including security updates, after the end of support date.

6.17 Data Deletion/Sanitisation Policy (DSP)

A policy must be in place covering data sanitisation requirements, procedures and validation steps for every media type used by the business.

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.

Appropriate 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/protection system (IDS/IPS). Appropriate change detection tools should also be used to enable the detection of changes to critical IT devices.

6.19 Distributed Denial of Service Defense (DDOS Defense)

Registrants must ensure they have conducted a risk analysis of the threat and impact from a Distributed Denial Of Service attack (DDOS) and to deploy the appropriate defences. The review should assess the following existing technical and process controls:

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

6.20 Secure Application Development

Secure application development practices should be in place, such as:

- The testing of application modules and security safeguards with a combination of source code review, exception testing and compliance review to identify insecure coding practices and system vulnerabilities
- The maintainance of separate physical or logical environments for unit, integration and user acceptance testing
- The separation of development and testing environments from the production environment
- The use of secure application development practices; the Open Web Application Security Project (OWASP) is an example of best practice

6.21 Logging and Monitoring

Registrants must complete an assessment of their logging and monitoring requirements. A logging and monitoring policy or procedure should then document the controls. 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, and take into account the criticality of systems
- Where logs contain personal data, they must be treated in accordance with relevant privacy law requirements

- All security logs must be protected from unauthorised access, disclosure, modification or destruction
- Investigation of anomalous activity must be detected in order to understand potential risk to the network
- Security events must be monitored in real-time 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 provide assurance they are secure and provide the functional services required.

7 SECTION III – RESPONSE AND RECOVERY CONTROLS

7.1 Business Continuity and Disaster Recovery Planning

Registrants must develop and implement effective Business Continuity Planning (BCP) and Disaster Recovery (DR) planning policies and procedures. Disaster recovery plans must be prepared to meet the requirements identified in the business continuity planning.

Recovery activities must be coordinated with internal and external parties. A communication plan must be in place to manage communication to internal and external stakeholders, including regulatory authorities and third-party vendors. Registrants must test and validate disaster recovery capability at least annually.

7.2 Crisis Management

The IT incident management framework should also define when a major incident becomes a crisis. Roles and responsibilities must be defined. Senior management must be kept apprised of the development of these incidents so that the decision to activate the disaster recovery plan can be made if required. Management of communications to internal and external stakeholders must also be clearly defined.

8 Definitions:

- **BCP: Business Continuity Planning**
  The process of creating systems of prevention and recovery to deal with potential threats to a registrant.
- **BYOD: Bring Your Own Device**
  Bring your own device refers to employees using personal devices to connect to their organisational networks and access work-related systems.
- **CISO: Chief Information Security Officer**
  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.
- **CSIRT: Computer Security Incident Response Team**

A Computer Security Incident Response Team is an organisation that investigates, manages and responds to computer security incidents

- **Cyber reporting event**
  Any act that results in unauthorised access to, disruption or misuse of the electronic systems or information stored on such systems of a licenced undertaking, including any breach of security leading to the loss or unlawful destruction or unauthorised disclosure of or access to such systems or information.
- **Cyber Security Event**
  Any act or attempt, successful or unsuccessful, to gain unauthorised access to, disrupt or misuse the electronic systems or information stored on such systems of a registrant.
- **DDOS: Distributed Denial Of Service**
  DDOS is short for Distributed Denial of Service. DDOS is a type of Denial of Service (DOS) attack where multiple compromised systems are used to attack a target.
- **DLP: Data Loss Prevention**
  Data loss prevention is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network.
- **DMZ: Demilitarised Zone**
  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.
- **Information Asset**
  The business owner of the asset.
- **Mobile Devices**
  Refers to any portable device, i.e. a cellphone, smartphone, tablet or laptop device.
- **PII: Personally Identifiable Information**
  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.
- **RPO: Recovery Point Objective**
  The recovery point objective is the age of files that must be recovered from backup storage for normal operations to resume if a computer, system or network goes down as a result of a hardware, programme or communications failure.
- **RTO: Recovery Time Objective**
  The recovery time objective is the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.
- **Zero-Day Vulnerability**
  A security flaw that is known to the vendor but the vendor has not released a patch to fix the flaw.