BERMUDA MONETARY AUTHORITY

11 May 2022

NOTICE

EXTENDED PERIOD TO SUBMIT COMMENTS

DIGITAL ASSET BUSINESS - OPERATIONAL CYBER RISK MANAGEMENT CODE OF PRACTICE

Cyber security is a key risk affecting all financial sectors regulated by the Bermuda Monetary Authority (Authority or BMA) and continues to garner global attention as the number and severity of risk incidents increase. As such, it is also an important area of concern within the Digital Asset Business (DAB) sector.

As part of its commitment to foster and encourage the prudent development of the growing DAB sector in Bermuda, the Authority is posting for consultation its draft new Digital Asset Business Operational Cyber Risk Management Code of Practice (Code) along with revised Digital Asset Business Custody Code of Practice, Digital Asset Business Code of Practice and Digital Asset (Cybersecurity) Rules (together, the Consultation Documents). These documents are annexed to this notice for ease of reference.

The Consultation Documents intend to streamline the obligations of DABs with those of other sectors. It is, therefore, to the fullest extent possible, harmonised with the Insurance and Banking, Trust, Corporate Services and Investments regulatory cyber frameworks. Nevertheless, in light of the heightened inherent cyber risk pertaining to DABs, the Consultation Documents contain more stringent requirements in key areas, including (i) audit trails (system logs) and audits both in the periodicity and number of controls in scope; (ii) systems/code testing, change management and incident reporting; and (iii) the addition of DAB-specific requirements (e.g., smart contracts and blockchain security).

The Consultation Documents are designed to promote the stable and secure management of information technology systems of regulated entities. They are deliberately not exhaustive and should remain flexible so as to accommodate a wide range of business models.

DABs are required to implement their own technology risk assessment programmes, and determine their top risks and decide the appropriate risk response. DABs must be able to evidence that there is adequate board visibility and governance of their cyber risk.

Failure to comply with provisions set out in the Consultation Documents will be an important 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.

The DAB industry and other interested parties are invited to submit their views on the proposals set out in the Consultation Documents. Comments should be sent to the Authority digitally, via the below survey link or QR code, no later than 6 June 2022 *(extended from 6 May 2022 as it appeared on the original notice)*.

https://www.surveymonkey.com/r/WQTTT88

ANNEX

BERMUDA MONETARY AUTHORITY

Digital Asset Business Operational Cyber Risk Management

Code of Practice

MAY 2022

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 Paragraph 7, Section 1 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 7 of the Digital Asset Business Act 2018
- Digital Asset Business (Cybersecurity) Rules 2022
- Digital Asset Business Code of Practice 2022
- Digital Asset Business Custody Code of Practice 2022

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 forguidance. 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 6.22). 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 2023, and DABs are required to be in compliance by 30 June 2023.

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.

BERMUDA MONETARY AUTHORITY

DIGITAL ASSET BUSINESS CUSTODY CODE OF PRACTICE

MAY 2022

Table of Contents

I. INTRODUCTION

Safeguarding client assets by preventing fraud or misappropriation is a primary concern of the Bermuda Monetary Authority (Authority or BMA). Section 18 (1) of the Digital Asset Business Act 2018 (Act) prescribes requirements relating to safeguarding client assets while the Digital Asset Business Code of Practice 2018 (which applies to all Digital Asset Businesses (DAB)) further prescribes that a DAB must:

> "*…ensure that any assets belonging to clients are kept segregated from the DAB's own assets. To ensure the return of client assets in the event the DAB is placed into liquidation, becomes insolvent or is a victim of theft.*"

Section 18 of the Act further requires that the DAB, "*…maintain in its custody a sufficient amount of each type of digital asset in order to meet its obligations to clients.*" Therefore, custodians of digital assets are not allowed to rehypothecate, transfer (except to another qualified custodian, where appropriate) or otherwise sell digital assets held for the benefit of their customers.

The purpose of this Digital Asset Business Custody Code of Practice (Code) is to provide more clarity to the digital asset industry as to what standards the Authority expects when considering whether a custodian is employing an acceptable level of care when safeguarding its clients' digital assets. The present Code should be read in conjunction with the DAB Operational Cyber Risk Management Code of Practice.

For the purpose of this Code, custodian is defined as any DAB that has sole or partial control over digital asset keys on behalf of clients. Where a DAB outsources custody of client digital assets to a qualified custodian, the DAB must satisfy itself that the qualified custodian maintains comparable standards to those outlined in the Code.

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
4. **Best practice -** Includes recognised standards such as those adopted by the National Institute of Standards and Technology or the International Organisation for Standardization.

The DAB must regularly assess the custody risks arising from its business model and implement higher standards than outlined in the Code where best practice warrants.

Instances where higher standards may be warranted, include when a DAB has a unique business model with extraordinary risk, or there are generally accepted knowledge breakthroughs in cybersecurity risk management and mitigation strategy, etc. The DAB's risk assessments must be documented and retained for at least five years in a manner that allows the risk assessments to be provided to the Authority upon request.

1.2 Status of the Code

The Code is made pursuant to section 6 of the Act. Section 6 requires the Authority to publish, in such a manner as it sees fit, a Code that provides guidance on the duties, requirements, procedures, standards and sound principles to be observed by persons carrying on digital asset business. Failure to comply with provisions set out in the Code will be taken into account by the Authority in determining whether a licensed DAB is meeting its obligation to conduct its business in a sound and prudent manner in accordance with the Act.

1.3 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 in nature, 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.

1.4 Purpose and Scope

Due to the unique nature of their composition, digital assets require specificity in dictating safekeeping and transaction handling custody procedures. Unlike traditional assets, where the physical asset itself, or a proxy of the asset, is held in custody, digital assets are held in digital form. By definition, digital assets mean "anything that exists in binary format and comes with the right to use it and includes a digital representation of value," which can exist on a public or private distributed ledger.

In the case of a public ledger, because the information is public and distributed, transaction reversals are not normally possible (or are difficult to reverse). This makes the practice of secure transaction handling and verification of paramount importance to proper digital asset custody standards.

