BERMUDA MONETARY AUTHORITY

GUIDANCE NOTE

DIGITAL ASSET BUSINESS

GUIDANCE FOR PROSPECTIVE APPLICANTS FOR LICENSING

September 2025

This document is intended for the use of applicants seeking a Digital Asset Business license under the Digital Asset Business Act, 2018.

Table of Contents

I. INTRODUCTION

1. The Bermuda Monetary Authority (BMA or the Authority) has issued this Guidance Note (GN) with the intention to set out its clear expectations for applicants seeking a license under the Digital Asset Business Act, 2018 (Act).

2. Within this GN, the Authority seeks to address the wide diversity of businesses that may seek to be licensed under the Act. It incorporates responses to frequently asked questions about the Digital Asset Business (DAB) framework and will be periodically updated to reflect evolving requirements and supervisory practices. While this GN outlines application expectations to support prospective applicants through the licensing process, it is not intended as post-licensure supervisory guidance. The Authority encourages applicants to pay close attention to this GN to ensure they have a clear understanding of regulatory expectations and can efficiently navigate the application process.

3. The rules, regulations, statement of principles, codes and guidance notes have been issued in accordance with specific sections of the Act (collectively referred to as the 'DAB Regulatory Framework') that prescribe certain requirements for businesses that operate within the digital asset space. The DAB Regulatory Framework, alongside this GN, provides clarity on the minimum standards that should be adhered to by all applicants. The DAB Regulatory Framework can be accessed on the Authority's official website (www.bma.bm). This GN should not be construed as legislation or binding rules. Instead, it provides a non-exhaustive overview of the minimum information and standards the Authority expects from applicants.

4. Applicants are advised to use their discretion when reviewing the guidance provided in this document. This GN provides a general framework for all DAB applicants. However, the Authority applies a proportionality principle when reviewing applications. This means that regulatory expectations will vary based on:

    I. The license class being sought (Class T, M or F); and

    II. The nature, scale, complexity and overall risk profile of the proposed business.

5. Prospective applicants should ensure their submissions align with both the regulatory standards for their license class and the expectations outlined in this GN. Before preparing an application, applicants should thoroughly review both this GN and the specific requirements outlined in the application form, which is available on the Authority's website. The depth and detail of information provided should be proportionate to the maturity and complexity of the applicant's proposed operations, with more established or complex business models requiring more comprehensive documentation.

II. ARCHITECTURE AND BUSINESS OPERATIONS

2.1 Legal and Operational Architecture

2.1.1 Organisational Structure

6. When applying for a DAB license, applicants should submit comprehensive documentation detailing their organisational structure. This documentation should include a detailed ownership chart that clearly illustrates all intermediary layers between the applicant and the ultimate beneficial owners. The chart should identify all direct and indirect shareholders, and also include their ownership percentages. Those qualifying as 'shareholder controllers'[1] should complete the Personal Questionnaires (PQs) and Institutional Questionnaires (IQs) and submit all supporting documents alongside the application package.

7. The organisational chart should also include all affiliated entities, including those outside the formal group structure and indicate the regulated status of each entity within the structure. For each affiliated entity, applicants should provide information on the country it is established, whether it is active or dormant, its regulated[2] or non-regulated status, the purpose of its operations, and if or how these operations are intended to interact with the Bermuda company.

8. For entities operating within broader group structures, applicants should provide information and available documentation regarding reporting lines, management hierarchy, operational dependencies, shared services arrangements, and intra-group relationships (e.g., financial, leveraging group policies, etc.). The application should clearly articulate the entity's strategic position and role within any broader group structure, highlighting how this alignment supports the entity's business objectives while maintaining appropriate independence.

