BERMUDA MONETARY AUTHORITY

OPERATIONAL CYBER RISK MANAGEMENT CODE OF CONDUCT

CORPORATE SERVICE PROVIDERS, TRUST COMPANIES, MONEY SERVICE BUSINESSES, INVESTMENT BUSINESSES AND FUND ADMINISTRATION PROVIDERS

15 March 2022

TABLE OF CONTENTS

I. LEGISLATIVE BASIS AND SCOPE OF CODE

1. This document outlines the Bermuda Monetary Authority's (Authority or BMA) Operational Cyber Risk Management Code of Conduct (Code) for corporate service providers, trust companies, money service businesses, investment businesses and fund administration providers.

2. In accordance with the threshold requirement that Relevant Licensed Entities (RLE) must conduct their business in a prudent manner, pursuant to the provisions set out in the Acts below, all corporate service providers, trust companies, money service businesses, investment businesses and fund administration providers (each a RLE), are required to implement adequate systems, appropriate to the nature, scale and complexity of their business risk profile:

   a) Corporate Service Provider Business Act 2012, Schedule 1, paragraphs 3(3) and 3(4);
   b) Trusts (Regulation of Trust Business) Act 2001, First Schedule, paragraphs 5(4) and 5(5);
   c) Investment Business Act 2003, Second Schedule, paragraphs 5(6) and 5(7);
   d) Fund Administration Provider Business Act 2019, Schedule 1, paragraphs 2(4) and 2(5); and
   e) Money Service Business Act 2016, Schedule 1, paragraph 2(4) and 2(5).

3. The Authority is issuing the Code pursuant to the powers under:
   - Section 7 of the Corporate Service Provider Business Act 2012
   - Section 7 of the Trusts (Regulation of Trust Business) Act 2001
   - Section 10 of the Investment Business Act 2003
   - Section 7 of the Fund Administration Provider Business Act 2019
   - Section 7 of the Money Service Business Act 2016

4. In this regard, "adequate systems" include systems that address the management of cyber risks and applies to all RLEs.

5. Failure to comply with provisions set out in the Code is considered by the Authority to determine if an RLE is meeting its obligation to conduct its business in a sound and prudent manner under the acts and regulations.

II. INTRODUCTION

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

7. The Code is designed to promote the stable and secure management of RLEs' Information Technology (IT) systems. It is not exhaustive. RLEs must implement adequate and sufficient technology risk programmes, which consider all relevant operational and business risks that then determine the appropriate risk response and processes and procedures to be implemented and adhered to. RLEs are required to show there has been a board review and continued governance of cyber risk exposures to ensure policies adopted remain relevant.

8. The Code establishes duties, standards, procedures and principles for compliance in relation to operational cyber risk management. The Code should be read in conjunction with applicable codes of practice and the Outsourcing Guidance Notes 2019.

9. The Authority supervises RLEs based on the proportionality principle and, therefore, does not adopt a "one-size-fits-all" approach. Instead, the expectation for RLEs is to implement cyber risk controls that are proportional to the nature, scale and complexity of the organisation. It is acknowledged that some entities will use a third party to provide technology services, and they may outsource their IT resources. In this regard, the Authority expects the RLE to include a review of any third-party services as part of their overall assessment and management of their cyber risk.

III. INTERPRETATION

10. RLEs 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 RLE must implement either what is prescribed in the Code, or a comparable or higher standard that yields similar protection levels (concerning its business model)
- **Should,** while not mandatory, denotes a strong recommendation from the Authority
- **May** denotes that the standard is optional
- **Best practice** includes internationally accepted standards such as those adopted by the National Institute of Standards and Technology or the International Organisation for Standardisation

IV. PROPORTIONALITY PRINCIPLE

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

12. Accordingly, the Authority will assess the RLE's compliance with the minimum criteria for licensing requirements by assessing if it has adhered to the Code in a proportionate manner relative to the nature, scale and complexity of its business operations. These elements are considered collectively rather than individually (e.g., a RLE could be relatively small in scale but manages an extremely complex business; therefore, it is required to maintain a sophisticated risk management framework). In defining these elements:

    - **Nature** defines the relationship between the client entity and the undertaking or characteristics of the service provided
    - **Scale** refers to the volume of business conducted or size of the balance sheet in conjunction with materiality considerations
    - **Complexity** includes organisational structures and ease of information transmission

13. In assessing the existence of prudent business conduct, the Authority regards both its prudential objectives and the appropriateness of each requirement specified in the Code. The proportionality principle described above applies to all sections of the Code, regardless of whether the principle is expressed in it.