The Code defines a standard for operating as a custodian of digital assets and is to be adhered to by every DAB that maintains or is responsible for the custody of its client(s)' private keys. This Code is split into the following four sections:

- Business control requirements
- Technology controls - custody safekeeping
- Technology controls - custody transaction handling and operations
- Technology controls - audit

II. BUSINESS CONTROL REQUIREMENTS

A DAB must not underestimate the importance of sound business controls. There are a number of facets to business controls relating to staffing, outsourcing partners, access controls, operational risk management and business continuity. The business control standards are as follows:

2.1 Liquidity

The DAB must have documented mechanisms in place to assess its liquidity needs, including sums required for trading and other client transaction types.

2.2 Hot and Cold Storage

A risk assessment must be completed for cold storage (offline) and hot storage (online). Factors for determining the best method of storage include, but may not be limited to, nature of the assets, the volume of transactions and speed at which transactions need to be completed, the ability to reverse transactions, and the risk tolerance of the DAB's clients.

2.3 Fraud Detection and Compliance Standards

DABs must develop a protocol for fraud detection and adherence to internal compliance requirements. This should include a detection system for identifying suspicious transactions as well as a procedure for reviewing suspicious transactions.

2.4 Personnel Dedicated Roles and Responsibilities

DABs must have established roles and responsibilities for custody operations and custody operational risk management that are formally documented and formally approved by the senior management team.

2.5 Insurability and Other Protections

DABs must demonstrate that assets under custody carry appropriate insurance or other financial protections to cover or mitigate potential loss exposure.

2.6 Proof of Reserves (POR)

Section 18(3) of the Act requires that, "A ... [DAB] that has custody of one or more digital assets for one or more clients must maintain in its custody a sufficient amount of each type of digital asset in order to meet its obligations to clients." To fulfil this requirement, a DAB must maintain adequate accounting and other relevant records and adequate systems and controls to accurately track ownership and quantity of client digital assets it has taken into custody.

The DAB must have adequate segregation of duties to protect the integrity of the record-keeping process and appropriate redundancy and business continuity processes, procedures and controls to be able to access records of client digital assets in custody at all times, including post-natural and other disasters.

2.7 Collusion Mitigation

DABs must demonstrate a method for controlling the signing process that prevents a quorum of individuals from acting in bad faith and/or collusion. Collusion mitigation may be accomplished in any of the following ways including but not limited to:

1. Controls including oversight or separation of duties that prevent a linear ability to create, approve,

sign transactions and broadcast to distributed ledger networks;
2. Distribution of signatories with differing incentives (e.g., client, custodian, third parties);
3. Unknown identities of signatories among each other; and
4. Rotation of signatories, signing times or signing locations.

The risk of collusion and other malicious acts must be addressed as part of recurring operational risk assessments.

III. TECHNOLOGY CONTROLS PART I: CUSTODY SAFEKEEPING

One of the most important responsibilities of the DAB is the safekeeping of digital assets in its custody. Controls must be in place to ensure digital assets are securely created and stored. Additionally, uninterrupted availability of assets is another important requirement.

3.1 Seed generation

The secure creation of cryptographic keys and seeds requires two things to be secure: confidentiality and un-guessable numbers. Confidentiality is required to ensure that the newly created keys or seeds are not read/copied by an unintended party. Un-guessable numbers are required to ensure the newly created key cannot be guessed or determined by an unintended party.

The seed should be created using a compliant deterministic random bit generator. DABs must create safeguards in the seed and subsequent key generation process that demonstrates resistance to supposition and potential bad actor collusion (note that secure non-deterministic key generation mechanisms may also be used).

The seed must have, as a minimum, random sequence 256-bit entropy. The result must be at least a 256-bit entropy input that is encoded into a mnemonic 24-word phrase, as a minimum. DABs must then utilise a hashing function to generate a 512-bit value minimally (note that the 24-word phrase is considered the backup seed because it can be utilised to regenerate a seed).

DABs must, at a minimum, utilise three individuals to perform the process of creating entropy in the creation and production of the seed, with no single person ever possessing the entirety of the seed or backup mnemonic word phrase. When a single seed is produced for a signatory, the signatory must not be involved in the production of the public and private keys.

None of the seed creators are permitted to participate in the act of cryptographically signing or having access to the systems that facilitate transactions.

3.2 Key Pair Generation

DABs must demonstrate adherence to an industry-standard method of key generation. Key generation must be performed in a manner in which a revoked signatory does not have access to the backup seed or knowledge of the phrase used in its creation. All keys must be encrypted in a manner preventing a compromised signatory from recovering the seed.

3.3 Data Sanitisation Post Seed and Key Generation

Secure deletion and destruction mechanisms must be in place to prevent unwanted artefacts from seed, key and wallet generation.

3.4 Seed and Key management procedure

A procedure must be formally documented detailing security, redundancy, backup, availability and logical access controls. This must include as a minimum:

1. Strong encryption and secure device storage are in place for client private keys that are not in use (i.e., client private keys stored in cold wallets);

2. DABs must, at all times, maintain logical access controls rendering it impossible to achieve a quorum of transaction signatures from keys stored in a single location;

3. DABs must demonstrate that once the mnemonic backup seed phrase has been generated, it is broken into at least two or more parts. DABs must demonstrate that under no circumstances will a sufficient number of backup seed phrases that could be used to facilitate a transaction be stored in any single facility;

4. Key and seed back-ups must be stored separately from the primary key and seed. Key and seed back-ups must be stored with strong encryption equal to or better than that used to protect the primary key. The seed and key backup must be protected by access controls to prevent unauthorised access; and

5. For the storage of critical seeds, keys and key parts, Hardware Security Modules (HSM) that are Federal Information Processing Standard 140-2 certified are recommended as the most secure key storage mechanism. Note that HSMs can be physical or virtual devices.

3.5 Key Access and Compromise Procedure

A formal documented procedure must be in place outlining the process to follow where a member of staff has had any access to keys or seeds. An audit trail must record every change of access including who performed the change.

A DAB must document a key compromise procedure. An event triggering the procedure must include, but not be limited to, the compromise of the whole seed, a partial seed or a key derived from a seed. In such a situation, if the underlying seed is believed to be compromised, the DAB's response procedure must include the mechanism for new wallet creation and asset migration. If it is determined by the DAB that a key is compromised, a risk event must be documented and investigated.