2.1.2 Legal Vehicle Design and Contractual Relationships

9. Applicants should provide comprehensive details on the specific legal arrangement they intend to deploy for their proposed business. For business models necessitating a bankruptcy remote structure, examples of which include, but are not limited to, a Segregated Account Company (SAC), an Incorporated Segregated Accounts Company (ISAC) or a trust arrangement, applicants should provide detailed information as outlined below. These examples are provided solely for illustrative purposes, based on business models that have employed these structures, as observed by the Authority, and should not be construed as an exhaustive list. Accordingly, if applicants propose to implement any other type of bankruptcy remoteness arrangement, they are required to submit the relevant documentation and address the following points to the extent they are applicable:

    9.1 A rationale for selecting the specific legal vehicle, demonstrating its appropriateness for the proposed business model and alignment with regulatory requirements.

[1] See Section 3(4) of the Act.
[2] For regulated entities, the following details should be provided: regulatory status (e.g., authorisation, registration, or license), permitted licensed activities, license or registration number, and the name of the regulatory body.

9.2 In the case of ISA or ISAC structures, a comprehensive and detailed explanation of how the proposed arrangement will be operationalised should be provided, including precise descriptions of the interactions between entities. For example, this should outline how a SAC will act on behalf of the Segregated Account (SA) and how an ISAC and Incorporated Segregated Account (ISA) will interact. Additionally, the explanation should include specific details regarding the SA/ISA representative(s), such as their roles, responsibilities and any relevant qualifications or authority. Further, it should provide thorough information on the composition, governance structure and decision-making processes of the ISA's board and management members, including their credentials, duties and how they will oversee and support the ISA's operations effectively.

9.3 In the case of trust structures, comprehensive information should be provided on the trust's nature (discretionary/non-discretionary) and the trustee's regulated status[3], as well as its powers and limitations, and the rights of beneficiaries.

10. Applicants are encouraged to provide a bankruptcy scenario simulation demonstrating how the proposed legal structure ensures client assets remain ring-fenced in the event of insolvency. This simulation should (i) illustrate how clients are protected from becoming general creditors to the applicant in a bankruptcy scenario (e.g., a step-by-step description of how client assets would be handled in various distress scenarios) and (ii) demonstrate the effectiveness of asset segregation mechanisms and the bankruptcy remote nature of the structure.

11. All applications should include the complete suite of legal documentation (in draft form) that establishes and governs the bankruptcy remote structure, including but not limited to:

11.1 SAC/SA agreements clearly evidencing that the SAC will be acting for and on behalf of the SA;

11.2 ISAC/ISA intercompany agreements specifying each entity's responsibilities and obligations, as well as any tri-party or multi-party agreements where both ISAC and ISA will be contracting parties, detailing the rights and obligations of each entity;

11.3 Trust deeds and supporting agreements that establish the bankruptcy remote structure, detailing the scope and purpose of the trust, beneficiary rights, governing law of the trust, trustee powers and the trust's duration. These documents should explicitly define the relationship between the applicant and trustee, including governance frameworks and reporting structures, clear delineation of legal and beneficial title over trust assets, decision-making protocols and established communication standards;

11.4 Contractual agreements with all (other) involved parties/functionaries, including investment managers, custodians, brokers and market makers; and

11.5 Legal opinions from qualified counsel on the effectiveness of the bankruptcy remote nature of the structure, particularly when utilising foreign trusts or complex multi-jurisdictional arrangements.

[3] Licence or registration number, and the name of the regulatory body.

12. All documentation in languages other than English should be accompanied by certified translations.

13. Applicants should document accounting and reconciliation processes as essential safeguards for their bankruptcy remote structure. This documentation should outline detailed asset tracking procedures that ensure proper attribution to the correct legal entities, along with reconciliation protocols and schedules that prevent client asset misallocation. The Authority emphasises that while proper accounting and reconciliation are required across all legal arrangements, these practices become even more pertinent in the case of bankruptcy remote structures, as they are critical to ensuring the proper allocation of client assets and maintaining the integrity of the protective arrangement.

2.2 Business Operations

2.2.1 Products and Services

14. Applicants should provide comprehensive details for all proposed business activities. The business plan should include explicit descriptions of all business lines and products, both regulated and unregulated, that applicants intend to offer. This should include a detailed breakdown of the projected number of customers, projected transaction volumes, projected balance sheet exposure (where relevant), and revenue streams for each business line and product offering.

