BERMUDA MONETARY AUTHORITY

Digital Asset Business Operational Cyber Risk Management

Code of Practice

JANUARY 2024

Table of Contents

I. LEGISLATIVE BASIS AND SCOPE OF CODE

This document outlines the Bermuda Monetary Authority's (Authority or BMA) Digital Assets Business (DAB) Operational Cyber Risk Management Code of Practice (Code). This Code applies to all DABs.

The Authority is issuing the Code pursuant to the powers under Section 6 of the Digital Asset Business Act 2018. The Code establishes duties, requirements, standards and procedures to be complied with in relation to operational cyber risk management. The Code should be read in conjunction with:

- Section 6 of the Digital Asset Business Act 2018
- Digital Asset Business (Cyber Risk) Rules 2023
- Digital Asset Business Code of Practice 2023
- Digital Asset Business Custody Code of Practice 2024

II. INTRODUCTION

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

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

For the specific purpose of reading this Code, DABs should have regard to the following:

1. ***Must*** - Denotes that the standard is mandatory; the DAB 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);
2. ***Should*** - While not mandatory, denotes a strong recommendation from the Authority; a registrant may depart from it where it has documented a valid reason;
3. ***May*** - Denotes that the standard is optional; and
   Best practice - Includes recognised standards such as those adopted by the National Institute of Standards and Technology or the International Organisation for Standardization.

III. PROPORTIONALITY PRINCIPLE

The Authority appreciates that DABs have varying risk profiles arising from the nature, scale, and complexity as well as the inherent risk profile of the business and that those DABs 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 DAB's compliance with the Code in a proportionate manner

relative to its inherent risk (i.e., nature, scale, complexity and risk profile). These elements will be considered collectively rather than individually (e.g., a DAB 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:

1. ***Nature*** **-** Includes the relationship between clients and the DAB or characteristics of the service provided (e.g., a DAB that maintains custody of clients' assets versus one that outsources the custody). To provide another example, an open blockchain infrastructure and a private blockchain infrastructure are different, with different inherent risks;
2. ***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 DAB's failure); and
3. ***Complexity*** - Includes items such as 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 Code provision for the DAB, taking into account that DAB's nature, scale, complexity and risk profile.

The proportionality principle discussed above applies to all sections of the Code, regardless of whether the principle is explicitly mentioned.

IV. SECTION I - IDENTIFICATION OF ASSETS AND RISKS

4.1 Board Level Governance of Cyber Risk

The board of directors (board) and senior management team must have oversight of cyber risks. The board 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 available to the board and senior management.

4.2 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.

4.3 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:

1. A risk assessment process to identify, evaluate and manage cyber risks;
2. Data governance, classification controls and information security controls; and
3. Detection, protection, response and recovery controls.

The programme should define, document and communicate policies, processes and procedures that direct the management of cyber risk. The DAB must employ adequate cyber risk personnel to manage its cyber security risks. The DAB must require personnel (and provide opportunity and resources) to remain current in changing cybersecurity threats and countermeasures.

Further, the cybersecurity programme should outline policies surrounding how the DAB will tackle market abuse and, where applicable, under what conditions it will halt trading, suspend or close offending client accounts and notify relevant authorities.

4.4 Three Lines of Defense Model (3LOD)

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

4.5 Risk Assessment Process

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

1. ***Identification*** **-** The organisation understands the cyber risk to operations, assets and individuals;
2. ***Measurement*** **-** The organisation understands the potential impact and consequences of these risks;
3. ***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; and
4. ***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.

4.6 The Re-evaluation of Controls

The control environment should be continuously monitored and evaluated to:

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

4.7 Information Technology (IT) Audit Plan

The third line of defence, audit, should provide the audit committee of the board (or equivalent) an independent and objective assessment of the effectiveness of controls as required. An annual IT audit plan must 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 qualified third-parties.

4.8 Cyber Insurance

DABs should consider the benefits of purchasing a cyber insurance policy, which may be used to mitigate financial loss from a cyber incident. DABs should review the adequacy of their cyber insurance coverage at least on an annual basis.

4.9 Assets Identification

An asset inventory must 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.

1. All information assets must be owned by a designated part of the business;
2. Information owners are responsible for classifying information and information assets;
3. 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; and
4. An appropriate set of procedures for information labelling and handling should be developed and implemented.

4.10 Managing Outsourcing and Third-Party Service Provider Cyber Risk

Where the DAB outsources cyber-related functions either externally to third parties or internally to other affiliated entities, the registrant must ensure 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 contain provisions governing the roles, relationships, obligations and responsibilities of all contracting parties.

A risk assessment must be completed before any third-party blockchain applications, smart contracts, platforms or services are used in any systems environment (i.e., development, test, production). DABs must ensure they are fully aware of risks associated with third-party IT suppliers.

4.11 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:

1. ***Governance and Enterprise Risk Management (ERM)*** **-** The ability of an organisation to govern and measure enterprise risk introduced by cloud computing, the ability to assess the risk of a cloud provider adequately, and the definition of roles and responsibilities;
2. ***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;

3. ***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 and legislative); and
4. ***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.

4.12 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.

4.13 Staff Vetting Process

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

4.14 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.

V. SECTION II – DETECT AND PROTECT CONTROLS

5.1 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

5.2 Performance and Capacity Management

A capacity and performance management process must be in place to ensure that services achieve agreed and expected performance, satisfying current and future demand. The following tasks must be undertaken as a minimum:

- Service performance and capacity analysis
- Research and monitoring of the current service performance

- Capacity and performance modelling
- Service performance and capacity planning
- Demand forecasting and resource planning

5.3 Threat Intelligence and Vulnerability Alerting

DABs 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.

5.4 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 to restore normal IT service following the incident and ensure minimal impact on business operations.