3.6 Key Revocation Procedure

DABs must promulgate procedures for immediately revoking a signatory's access. Procedures must follow the standard protocol around removing user access without the need to create a new wallet. Internal audits to recertify access should be performed at least quarterly.

DABs must have a written procedure document that is followed for on/off-boarding. The procedure must outline every permission to grant/revoke for every role in the information system. In addition, all grant/revoke requests must be made via an authenticated communication channel (transmitted using an encrypted protocol).

3.7 Perpetual Access

A DAB must demonstrate that it can provide clients with perpetual access to all assets in custody in the event a DAB ceases to operate or cannot fulfil its custody agreement. Any exceptions to this must be clearly defined as a service level agreement and communicated to the customer. This may include a formal

disbursement or custody transfer process.

3.8 Account Segregation

While keeping client assets separate from their own, DABs may commingle client assets in order to benefit clients; however, proper accounting must be in place to accurately allocate each holding to the respective client. Where the DAB commingles client assets, it must document and implement measures to demonstrate that the level of security achieved is commensurate with an arrangement where every client has a one-to-one relationship with a given address.

3.9 Physical Security and Access Standards for On-Site Cold Storage

For on-site cold storage, a risk assessment must 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.

IV. TECHNOLOGY CONTROLS PART II: CUSTODY TRANSACTION HANDLING

A DAB must ensure that transactions are subject to controls to ensure they are secure and trusted and that measures are in place to prevent fraud. Transactions must be recorded in system audit records. These records must then be subject to periodic audits.

4.1 Multi-Signature Authorisation

A documented procedure must be in place detailing the use of multiple signature authorisation. DABs should use an M-of-N multi-signature standard with a minimum of three signatories required for a quorum signature standard for all transaction types. Where this is not possible, an appropriate mitigating authorisation control that uses the principle of multiple signatures must be used. Multi-signature authorisations must be audited on an annual basis.

4.2 Transaction Authorisation Requirements

A risk assessment of transaction types must be completed. This assessment must define appropriate transaction authorisation control requirements. Based on the assessment outcome, appropriate controls must be put in place. Decision approval evidence, including chain of custody, must be retained for review for five years.

4.3 Periodic Transactions Audit

Each quarter DABs must draw a sample of transactions to be audited internally to ensure that internal processes are functioning as intended. DABs must take remediation action as needed in the event faults are discovered. Integrity controls must be in place to ensure that records and audit trails cannot be changed.

1. ***Contractual Nature of Evidence:*** The evidence required for each signatory to prove true in order to authorise a transaction must be contractually agreed upon by all signatories. In the event approval signing and transaction (Tx) signing are abstracted, Tx approvers must have access and appropriate expertise to evaluate required evidence prior to an authorised signing ceremony.
2. ***Proof of Evidence:*** Each approver or signatory is required to provide proof of the evidence referenced for an authorisation.
3. ***Proof of Elapsed Time:*** Each transaction and signature action associated with a transaction must have a specific time duration tracked against each option for any transaction where the conditions of the evidence are time-based.

4. ***Auditability:*** DABs must store all evidence internally and must have it reviewed at multiple-levels within a transaction. A minimum of two separate individuals must perform reviews around a specific request. Evidence is collected based on a set checklist of necessary documentation based on the role the signatory is representing. DABs must establish controls around the processes, which must be evaluated on a periodic basis and adjusted if necessary.
5. ***Books and records:*** DABs must maintain a full audit trail of all user/admin actions. This includes specific information about each transaction, including but not limited to:
    - Date and time of the transaction
    - Transaction event type
    - Jurisdiction of the client and relevant signatories
    - Account balances and the value of the transaction

This audit log must be stored so that it is available for review by the Authority for at least five years.

V. TECHNOLOGY CONTROLS PART III: AUDIT

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.

5.1 Recurring Audit Requirements for Digital Assets

The following procedures must be subject to an audit every six months as a minimum frequency. Evidence of the audits must be documented and made available to the BMA upon request.

The bulleted list below details audit requirements that are referenced throughout this document and must be audited every six months as a minimum frequency:

- Key and seed generation and management processes
- Key revocation procedure - (ref 3.6)
- Multi-signature authorisations - (ref 4.1)
- Transaction system audit logs consisting of: - (ref 4.3)
    - Contractual nature of evidence - quarterly audits
    - Proof of evidence - quarterly audits
    - Proof of elapsed time - quarterly audits
    - Completed transaction audit to ensure compliance of proof of evidence protocols
- Suspicious transaction handling
- Migration of storage devices (cold to hot storage)
- Proof of solvency random address

All audit records must be retained for at least five years in a manner that can be made available to the Authority upon request.

VI. GLOSSARY:

For the purpose of the Code, the following terms and definitions shall apply:

Address: A cryptocurrency address is (usually) an encoded form of a public key from a wallet that can be used as the recipient of a transaction. In multi-signature schemes, an address may be an encoding of information, including several public keys and other information like a bitcoin Pay to Script Hash (P2SH) address.

Cold storage: A method of storing information that is not connected to the internet.

Custodian: A financial institution, including a DAB, charged with the custody of digital asset keys on behalf of clients. The custodian may have sole or partial control over the digital asset keys.

Custody: The protective care or guardianship of digital assets that are held or being transacted.

Entropy: Randomness or unpredictability within source code applied during generation of a cryptographic seed to ensure a seed cannot easily be recreated.

Evidence: The available body of facts or information indicating whether a belief or proposition is true or valid.

Multi-signature: An M-of-N method of transacting. This refers to needing a minimum number of signatures (M) out of the total available signatures on a wallet (N).

Safekeeping: The contractual responsibility of securing and preserving digital assets held in custody by a custodian.

Seed: A slice of entropy typically used to initialise a random number generator, pseudorandom number generator/deterministic random bit generator (PRNG/DRBG) or other crypto-system (e.g., hierarchical deterministic wallets, deterministic signatures).

Signatory: An individual tasked with providing one of the signatures in an M-of-N multi-signature scenario.

Signature: A cryptographic authorisation applied by a designated signatory in a transaction.

Transaction: An exchange or interaction specific to the digital assets in custody.

Transaction type: Classification of a transaction purpose and distinguishable by its purpose (e.g., "withdraw" versus "deposit" versus "fee").