15. Applications should include focused process flow diagrams that specifically address the handling of client assets within each relevant business line. These diagrams should outline key operational steps, highlighting involved functions/entities, such as internal departments, external service providers and relevant technology platforms. Visual representations should clearly show: (i) the flow of client assets between the applicant, its clients, and other entities; (ii) distinctions between on-chain and off-chain transactions; and (iii) key compliance checkpoints. To enhance clarity, applicants are encouraged to indicate decision points, responsibility transitions and whether processes are automated or manual. Each diagram should be accompanied by concise explanatory notes that detail the purpose of each component and clarify relationships between the entities involved.

16. When applicants' business models encompass both regulated and unregulated activities (such as conducting investment business in an ancillary manner[4]), they should provide comprehensive details for all activities, as these collectively impact the overall risk profile and should be integrated across all three Lines of Defence (3LOD). For those seeking exemption under the Investment Business Act 2003 due to their non-registrable status while conducting ancillary investment business, applications should include detailed descriptions of the control and monitoring systems to be implemented for proper threshold monitoring and ongoing compliance verification.

17. Applicants should ensure that their financial projections comprehensively include all business lines, including unregulated activities[5], to provide the Authority with a complete understanding of their proposed operations.

---

[4] In which case the applicant will qualify as 'non-registrable' pursuant to the Investment Business (Non-Registrable Persons) (Designation) Order 2022 (as amended).
[5] Broken down by quarter for the first 12 months.

18. Applicants should submit a detailed product and business line rollout strategy as part of their application. This roadmap should clearly distinguish between offerings that will be available immediately upon licensure and those planned for future implementation. The roadmap should include: (i) a comprehensive timeline with specific launch dates for each product and business line; (ii) detailed descriptions of all initial offerings that will be operational upon license approval; (iii) phased implementation plans for future products and services, including dependencies and contingencies; and (iv) resource allocation projections for each phase of the roadmap.

    Note: The Authority will focus its initial assessment primarily on the products and services intended for immediate launch upon licensure. While future offerings will be considered in evaluating the overall business strategy and risk profile, applicants should note that these planned additions will not be automatically covered by the initial license. Any subsequent introduction of new products, services or business lines will require a material change notification pursuant to section 22 of the Act. This distinction ensures the Authority can properly evaluate whether the applicant has appropriate operational infrastructure, risk management frameworks, compliance procedures, governance policies and staffing levels to support their immediate business activities.

19. In case of vertical integration of activities and functions[6], this integration should be clearly reflected across all assessment areas outlined in the GN.

20. Applicants seeking waivers or modifications under Section 8 of the Act should provide comprehensive supporting documentation with their applications. For example, applicants seeking exemption from the material change notification requirement (Section 22 of the Act) for new digital asset products would be expected to submit a comprehensive policy that clearly defines their selection criteria. This policy should detail the financial, technical and compliance parameters used to evaluate digital assets and outline the procedures for their ongoing monitoring. Similarly, those seeking Section 22 waivers for outsourcing additional functions or changing service providers should demonstrate that their outsourcing and vendor management policies adequately address the selection criteria, due diligence processes and proper governance frameworks. These policies should detail the ongoing monitoring mechanisms for outsourced functions and service providers, including performance metrics, compliance verification procedures and contingency arrangements. The Authority expects all waiver requests to be accompanied by evidence showing how the applicant will maintain regulatory compliance and prudent risk management despite the requested modification.

21. Class M and Class T applicants should submit a graduation plan as a component of their application package. This plan should outline the objectives for the Sandbox testing period that defines in detail what will be tested, developed or refined during this critical phase. For Class M applicants, who are focused on scaling operations, the graduation plan should demonstrate advancements in governance, compliance, and risk management frameworks. For Class T applicants, with a focus is on identifying risks and developing foundational compliance and risk management programs, the graduation plan should emphasise the establishment of basic but robust frameworks essential for future growth and regulation adherence. In all cases, applicants should include well-defined timelines for achieving milestones, measurable deliverables and relevant performance metrics to demonstrate readiness for full licensure.