5.5 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 must 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. DABs 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.

5.6 Notification of Cyber Reporting Events to the Authority

DABs must have documented policies and procedures to address actions taken, client notifications and notifications to the Authority applicable to an event or suspicion of hack, theft, compromise or attack. This includes any situation whereby a digital asset being kept in custody has been compromised (or cyber reporting event as defined in the Act). Procedures must be reviewed and audited annually and include velocity limit, freeze and circuit breaker actions designed to protect assets in an emergency.

As per the Act, 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 clients;

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

(c) a DAB 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) a DAB 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;

(e) a DAB has become aware that there is a likelihood that a digital asset being kept in custody has been compromised; or

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

When in doubt about whether an event is reportable, DABs should consult with the Authority for guidance. A senior representative must notify the Authority within 24 hours from the time that there is either a determination or a confirmation of an event (whichever is sooner).

Following the initial notification, DABs 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 the 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.

DABs are expected to maintain logs of all cybersecurity incidents together with a timeline of events and 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.

5.7 Multi-factor Authentication

For any web-based services provided by a DAB where user authentication is required, multi-factor authentication must be used.

5.8 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 access changes must be maintained to demonstrate proof of proper access rights management. Specific processes and audit trails should exist to manage the access and transactions performed by super users or system administrators. Audit logs must be stored so

that they are available for review by the Authority for at least five years.

5.9 Awareness and Training

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

5.10 Data Classification and Security

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

5.11 Data Loss Prevention (DLP)

DABs must have DLP controls in place for their primary business applications. Therefore, DABs must perform an assessment of their (DLP) control requirements. Typically, this assessment references the level of data classification, potential unauthorised data egress points and appropriate mitigating controls.

5.12 Data Protection and Governance

DABs 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).

5.13 Mobile Computing

Mobile computing services, including “bring your own device” scenarios, must be subject to a risk assessment and secured with appropriate controls.

5.14 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.

5.15 Securing Nonpublic Data

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

5.16 Data Availability Management

DABs should put in place a data integrity and availability strategy commensurate with the requirements of the business service. The strategy may include one or more backups, replication, database logs and image snapshots. Periodic testing of the strategy should be performed.

5.17 Penetration Testing and Vulnerability Assessments

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

1. Regular penetration testing of internet-facing services by an independent and qualified testing company (minimum annual frequency);
2. 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;
3. Internal vulnerability scanning (minimum six-month frequency);
4. External vulnerability scanning (minimum monthly frequency); and
5. Baseline standards to document secure configuration baselines of all network devices.

5.18 Patch Management

DABs must have patch management procedures that define the identification, categorisation and prioritisation of security patches. Security patches must be tested and installed within a reasonable time frame. DABs must pay close attention to a vendor's end-of-support date as patches may no longer be available after this date.

5.19 Data Deletion/Sanitisation Policy

The process for data deletion, sanitisation and disposal of all media types that are used by the business should be documented and communicated to the appropriate staff. The media disposal and sanitisation process should be tested periodically.

5.20 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 an enhanced security zone.

Network security tools should be used to detect network intrusions and provide alerts when an intrusion occurs. Examples of a network intrusion detection tool include a network intrusion detection system/intrusion protection system.

5.21 Denial of Service (DOS) Defence

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

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

5.22 Secure Application Development

Where application development takes place, a Secure Software Development Lifecycle must be in place to embed secure development practices. Decentralised applications (Dapps) must be subject to a formal secure software development life cycle. This should formalise the following activities:

1. Design, build, test, deploy, monitor;
2. Secure application development in line with best-practice standards (e.g., the Open Web); and
3. Open Web Application Security Project (OWASP) and the Decentralised Application Security Project (DASP).

Best practices must include:

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

5.23 Smart Contracts

The development of smart contracts must be subject to secure development practices (see section 5.22). In addition, smart contracts should be subject to:

1. Benchmarking against a smart contract-specific vulnerability standard (e.g., the Smart Contract Weakness Classification Registry);
2. A best practice security assessment relevant to the blockchain environment;
3. A review of implementation risks - intrinsic errors that result in unintended smart contract behaviour (e.g., unnecessary functionality that may add vulnerabilities to code, enabling front running transactions; and
4. A review of design risks - system features that are exploited to alter intended smart contract behaviour (e.g., lack of privacy).

An assessment of the security testing required must be completed before any new smart contracts are deployed. Any changes to smart contracts must also be assessed to determine what level of security testing is required.

5.24 DLT/Blockchain Security

The use of Blockchain services must be risk-assessed. Services interfacing with blockchain should be subject to best-practice security controls to include:

- Enforce identity and access controls to access the blockchain solution and data
- Use privileged access management practices for escalated actions
- Use Application Programming Interface (API) security best practices to safeguard API-based transactions
- Secure communications both internally and externally using transport layer security
- Use strong cryptographic key/certificate management
- Have a security incident and event management capability

5.25 Logging and Monitoring

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

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

5.26 Use of Cryptography

DABs must 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 security issues.

5.27 Physical Security Requirements of Storage Facilities

A risk assessment should take place to assess what assets are stored at each storage facility and what associated physical controls are required. DABs must demonstrate that all storage facilities are equipped to an appropriate industry standard.

VI. SECTION III – RESPONSE AND RECOVERY CONTROLS

6.1 Disaster Recovery (DR) and Business Continuity Planning (BCP)

DABs must implement effective BCP and DR policies and procedures to include:

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

VII. IMPLEMENTATION

The Code comes into force on 1 January 2024, and DABs are required to be in compliance by 30 June 2024.

VIII. GLOSSARY

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): 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 CSIRT 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 the practice of detecting and preventing data breaches, exfiltration, or unwanted destruction of sensitive data.

Enhanced security zone: An enhanced security 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 device: 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.