BERMUDA MONETARY AUTHORITY

DIGITAL ASSET BUSINESS ACT 2018

CODE OF PRACTICE

MAY 2022

Table of Contents

I. INTRODUCTION

1. This Code of Practice (Code) is made pursuant to section 6 of the Digital Asset Business Act 2018 (Act). Section 6 requires the Bermuda Monetary Authority (Authority or BMA) to publish, in such manner as it sees fit, a Code that provides guidance on the duties, requirements, procedures, standards and sound principles to be observed by persons carrying on Digital Asset Business (DAB).

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

3. The Code should be read in conjunction with the DAB Statement of Principles issued under section 5 of the Act.

II. PROPORTIONALITY PRINCIPLE

4. The Authority appreciates that DABs have varying risk profiles arising from the nature, scale and complexity of their 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.

5. Accordingly, the Authority will assess the DAB's compliance with the Code in a proportionate manner relative to its 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 considering these elements:

    a. Nature includes the relationship between clients and the DAB or characteristics of the service provided (e.g., a DAB that takes custody of a client's assets versus one that does not);
    b. 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
    c. Complexity includes items such as organisational structures and product design.

6. 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.

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

III. CORPORATE GOVERNANCE

8. The DAB must establish and maintain a sound corporate governance framework, which provides for appropriate oversight of the DAB's business and adequately recognises and protects clients' interests. The framework should have regard for international best practice on effective corporate governance. Corporate governance includes principles of corporate discipline, transparency, accountability, responsibility, compliance and oversight.

9. The ultimate responsibility for sound and prudent governance and oversight of the DAB rests with its board of directors or equivalent governing body (board). In this regard, the board is responsible for ensuring corporate governance policies and practices are developed and applied in a prudent manner that promotes the efficient, objective and independent judgment and decision-making by the board. The board must also have adequate powers and resources to be able to discharge its duties fully and effectively.

3.1 The board

10. The Authority recognises that the board plays a critical role in the successful operation of a DAB. The board is chiefly responsible for setting corporate strategy, reviewing and monitoring managerial performance, and determining an acceptable level of risk. Therefore, the effectiveness of the DAB's board is a basic tenet of the Authority's risk-based supervisory approach. Pragmatically, the board will likely delegate tasks; however, the delegation of authority to board committees, chief and senior executives, employees, or external parties does not absolve the board from its ultimate responsibilities.

11. The board must ensure the business is effectively directed and managed, and conducted in a professional manner with appropriate integrity and due care. It is the responsibility of the board to ensure that processes exist to assess and document the fitness and propriety of its members, controllers and officers. The board must also take into account the fact that conflicts of interest, or potential conflicts of interest, may on occasion preclude the involvement of specific individual members on particular issues or decisions.

12. To effectively discharge its duties, the board must have an appropriate number and mix of directors to ensure that it has requisite experience, knowledge, skills and expertise commensurate with the nature, scale complexity and risk profile of the DAB's business.

13. Individual board members must:

    a. Act in good faith and honestly and reasonably exercise due care and diligence;
    b. Ensure the interests of clients are protected;
    c. Exercise independent judgment and objectivity in their decision-making; and

d. Ensure appropriate policies and procedures exist to effectively deal with conflicts of interest.

3.2 Oversight responsibilities of the board

14. As the DAB's governing body, a key board responsibility is setting appropriate strategies and overseeing implementation. This includes ensuring that chief and senior executives establish a framework to implement the DAB's strategic business objectives.

15. The board is also responsible for providing suitable oversight of the DAB's governance, risk management and internal controls frameworks, including any activities and roles that are delegated or outsourced. A list of oversight responsibilities that the board must consider when establishing and assessing the effectiveness of the corporate governance framework includes ensuring the existence of:

    a. An operational framework (including risk management, internal audit and compliance functions) to ensure adequate oversight responsibilities so that sound corporate governance exists throughout the organisation;
    b. Processes to assess and document the fitness and propriety of board members, controllers, the chief and senior executives, senior representatives and third-party service providers, including auditors, custodians, investment managers, etc.;
    c. Board committees (where required) to provide oversight of key operational areas, including finance and investments;
    d. Policies and procedures to ensure adequate board oversight of the chief and senior executives;
    e. Processes for the engagement and dismissal of the chief and senior executives and third-party service providers;
    f. Policies and procedures to manage and mitigate conflicts of interest;
    g. Processes to ensure key employees are adequately skilled to execute and discharge their duties and are compensated in a manner that encourages sound risk management and compliance;
    h. Clearly defined charters, roles and responsibilities for the board, committees, chief and senior executives, and other key employees;
    i. Business and operational strategies, plans, budgets, and significant policies and procedures, including those surrounding oversight;
    j. Review and approval of significant policies and procedures promoting effective corporate governance across the organisation, including those for risk management and internal controls, internal audit and compliance functions;
    k. Clear documentation and regular review of processes regarding the roles and responsibilities of the board, the chief and senior executives, and other key employees delegated corporate governance responsibilities (including appropriate segregation of the oversight function from management responsibilities);

l. Adequate independence for the risk management, internal audit and compliance functions to assist in oversight responsibilities and ensure these functions have a direct communication channel to the board and relevant committees; and
m. Processes to confirm that the board has appropriate access to accurate, relevant and timely information to enable it to carry out its duties and functions, including the monitoring and review of the performance and risk exposures of the DAB and the performance of the chief and senior executives.

3.3 Responsibility of the chief and senior executives

16. Given the important roles these individuals play, the board must ensure that great care is taken in the selection of the chief and senior executives. In addition to supporting the board, the chief and senior executives are also responsible for the prudent administration of the DAB. Such responsibilities include:

    a. Managing and executing the day-to-day operations of the DAB, subject to the mandate established by the board and the laws and regulations in the operating jurisdiction;
    b. Assisting the board to develop and implement an appropriate control environment, including those around reporting and security systems;
    c. Providing recommendations on strategic plans, objectives and key policies and procedures to the board for evaluation and authorisation;
    d. Assisting the board with its oversight responsibilities by ensuring that the board has accurate and timely information, allowing the board to conduct robust and candid discussions on operational performance, strategy and major policies, and to appraise the performance of management;
    e. Supporting oversight of both internal control functions (e.g., risk management, internal audit and compliance) and external third-party services;
    f. Ensuring that key functions assigned corporate governance responsibilities are supported with adequate resources to execute and discharge their duties;
    g. Ensuring that external service providers, including approved auditors, have adequate resources and information to fulfil their role, including access to timely and accurate internal and outsourced records; and
    h. Ensuring the proper vetting of all staff.