[6] I.e. when applicants engage, or propose to engage, in multiple functions and activities under 'one roof'.

22. Additionally, all applicants should provide wind-down plans for their operations. For Class M and T applicants, these plans may be more conceptual in nature, outlining the general approach to orderly cessation of activities if testing or development goals are not achieved. However, Class F applicants are expected to submit more detailed and operationally focused wind-down plans. These comprehensive plans should include specific triggering events that would initiate the wind-down process, a detailed inventory of resources required (financial, human and technological), a step-by-step operational sequence for winding down activities, realistic timelines for each phase, and a thorough estimation of associated costs. Class F wind-down plans should also address client asset protection measures, data retention protocols, contractual obligation management, and communication strategies for all stakeholders during the wind-down process.

2.2.2 Customer Base, Jurisdictional Presence and Existing Operations

23. Applicants should clearly specify the jurisdiction(s) in which they operate or plan to operate, including situations where they are part of a group or affiliated entities with existing operations. Where relevant, applicants with proposed operations in multiple jurisdictions should identify and address cross-jurisdictional risks associated with such activities. These risks may include compliance with jurisdiction-specific regulations, trade sanctions, currency restrictions, data protection requirements, and emerging regulations specific to digital assets. A comprehensive assessment should also consider operational, legal and business model implications across all relevant jurisdictions. For applicants that are part of a group or other affiliated entities with existing operations in multiple jurisdictions, this cross-jurisdictional risk assessment should consider any implications to the operations of those affiliated entities. It is recommended to evaluate the cumulative exposure to jurisdictional risks across the group structure and address these risks comprehensively, particularly where interconnected operations or regulatory overlap may arise.

24. Applicants are further expected to describe their proposed monitoring systems and controls (whether automated or manual) for tracking regulatory changes across all relevant jurisdictions. These systems should have well-defined reporting protocols that establish how regulatory developments are documented, escalated internally, and, where required, reported to the Authority. The monitoring framework should include designated responsible parties, clear monitoring frequencies, reliable information sources, and thresholds for determining when regulatory changes necessitate adjustments to the business model.

    Note: The monitoring requirements should be tiered based on the applicant's actual jurisdictional footprint and exposure to regulatory changes. Applicants with limited cross-jurisdictional activity may propose scaled-down frameworks appropriate to their scope, provided they maintain effective mechanisms for identifying and responding to changes in applicable regulations within their operational jurisdictions.

25. Applicants should provide a comprehensive overview of their target customer base in their submission. This should include detailed information on target demographics, clearly distinguishing between (i) non-retail (institutional or sophisticated); and (ii) retail clients, together with anticipated customer volume and an assessment of expected customer sophistication levels. If the target customer base includes sophisticated customers (or similar segmentation), applicants should clearly define the precise eligibility criteria used for said classification (e.g., minimum net worth thresholds, income requirements, trading experience or other relevant qualifiers). If relevant, applicants should describe the processes and procedures they will implement to verify client

eligibility during onboarding and how they will periodically reassess this ongoing status to ensure continued qualification.

26. Applicants with existing operations seeking to migrate customers to their Bermuda-licensed entity should provide comprehensive migration details as part of their application.

    26.1 For applicants where group or affiliated entities have existing customers that will be migrated to the Bermuda entity, documentation should clearly identify the originating entity's relationship to the applicant, detail the legal and operational transfer mechanisms, and outline customer communication and consent processes for the transition to a new service provider.

    26.2 For applicants currently operating directly in another jurisdiction who wish to relocate their operations to Bermuda (where the customer base already belongs to the applicant), documentation should focus on the jurisdictional transition process, including regulatory notifications in the current jurisdiction, contract amendments and service continuity plans during the transition period.