V. IDENTIFICATION OF ASSETS AND RISKS

Board Level Governance of Cyber Risk

14. The board of directors (board) and senior management team must have oversight of cyber risks. The board must, at least annually, approve a cyber risk policy. The cyber risk policy may be a standalone policy or a section in a broader risk management 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.

The Operational Cyber Risk Management Programme

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

    a) A risk assessment process to identify, evaluate and manage cyber risks;
    b) Data governance, classification controls and information security controls; and
    c) Detection, protection, response and recovery controls.

16. The programme should define, document and communicate policies, processes and procedures that direct the management of cyber risk.

The Role of the Chief Information Security Officer

17. The person appointed to the role of Chief Information Security Officer (CISO) must be an appropriately qualified member of staff or a similarly experienced outsourced resource. Nevertheless, RLEs should be aware that the board is ultimately responsible for oversight of the outsourced activity.

    Guidance Note: A RLE may outsource the CISO role to a group resource.

18. The role of the CISO is, among other things, to deliver the operational cyber risk management programme. The CISO role should have the necessary experience and competencies to facilitate the delivery of the operational cyber risk management programme. For smaller institutions, the responsibilities may, for example, be assigned to a risk executive who also provides oversight of cyber risk activities.

The Three Lines of Defence

19. Cyber risk governance should follow a "three lines of defence" model, namely: operational management, risk management and audit.

Risk Assessment Process

20. The operational cyber risk management programme must include a risk assessment process, comprising:

    - **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

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

The Re-evaluation of Controls

22. The control environment should be continuously monitored and evaluated to:

    a) Identify control deficiencies and initiate improvement actions;
    b) Plan, organise and maintain standards for internal control assessment and assurance activities; and

c) Evaluate whether the control environment is compliant with laws, regulations and contractual requirements.

Information Technology Audit Plan

23. 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 as required. Based on the internal risk assessment, an IT audit plan should be developed and approved by the board's audit committee or its equivalent. Audits may be carried out by a qualified internal audit resource or by qualified third parties.

Cyber Insurance

24. RLEs should consider the benefits of purchasing a cyber insurance policy, which may be used to mitigate financial loss from a cyber incident. RLEs should review the adequacy of their cyber insurance coverage at least annually.

Asset Identification

25. 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, including that:

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

Managing Outsourcing and Third-Party Service Provider Cyber Risk

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

27. The RLE 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. Senior management must understand the risks associated with IT outsourcing. It is important to note an organisation must never outsource responsibility for governance and risk.

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

Guidance Note: This section of the Code should be read in conjunction with the Outsourcing Guidance Notes 2019.

Cloud Computing

29. 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 (e.g., 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:** 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 and evaluating how cloud computing affects compliance with internal security policies, as well as compliance requirements (e.g., 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

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

Guidance Note: This section of the Code should be read in conjunction with the Outsourcing Guidance Notes 2019.

End-User Developed Systems (End-User Computing)

31. 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.

The Security Review of New Projects and Information Technology Systems

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

VI. DETECT AND PROTECT CONTROLS

Information Technology Services Management

33. 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

Threat Intelligence and Vulnerability Alerting

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

Information Technology Incident Management

35. 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.

Information Technology Security Incident Management

36. A formal IT security incident response process must be established. Consideration should be given to creating a computer security incident response team. All employees, contractors and third-party users must be made aware of the procedure for reporting incidents.

37. A post-incident review should occur; this review should establish the root cause of the incident and conclude any remedial action required.

38. 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.

39. Scenario-based or "tabletop" incident response exercises should be held annually to prepare for any actual incidents that may occur and test the processes in place.

40. RLEs should consider contracting with an external organisation that specialises in security incident investigation and response so that their services are available in the event of a major security incident.

Notification of Cyber Reporting Events to the Authority

41. 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 (an):

    a) Cyber-reporting event has the likelihood of adversely impacting clients;
    b) RLE has reached a view that there is a likelihood that loss of its system availability will have an adverse impact on its business;
    c) RLE 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 business;
    d) RLE 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 business; or
    e) Event has occurred for which a notice is required to be provided to a regulatory body or government agency.

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

43. When in doubt about whether an event is reportable, RLEs should consult with the Authority for guidance. An officer 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, RLEs are expected to keep the Authority updated regularly 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 the root cause has not been confirmed, then the report must still be submitted detailing information known to date, with a final report delivered at the conclusion of the investigation. The Authority may request interim updates, but this will be determined on a case-by-case basis.

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

Logical Access Management

45. 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.

46. 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. Specific processes and audit trails should exist to manage the access and transactions performed by super users or system administrators.

Awareness and Training

47. Staff cyber risk awareness training must be completed at least annually. Staff responsible for cyber risk and cybersecurity should also have relevant skills and training to carry out their role. The board and senior management should participate in the training, as well. Periodic updates, as new threats arise, should be provided to all staff throughout the year.