    Given the governance responsibilities, where requirements are imposed upon the DAB throughout the Code, the Authority will look to and expect the chief and senior executives, and ultimately the board, to ensure compliance.

IV. SENIOR REPRESENTATIVE

17. The role of the approved senior representative is integral to the BMA's DAB supervisory and regulatory framework. While the DAB's board and the chief and senior executives have primary responsibility for the DAB's conduct and performance, the approved senior representative acts in an "early warning" role and monitors the DAB's

compliance with the Act on a continuous basis in accordance with Section 20 of the Act.

18. The Act requires every DAB to appoint a senior representative who must maintain a head office in Bermuda except in the case of Class T (test) licence holders whose senior representative may maintain an office outside of Bermuda. The appointed senior representative must be knowledgeable in digital asset business and related Bermuda laws and regulations.

19. The approved senior representative would generally be a director or senior executive of the DAB who, under Section 20 of the Act, has the legislated duty to report certain events to the Authority.

20. The board and chief and senior executives must make arrangements to enable the approved senior representative to undertake their duties pursuant to the Act efficiently and effectively, including providing access to relevant records.

V. RISK MANAGEMENT FRAMEWORK

21. The board and the chief and senior executives should, based on their judgement, adopt an effective risk management and internal controls framework. The framework should have regard for international best practices on risk management and internal controls. This includes ensuring the fitness and propriety of individuals responsible for the management and oversight of the framework.

5.1 Risk management function

22. The DAB must establish a function to assist it with the oversight responsibility of the organisation's risk management framework. Depending on its risk profile, the function may be headed by a chief risk officer or the responsibilities assigned to, or shared among, the DAB's operational unit leaders. Regardless, there should be a mechanism to allow direct reporting to the board or its established committees.

23. The risk management function should include:

    a. Clearly defined and documented roles and responsibilities that are reviewed and approved by the board on a frequent basis;
    b. A sound and effective risk management framework, including developing (with the support of operational unit leaders) policies, procedures and internal controls promoting the timely identification, assessment, monitoring and reporting of material risks;
    c. Key policies (e.g., risk policy, cybersecurity policy, customer private key storage policy and policies required under the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008 (POCR)) and effectiveness and compliance assessments with established benchmarks, such as

risk appetite and risk tolerance limits;

d. Measurement techniques, such as benchmarking or stress and scenario testing;
e. Regular review of the risk management techniques employed in light of changing operational, regulatory and market developments to ensure continued effectiveness and adoption of international best practice; and
f. Operation policies for the transfer of assets between wallets, which requires additional signatures from senior management based on the amount being transferred.

24. Risk management, risk identification, risk assessment, risk monitoring and risk reporting are critical for an effective risk management framework. As such, the DAB must implement these in an effective manner for the benefit of the DAB's stakeholders and to support its business objectives.

VI. CLIENT DUE DILIGENCE AND MONITORING

25. Industry participants, including clients, have the potential to adversely impact a jurisdiction's reputation and bring harm to society at large. Accordingly, the DAB must have procedures in place to ensure that proper due diligence is carried out before a decision is made to act for any new client. At a minimum, the DAB needs to be able to comply with the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008, the POCR and the Anti-Terrorism (Financial and Other Measures) Act 2004, together with any other relevant legislation that may come into force from time to time.

26. The duty of vigilance includes verification, recognition and reporting of suspicious transactions; the keeping of "know your client records"; and delivering the appropriate anti-money laundering training to all staff. The DAB must ensure that its procedures enable it to determine and verify the true identity of customers requesting its services. Copies of photo identification such as a driver's licence or passport should be retained in compliance with the Proceeds of Crime Act 1997 and relevant guidance notes and codes. The DAB must undertake due diligence checks on clients to protect against illegal activity, including money laundering and terrorist financing.

27. Where appropriate, measures that the DAB should consider putting in place to minimise the risk of abuse, include (depending upon client risk ratings) appropriate standard rules relating to maximum individual transaction sizes for its different digital asset services. In such cases, the DAB should have the ability to collate and aggregate individual transactions that may form part of a larger transaction and may be intended to avoid standard limits or reporting requirements.

28. The DAB must maintain detailed records for both sides of a transaction that include: information to identify the parties, the public key addresses or accounts involved, the nature and date of the transaction, and the amount transferred. The DAB must monitor

transactions for the purpose of detecting those that lack originator or beneficiary information and take appropriate measures. These measures may include taking action to freeze an account or to prohibit conducting transactions with designated persons and entities.

29. As part of protecting its clients and the jurisdiction's reputation, the DAB should have policies related to market manipulation and the appropriate use of its products and services. Where the DAB suspects or detects abuse, such as spoofing or wash trading, the DAB should report such abuse to the Authority and take the appropriate action, including account closure and termination of the business relationship with the offending party.

VII. INTEGRITY AND ETHICS

30. The DAB must conduct its business with integrity at all times, acting with due care, skill and diligence. It must deal fairly with all clients and seek to ensure that clients are not misled as to the service being provided and the DAB's duties and obligations.

VIII. DISCLOSURE OF INFORMATION

31. A DAB should implement industry best standards of disclosure and operational transparency. At a minimum, there must be adherence to legally required disclosures in the jurisdictions in which it operates. Statements are to be designed to assure the integrity of the client accounts and permit clients to identify any erroneous or unauthorised transactions, withdrawals or balances.

    a. Customer Statements: Statements must be available at least quarterly to clients upon request and must include:
        i. Timeframe of statement activity;
        ii. All transactions specific to a client's account with dates and transaction amounts of corresponding transactions;
        iii. Distinct balances (provided in the unconverted digital asset unit); and
        iv. Valuation of assets if required for each digital asset type.
    b. Corporate Actions: Any action taken by a DAB that impacts existing agreements with clients related to the custody of their assets must be disclosed to the client.
    c. Digital Asset Specific Disclosures: DABs must clearly disclose intent and obligations pertaining to airdrops, forks, metacoins, coloured coins, side chains, dividends, splits or other digital asset derivatives. DABs must also clearly disclose responsibilities for ascertaining or taking action with respect to calls, conversions, votes, exchanges, maturities, tenders or other matters relating to assets.
    d. Changes to Account Information: A DAB should notify clients of any changes that are made to the client's account information.

