BERMUDA MONETARY AUTHORITY

DIGITAL ASSET BUSINESS ACT 2018

CODE OF PRACTICE

MAY 2021

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 thinks 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, complexity and 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.

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:

    i 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)
    ii 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)
    iii 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 the interests of clients. 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.

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:

    i Act in good faith and honestly and reasonably exercise due care and diligence
    ii Ensure the interests of clients are protected
    iii Exercise independent judgment and objectivity in their decision-making

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

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:

i. 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
ii. 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.
iii. Board committees (where required) to provide oversight of key operational areas, including finance and investments
iv. Policies and procedures to ensure adequate board oversight of the chief and senior executives
v. Processes for the engagement and dismissal of the chief and senior executives and third-party service providers
vi. Policies and procedures to manage and mitigate conflicts of interest
vii. 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
viii. Clearly defined charters, roles and responsibilities for the board, committees, chief and senior executives, and other key employees
ix. Business and operational strategies, plans, budgets, and significant policies and procedures, including those surrounding oversight
x. 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
xi. 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)

xii. 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

xiii. 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

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:

xiv. 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

xv. Assisting the board to develop and implement an appropriate control environment, including those around reporting and security systems

xvi. Providing recommendations on strategic plans, objectives and key policies and procedures to the board for evaluation and authorisation

xvii. 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

xviii. Supporting oversight of both internal control functions (e.g., risk management, internal audit and compliance) and external third-party services

xix. Ensuring that key functions assigned corporate governance responsibilities are supported with adequate resources to execute and discharge their duties

xx. 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

xxi. 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 conduct and performance of the DAB, 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. 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 his/her duties pursuant to the Act in an efficient and effective basis, 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 practice on risk management and internal controls. This includes ensuring the fitness and propriety of individuals responsible for the management and oversight of the framework.

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:

    i. Clearly defined and documented roles and responsibilities that are reviewed and approved by the board on a frequent basis
    ii. 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
    iii. 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
    iv. Measurement techniques, such as benchmarking or stress and scenario testing

v. 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
vi. 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 (AML) 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 and/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 that 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 duties and obligations of the DAB.

VIII. DISCLOSURE OF INFORMATION

31. 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.

32. 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.

33. 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."

IX. BUSINESS OVER THE INTERNET

34. **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 shall 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.

35. **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.

36. **Record-keeping**

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

X. PRODUCT DUE DILIGENCE

37. 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.

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

i. Product or service details
ii. Product or service intended usage
iii. Product or service risk profile
iv. Targeted customers
v. Evaluation of risks to the DAB
vi. Evaluation of risks to customers
vii. AML and anti-terrorist financing implications
viii. Marketing strategy

ix. Fee model
x. Internal training
xi. Customer training
xii. Potential conflicts of interests
xiii. Systems requirements
xiv. Impact on staffing
xv. Legal implications

PDD shall 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.

39. 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.

40. 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:

i. Monitoring of customer complaints related to the product or service
ii. Ongoing training
iii. Monitoring of compliance with any restrictions imposed on the product or service by the Authority or the DAB itself

XI. INTERNAL MANAGEMENT CONTROLS

41. 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.

Segregation and protection of client assets

42. Section 18 (1) of the Act directs a DAB to ensure that any assets belonging to clients are kept segregated from the DAB's own assets. The DAB may place client assets in a trust with a qualified custodian, have a surety bond or indemnity insurance, or implement other arrangements to ensure the return of client assets in the event the DAB is placed into liquidation, becomes insolvent or is a victim of theft. While keeping separate from its own, the DAB may commingle client assets where such would benefit clients; however, proper accounting must be in place to accurately allocate each holding to the respective client.

43. 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.

Competent and effective management

44. 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.

Delegation

45. 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.

Accounting and other record-keeping

46. 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.

47. 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.

Adequate personnel

48. 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 his/her qualifications and experience, and that staff receive the necessary training appropriate for their roles.

49. 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.

Cyber security programme

50. In many respects, DABs are susceptible to risks such as cyber threats or systems failure. Accordingly, the DAB must have a comprehensive cyber security programme that is commensurate with the nature, scale complexity and risk profile of its business; including a documented cyber security policy.

51. The DAB must implement a written cyber security policy setting forth the DAB's policies and procedures for the protection of its electronic systems and client and counterparty data stored on those systems. The policies must be reviewed and approved by the DAB's board at least annually.