Data Classification and Security

48. 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.

Data Loss Prevention

49. RLEs should have Data Loss Prevention (DLP) controls in place for their primary business applications. RLEs must perform an assessment of their DLP control requirements. Typically, this assessment would reference the level of data classification, potential unauthorised data egress points and appropriate mitigating controls.

Data Protection and Governance

50. RLEs 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.

51. 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. The retention policy should clearly delineate the time periods appropriate for the

different classifications of data. The documentation should include a glossary to facilitate clarity and ease of use.

Mobile Computing

52. RLEs must establish documented policies, standards, procedures and controls for addressing and enforcing security related to mobile device usage including "bring your own device" programs. Specifically, mobile computing services must be subject to a risk assessment and then secured with appropriate controls.

Protection against Malicious Code

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

Securing Non-public Data

54. Data classified as non-public must be protected by an appropriate level of security. The Authority requires that non-public data (including 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.

Data Availability Management

55. RLEs should put in place a data integrity and availability strategy commensurate with the requirements of the business service (e.g., recovery time objective, recovery point objective and timeliness), as well as threats to that data (e.g., ransomware). The strategy may include one or more of the following: backups, replication, database logs and image snapshots. Periodic testing of the strategy should be performed.

Penetration Testing and Vulnerability Assessments

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

    a) Regular penetration testing of internet-facing services by an independent and qualified testing company;
    b) Security assessment for any new internet-facing services, or changes to existing services, to determine if they should be penetration tested before they go live;
    c) Internal vulnerability scanning;
    d) External vulnerability scanning; and
    e) Baseline standards to document secure configuration baselines of all network devices.

Patch Management

57. RLEs must have patch management procedures that define the identification, categorisation, prioritisation and implementation of security patches applicable to information systems (e.g., operating systems, applications and databases). Security patches must be installed in a reasonable timeframe in accordance with the patch management procedures and tested for effectiveness and potential side effects before installation. RLEs must pay close attention to a vendor's end-of-support date, as patches may no longer be available after this date.

Data Deletion/Sanitisation Policy

58. RLEs should have documented procedures for data deletion, sanitisation and disposal of all media types containing company data in a manner that adequately protects the confidentiality of the data and renders it unrecoverable (e.g.., overwriting, modifying or physically destroying the electronic media to make it unreadable). The media disposal and sanitisation procedure should be tested periodically and communicated to appropriate staff.

Network Security Management

59. Network security standards should be documented in a formal document. Segregation should be used effectively to create zones of enhanced security within a network. Any service accessing the internet should be routed through an enhanced security zone.

60. 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.

61. Defined processes that guide responders to take an appropriate level of response to alerts should be in place.

Denial of Service Defence

62. RLEs should ensure they have conducted a risk assessment of denial-of-service attacks and then deploy the appropriate defences. The review should assess the following:

    a) Inherent risk from a denial-of-service attack to business services;
    b) Detection controls (i.e., how quickly an attack could be detected); and
    c) Mitigation controls (i.e., how effectively traffic can be dropped/cleaned).

Secure Application Development

63. Where application development takes place, a secure development lifecycle should document secure development practices. Examples include:

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

Logging and Monitoring

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

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

Use of Cryptography

65. RLEs should evaluate cryptographic implementations and ensure that only cryptographic modules based on authoritative standards and reputable protocols are enabled. 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.

VII. RESPONSE AND RECOVERY CONTROLS

Business Continuity and Disaster Recovery Planning

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

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

VIII. IMPLEMENTATION

67. The Code comes into force on 15 March 2022 and RLEs are required to comply by 15 February 2023.

IX. DEFINITIONS

- **Business Continuity Planning (BCP)**: The process of creating systems of prevention and recovery to deal with potential threats to an RLE
- **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)**: The senior executive, by whatever title called, appointed by the RLE to oversee and implement its cyber risk programme and enforce its cyber risk policies
- **Computer Security Incident Response Team (CSIRT):** An organisation that investigates, manages and responds to computer security incidents
- **Distributed Denial Of Service (DDOS):** A type of denial-of-service attack where multiple compromised systems are used to attack a target
- **Data Loss Prevention (DLP):** A strategy for ensuring that end users do not inappropriately send sensitive or critical information outside the corporate network
- **Information Asset:** An asset is any data, device or other components of the environment that supports information-related activities
- **Mobile Devices:** Refers to any portable device (e.g., a cell phone, smartphone, tablet or laptop device)
- **Personally Identifiable Information (PII**): 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 Software Development Lifecycle (SDLC):** A document outlining secure application development practice