32. Any obligation to observe the confidentiality of information communicated by clients must be adhered to by the DAB (including its shareholders, directors, officers, senior executives, employees, outsourced partners, etc.) unless the DAB is given relevant consent, is required by applicable law to disclose information or provides information in accordance with the terms of the client constitutional documents. Accordingly, persons who have access to the DAB's confidential information should be advised in writing upon engagement. Further, the DAB should provide periodic reminders thereafter of confidentiality issues.

33. To comply with its duty to uphold integrity and ethics, the DAB's communication with clients and prospective clients must be a clear and fair representation. This includes marketing and promotional material. The DAB's public platform or materials provided to prospective clients prior to entering into an arrangement must include details of the board, the chief and senior executive team, head office (and registered office, if different), a description of its complaints procedure, and arrangements in case of business failure. The DAB must disclose to clients any material business changes that impact clients.

34. A DAB is required to disclose the methodology related to its asset valuation calculations and, when possible, use recognised benchmarks or observable, bona fide, arms-lengths market transactions. When transaction prices are not readily available or recent enough, bid quotes may be used, but attention should be paid to quote size and overall liquidity conditions.

35. A DAB should take extra care where the current market value of an asset is a conditional element of the transaction being executed. A DAB must ensure adherence to its client agreement and industry best practices. When executing a conditional transaction, a DAB should also disclose the source of the asset valuation and the unit of valuation to the client and all signatories of the transaction. The unit of valuation should be the same as the unit of the asset taken under custody.

36. For transparency purposes, the DAB must also ensure that its status as a licensed undertaking is disclosed in all advertisements and correspondence. The following wording is suggested:

    "Company X is licensed to conduct digital asset business by the Bermuda Monetary Authority."

37. Customer service level agreements must be prominently and clearly communicated to clients. DABs must demonstrate competence in meeting service level agreements, especially in relation to fund access upon deposit and withdrawal requests.

IX. BUSINESS OVER THE INTERNET

38. Delivery of disclosure documents and other information

The DAB, which uses the internet to communicate with and send informational material to customers and potential customers, must provide the same disclosure about their firm, products or services that would be provided in a paper-based medium so that consumers can fully evaluate the risk and value of the services/products. The DAB may deliver the necessary disclosure documents and other information electronically where a consumer has given informed consent to this form of delivery.

The DAB must pay particular attention to ensure that all important information, including any disclosures required under the Digital Asset Business (Client Disclosure) Rules 2018, are prominently displayed and easily accessible by customers and potential customers.

39. Communications and customer orders

The DAB must ensure that its systems have sufficient operational integrity and that it has adequate personnel to handle internet communications, electronic transmission of orders and trading information to maintain appropriate service standards as disclosed to its clients or, if no specific service standard is disclosed to its clients, as can be reasonably expected from its clients.

40. Record-keeping

Record-keeping requirements applicable to the DAB also apply to internet transactions.

X. PRODUCT DUE DILIGENCE

41. Where a DAB seeks to introduce a new product or service, or materially modify an existing product or service, such DAB shall be required to carry out appropriate Product Due Diligence (PDD) in relation to said product or service and ensure that risks identified by the PDD have been appropriately weighted against the business risk appetite and mitigated prior to implementation of the new product.

42. PDD must be documented and include, at a minimum, an evaluation of the following:

- Product or service details
- Product or service intended usage
- Product or service risk profile
- Targeted customers
- Evaluation of risks to the DAB
- Evaluation of risks to customers
- Anti-money laundering and anti-terrorist financing implications

- Marketing strategy
- Fee model
- Internal training
- Customer training
- Potential conflicts of interests
- Systems requirements
- Cyber risk
- Impact on staffing
- Legal implications

PDD must be reviewed internally by the appropriate members of the executive team (e.g., chief compliance officer, chief risk officer) or a committee formed by the DAB with the appropriate delegated authority. The review should be appropriately documented and may be required by the Authority during normal supervision or following the material change to the business notification filed with the Authority under section 22 of the Act.

43. PDD should be reviewed periodically upon a frequency commensurate with the nature, scale, complexity and risk profile as determined by the DAB but not less than annually.

44. Once a new product or service, or a material change to a product or service, is introduced, follow-ups are required and should be documented, inclusive of but not limited to:
    a. Monitoring of customer complaints related to the product or service;
    b. Ongoing training; and
    c. Monitoring of compliance with any restrictions imposed on the product or service by the Authority or the DAB itself.

XI. INTERNAL MANAGEMENT CONTROLS

45. The board and the chief and senior executives must review and assess the effectiveness of the internal reporting and operating controls. Any material deficiencies must be documented, and resolution measures should be implemented in a timely manner. The board and the chief and senior executives should ensure the implementation of policies and procedures requiring that internal control weaknesses are reported directly to the board and chief and senior executives.

11.1 Segregation and protection of client assets

46. Section 18 (1) of the Act directs a DAB to place client assets in a trust with a qualified custodian, have a surety bond or indemnity insurance, or implement other arrangements as the Authority may approve as a basis to ensure that any assets belonging to clients are kept segregated from the DAB's own assets and to ensure the return of client assets in the event the DAB is placed into liquidation, becomes insolvent or is a victim of theft.

47. While keeping client assets separate from its own assets, the DAB may commingle

client assets together (i.e., assets belonging to one of its clients with assets belonging to other clients) where such would benefit clients; however, proper accounting and reconciliation practices must be in place to accurately allocate each holding to the respective client.

48. The DAB must have mechanisms in place to assess its liquidity needs, including sums required for trading and other client transaction types. These mechanisms must be used to inform the DAB's client private key storage policy. The client private key storage policy should require that the majority of client private keys, not required for client transactions, should be held in cold storage to mitigate against client loss arising from cyberattacks. The Authority also expects that only a minimal balance should be kept in hot storage and that the mechanism and thresholds for transfer between hot, cold and other storages should be well documented and audited.