52. The cyber security policy must minimally address the following areas:

    i. Information security
    ii. Data governance and classification
    iii. Access controls
    iv. Business continuity and disaster recovery planning and resources
    v. Capacity and performance planning
    vi. Systems operations and availability concerns
    vii. Systems and network security
    viii. Systems and application development and quality assurance
    ix. Physical security and environmental controls
    x. Customer data privacy
    xi. Vendor and third-party service provider management
    xii. Monitoring and implementation of changes to core protocols not directly controlled by the DAB, as applicable
    xiii. Incident response

53. Further, the DAB must designate a qualified employee to serve as its chief information security officer responsible for overseeing and implementing the DAB's cyber security programme and enforcing its cyber security policy.

54. The DAB must employ adequate cyber security personnel to manage its cyber security risks. The DAB must require personnel (and provide opportunity and resources) to remain current in changing cyber security threats and countermeasures.

55. An effective cyber security programme should be able to ensure the availability and functionality of the DAB's electronic systems, and to protect both those systems and any sensitive data stored on those systems (including customer assets) from unauthorised access, use or tampering. The programme will also need to address risks arising from third-party vendors where there is system connectivity, and include policies related to hot and cold client private key storage.

56. Further, the cyber security 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.

57. In summary, at a minimum, the DAB's cyber security programme will be required to satisfy five core functions:

    i. Identify internal and external risks
    ii. Protect licensee electronic systems and the information stored on those systems
    iii. Detect system intrusions and breaches
    iv. Respond to a detected event and mitigate negative effects
    v. Recover from operational disruption to the normal course of business

58. The DAB must annually commission an external independent audit of its cyber security programme. The external auditor's report must detail the review of the DAB's business processes, systems, policies and dependencies/relationships with the systems of third-party partners and affiliates to confirm that control measures are adequate to ensure consistent compliance with the Act, related Rules and this Code.

59. The DAB must also be proactive in alerting the Authority to any significant developments relevant to its staffing or to its systems and controls environment. This includes any failure or breach of its systems that involve the loss of, the unlawful destruction of or unauthorised access to any personal identifiable information that it holds on its clients or any assets that it holds on behalf of its clients.

Internal audit function

60. 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:

    i. Be segregated and staffed by persons adequately independent of operational functions, including risk management, compliance, operations and finance
    ii. 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

iii. Document material policies and procedures to be reviewed and approved by the board
iv. 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)
v. Have unrestricted access to all areas of the organisation, including access to any records held by third-party service providers
vi. Examine operational practices to ensure the adequacy and effectiveness of governance, risk management, policies, procedures and controls
vii. Report governance and control deficiencies directly to the board or a committee appointed by the board
viii. 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
ix. 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
x. Have sufficient resources and fit and proper staff to carry out duties and responsibilities
xi. Have sufficient knowledge and experience to employ methodologies designed to assist the DAB in identifying key risks
xii. Assist the board in identifying areas for improvement

Compliance function

61. 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.

62. The compliance function should include:

i. Policies, procedures and processes documenting compliance with the risk management framework, legal and ethical conduct, applicable laws, rules and standards
ii. A system of compliance monitoring and testing, including a plan to address any deficiencies or non-compliance that may be identified

iii. Training programmes for staff about compliance issues, and also a mechanism for staff to report confidentially concerns regarding compliance deficiencies and breaches

Self-assessment

63. 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:

    i. Be an integral part of the DAB's risk management framework
    ii. 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
    iii. 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
    iv. Ensure an appropriate oversight process whereby material deficiencies are reported on a timely basis and suitable actions are taken

64. 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.

Fees

65. 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.

Client agreements

67. 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:

i. Clear description of the services to be provided, fees to be charged and the manner in which fees are expected to be paid
ii. General description of how, and by whom, requests for action are to be given
iii. General description of any provisions for the termination of the agreement and the consequences of termination
iv. 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

Responsibility to clients and client complaint procedures

68. 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.

69. 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.

Conflicts of interest

70. 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 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.

71. 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.

72. 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.

XII. OUTSOURCING

73. 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.

74. Where the DAB outsources roles, either externally to third parties or internally to other affiliated entities, the board 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 board should also ensure that the service agreement includes terms on compliance with jurisdictional laws and regulations. Agreements should not prohibit cooperation with the Authority or the Authority's access to data and records in a timely manner.

75. Where the board has outsourced a role and/or is considering outsourcing a role, the board must assess the impact or potential impact on the DAB. The board 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:
    i. Adversely affect the DAB's governance and risk management structures
    ii. Unduly increase operational risk
    iii. Affect the Authority's ability to effectively supervise and regulate the DAB
    iv. Adversely affect client protection

XIII. COOPERATION WITH REGULATORY AUTHORITIES

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

77. The DAB should also ensure that any contracts or agreements that it enters into does not intentionally, or otherwise, frustrate the Authority's ability to carry out its supervisory or regulatory obligations in relation to the DAB.

***