11.2 Competent and effective management

49. The DAB should have competent management commensurate with the nature, scale, complexity and risk profile of its business. The DAB must also have appropriate management resources to control the affairs of the licensed business, including ensuring compliance with legal obligations and standards under the Code.

11.3 Delegation

50. The board may delegate the administration and other duties to directors, chief and senior executives, employees or committees as it deems appropriate. When doing so, decisions should align with authorisation and signing powers outlined in policies and procedures, and regard must also be given to stakeholder protection risks and applicable laws.

11.4 Accounting and other record-keeping

51. Appropriate records must be kept and preserved in Bermuda. These records will at least include information for the DAB to effectively carry out its functions and comply with applicable law. Systems must be in place to ensure that decision-makers, regulators, clients and other relevant stakeholders can receive requisite information in a timely manner. This should include the identity of shareholders, directors, officers or business partners. In addition, records of account and client transactions must be maintained in accordance with the applicable law.

52. The DAB's accounting and record-keeping systems must support its compliance with regulatory reporting, such as the annual statutory and other returns or other reporting that the Authority may require on an ad hoc basis in fulfilment of the Authority's regulatory oversight responsibilities.

11.5 Adequate personnel

53. The DAB must have available suitable numbers of staff who are appropriately trained and competent to discharge their duties effectively. The DAB should ensure that the responsibilities and authority of each staff member are clear and appropriate given their qualifications and experience, and that staff receive the necessary training appropriate for their roles.

54. The DAB should ensure that it has in place systems, controls, policies and procedures to ensure that staff members perform their duties in a diligent and proper manner. It is important that staff understand and comply with the established systems, policies and procedures, including those dealing with new business acceptance, financial transactions and staff training.

11.6 Cyber risk

55. In many respects, DABs are susceptible to risks such as cyber threats or systems failure. The Code should be read in conjunction with the Digital Asset Business Custody Code of Practice and the Digital Asset Business Operational Cyber Risk Management Code of Conduct (Cyber Risk Management Code). The Cyber Risk Management Code establishes duties, requirements, standards and procedures to be complied with in relation to operational cyber risk management, and it applies to all licensed DABs.

11.7 Internal audit function

56. Sound practice requires the implementation of the "three lines of defence", with the first line being risk taking, the second being risk control and compliance, and the third being the internal audit. As such, the DAB must have an internal audit function, which should:

    a. Be segregated and staffed by persons adequately independent of operational functions, including risk management, compliance, operations and finance;
    b. Have clearly defined and documented charters, roles and responsibilities that are reviewed and approved by the board on a regular basis and that demonstrate the independence and separation of the function;
    c. Document material policies and procedures to be reviewed and approved by the board;
    d. Prepare an internal audit plan to ensure assessment of governance and controls of key risk areas at appropriate intervals, taking into consideration the nature, scale, complexity and risk profile of the DAB (the internal audit plan should be reviewed at least annually and approved by the board of directors);
    e. Have unrestricted access to all areas of the organisation, including access to any records held by third-party service providers;
    f. Examine operational practices to ensure the adequacy and effectiveness of governance, risk management, policies, procedures and controls;
    g. Report governance and control deficiencies directly to the board or a committee appointed by the board;

h. Establish a robust mechanism to monitor deficiencies until remediation efforts are completed and report remedial progress to the board at regular intervals, taking into consideration the level of risk involved;
i. Have appropriate authority within the organisation to ensure management addresses any internal audit findings and recommendations with respect to the adequacy and effectiveness of governance, risk management, policies, procedures and controls;
j. Have sufficient resources and fit and proper staff to carry out duties and responsibilities;
k. Have sufficient knowledge and experience to employ methodologies designed to assist the DAB in identifying key risks; and
l. Assist the board in identifying areas for improvement.

11.8 Compliance function

57. Regulatory and other requirements (such as internal policies and procedures) are imposed for the protection of the DAB itself, clients and stakeholders more widely. The establishment of a function focused on how well the DAB adheres to the varied requirements is valuable. The DAB must develop a function to assist it in monitoring and evaluating its compliance with jurisdictional laws and regulations, internal controls, policies and procedures. The compliance function should also promote and sustain a corporate culture of compliance and integrity.

58. The compliance function should include:

a. Policies, procedures and processes documenting compliance with the risk management framework, legal and ethical conduct, applicable laws, rules and standards;
b. A system of compliance monitoring and testing, including a plan to address any deficiencies or non-compliance that may be identified; and
c. Training programmes for staff about compliance issues, and also a mechanism for staff to report confidentially concerns regarding compliance deficiencies and breaches.

11.9 Self-assessment

59. The DAB must have a comprehensive and integrated, forward-looking view of all material and reasonably foreseeable risks that arise from its business model and interaction with the wider environment. This allows a more informed assessment of the appropriateness of its business strategy and enhances its ability to position itself for future success and sustainability. The DAB must, therefore, develop policies, processes and procedures to assess all of its material and reasonably foreseeable risks over its forward-looking planning horizon and self-determine its capital (both quality and quantity), liquidity and resourcing needs to inform its business strategy. The risk self-assessment must be performed at least annually and reported to the Authority. The DAB

should be guided by the proportionality principle in establishing the risk self-assessment framework. Minimally, the assessment should:

a. Be an integral part of the DAB's risk management framework;
b. Be clearly documented, reviewed and evaluated regularly by the board and the chief and senior executives to ensure continual advancement in light of changes in the strategic direction and market developments;
c. Cover both (i) all material and reasonably foreseeable risks and (ii) a forward-looking time horizon deemed appropriate by the board, having regard for the dynamics of the digital asset business industry and wider relevant influences; and
d. Ensure an appropriate oversight process whereby material deficiencies are reported on a timely basis, and suitable actions are taken.

60. The DAB must ensure the fitness and propriety of key individuals overseeing and performing the assessment; this includes third-party service providers, if applicable, assisting with the assessment process.

11.10 Fees

61. The DAB is expected to exhibit proper transparency in its dealings with clients and potential clients and to act ethically and with integrity at all times. Terms of business, including fees and commissions for its different services, must be explicitly disclosed prior to transactions, and any changes promptly brought to the attention of customers to ensure that there is no misunderstanding with regard to transaction charges and other fees.

11.11 Client agreements

62. To ensure clients are dealt with fairly and are informed, the DAB must disclose terms of business with each prospective client and keep a record of the terms of the agreement with each client, including evidence of the client's agreement to those terms. That agreement should include, but not be limited to, the following provisions:

a. Clear description of the services to be provided, the fees to be charged, and the manner in which fees are expected to be paid;
b. General description of how and by whom requests for action are to be given;
c. General description of any provisions for the termination of the agreement and the consequences of termination; and
d. Statement that the DAB is licensed by the Authority, including the type of licence issued as well as the activities(s) allowed under the said licence.

11.12 Responsibility to clients and client complaint procedures

63. The DAB must ensure that its business is conducted in such a way as to treat its clients fairly, both before the inception of the contractual arrangement and through to the point at which all obligations under a contract have been satisfied. The DAB must establish

and implement policies and procedures to ensure that this occurs.

64. The DAB must ensure that the client complaints are properly logged and dealt with in a timely manner. A record of the details of the complaint, the DAB's response and any action taken as a result should be maintained.

11.13 Conflicts of interest

65. Conflicts naturally arise in the course of business and may be exploited on account of information asymmetry. The DAB must ensure it has policies and procedures to mitigate conflicts and to avoid harm to clients and stakeholders more widely, including policies and procedures regarding disclosing relevant information. The DAB needs to implement internal rules and procedures for dealing with conflicts of interest. Where conflicts cannot be avoided, the DAB must seek to ensure that the interests of clients are not damaged through undisclosed conflicts of interest.

66. This includes whether the conflict arises directly in the course of its own role or, as relevant, between the DAB and its service providers or, for example, between different classes of clients.

67. The nature and relative market cap of the digital asset business industry inherently exposes it to arbitrage and market valuation manipulation. With information asymmetry and global connectivity, the DAB's board, officers or staff may at times be positioned to exploit opportunities at the expense of stakeholders. The conflict of interest policies and procedures must also include measures that would prevent market manipulation such as insider trading, pump and dump or other schemes that may bring harm to clients.

11.14 Operational Risk Incident Reporting

68. A risk incident is defined as any interruption to an executed operational procedure. The cause may be known or unknown. In the event of a risk incident, a report must be generated documenting the following:

    - Known cause of the incident
    - Impact of the incident
    - Incident resolution
    - The timeline of the incident, including the duration of time to resolve the incident

    This report must be disclosed to both senior leadership and the board, and referenced for future revisions to the Operational Risk Management documented policies and procedures.

    In the event the risk incident results in revisions or additions to standard policies and procedures, the operational risk function must establish a timeline for complying with

the necessary changes and must document the compliance of meeting the goal in a timely manner.

XII. OUTSOURCING

69. While the DAB may outsource certain important business roles (such as asset management, custodial services, cyber security, compliance and internal audit) to third parties or affiliates, such action does not remove the responsibility from the DAB to ensure that all the requirements of the Act and related legislation, and this Code, are complied with to the same level as if these roles were performed in-house.

70. Where the DAB outsources roles, either externally to third parties or internally to other affiliated entities, the DAB must ensure that there is oversight and clear accountability for all outsourced roles as if these functions were performed internally and subject to the DAB's own standards on governance and internal controls. The DAB should also ensure that the service agreement includes terms on compliance with jurisdictional laws and regulations. Service agreements should not prohibit cooperation with the Authority or the Authority's access to data and records in a timely manner.

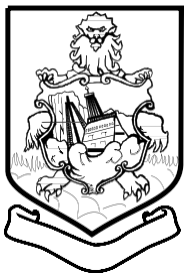
71. Where the DAB has outsourced a role or is considering outsourcing a role, the board must assess the impact or potential impact on the DAB. The DAB must not outsource a role that is reasonably expected to adversely affect the DAB's ability to operate prudently. These considerations include where outsourcing is reasonably expected to:
    a. Adversely affect the DAB's governance and risk management structures;
    b. Unduly increase operational risk;
    c. Affect the Authority's ability to effectively supervise and regulate the DAB; and
    d. Adversely affect client protection.

XIII. COOPERATION WITH REGULATORY AUTHORITIES

72. The DAB is expected to deal openly and in a spirit of cooperation with the Authority and any other relevant regulatory authorities.

73. The DAB should also ensure that any contracts or agreements that it enters into does not, intentionally or otherwise, impede the Authority's ability to carry out its supervisory or regulatory obligations in relation to the DAB. These contracts or agreements should contain a provision that ensures that any outsourced vendors are aware of their role in assisting the DAB in meeting its obligations under the Act and related legislation, and this Code.

***



BERMUDA

DIGITAL ASSET BUSINESS (CYBER RISK) RULES 2022

BR [ ] / 2022

The Bermuda Monetary Authority, in exercise of the power conferred by section 7 of the Digital Asset Business Act 2018, makes the following Rules:

Citation

1 These Rules may be cited as the Digital Asset Business (Cyber Risk) Rules 2022

Definitions

2 In these Rules –

"Act" means the Digital Asset Business Act 2018;

"Authority" means the Bermuda Monetary Authority established under the Bermuda Monetary Authority Act 1969;

"Chief information security officer" means the senior executive, by whatever title called, appointed by the licensed undertaking to oversee and implement its cyber security programme and enforce its cyber security policies.

Cyber Risk Return

3 (1) Class F licence holders shall annually file with the Authority a written cyber risk return whereas Class M and Class T licence holders shall file such return on the date specified in their licence.

(2) The cyber risk return referred to in subparagraph (1) shall be in such form as the Authority may direct and shall be set out on the website of the Authority: www.bma.bm.

Declaration

4 Every cyber return made by a licensed undertaking under paragraph 3 shall be accompanied by a declaration signed by the chief information security officer and a senior executive or director of the licensed undertaking, declaring that to the best of their knowledge and belief, the return is accurate in all material respects.

Made this X day of [MONTH] [YEAR]

Chairman
Bermuda Monetary Authority

[Operative Date: X MONTH YEAR]