In both scenarios, applications should include a detailed breakdown of the customer base to be migrated, specifying the number and types of customers categorised by classification (retail versus non-retail: institutional/sophisticated), along with their respective business and risk profiles and transaction volumes. The application should contain a thorough migration plan outlining precise timelines, distinct operational phases and a step-by-step process explanation for the transition. Applicants should detail the specific tools, monitoring procedures and reporting mechanisms that will be implemented to track migration progress, including monitoring frequency and key performance indicators. The application should clearly identify the organisational teams responsible for managing and overseeing the migration process, including escalation procedures for addressing potential issues.

Additionally, applicants should explain their approach to customers who will not be migrated. For example, when migrating custodied assets from a group or affiliated entity to Bermuda, applicants should clearly explain the handling of 'unclaimed' client assets (those belonging to clients who do not consent to migration or cannot be contacted). The application should specify whether these assets will be transferred to the Bermuda entity or remain with the original entity. For assets being transferred, applicants should detail comprehensive safeguards and procedures for managing said assets, which should include: multi-channel communication strategies, defined asset retention periods, and legally compliant disposition plans that adhere to regulations in all relevant jurisdictions.

2.2.3 Staffing and Head Office

27. Applicants should provide comprehensive information regarding their staffing resources and future projections as part of their application package. For resources that will be available upon licensure, applications should include a detailed breakdown across all 3LOD (operational management, risk/compliance functions and internal audit). This breakdown should list all staff positions, clearly indicating whether each position is Bermuda-based or outsourced/insourced, and for non-Bermuda-based roles, specify the percentage of time that will be dedicated to Bermuda operations.

28. This information should be accompanied by an organisational chart that visually represents the reporting structure, indicates the number of employees in each function or business unit, and explicitly identifies any external staff sourced from group entities. Where resource sharing agreements or other service level agreements exist, these documents should be submitted as part of the application package.

29. Additionally, applicants should submit a forward-looking staffing roadmap that outlines projected growth following the commencement of operations. This roadmap should detail how staffing will scale in alignment with business expansion, including estimated hiring timelines, key positions to be added, and transitions from outsourced to in-house functions where applicable. When developing these projections, applicants should also consider the Head Office Guidance issued by the Authority.

30. For both current staffing plans and future projections, applicants should demonstrate that their human resources are commensurate with the nature, scale, complexity and overall risk profile of their (proposed) operations. This is particularly critical for entities with vertically integrated functions and activities. Applicants are also encouraged to include in their submission a staffing adequacy assessment that demonstrates how their proposed personnel resources align with their operational complexity, risk profile and business objectives.

31. In their submission, applicants should detail how they plan to meet head office requirements, outlining the factors taken into consideration for determining compliance and the application of the proportionality principle to meet these requirements. To ensure alignment with expectations, applicants are advised to consult the Head Office Guidance available on the Authority's website.

    Note: While Class T license holders are exempt from this requirement, they should nonetheless consider a roadmap demonstrating their planned progression toward fulfilling these requirements, particularly following successful testing and anticipated graduation to a full license.

2.2.4 Outsourcing

32. Applicants should describe all outsourced and insourced functions, accompanied by details for each arrangement. This documentation should clearly identify the nature and criticality of each outsourced function, specifying whether the service provider is a group entity or an external third party. For each outsourced function, applicants should detail the due diligence process conducted during service provider selection, including assessment criteria, evaluation methodologies and findings. The application should also explain how each outsourcing relationship will be managed, including governance structures, escalation procedures and performance monitoring frameworks. This information could be part of the applicant's outsourcing or third-party vendor policy.

33. Applicants should identify and document all interdependencies with key service providers or intragroup functions, particularly where the business model relies heavily on third-party services such as liquidity providers or custodians. For each critical dependency, applications should include an assessment that identifies potential vulnerabilities, outlines mitigation strategies, and establishes contingency plans for service disruptions. Where regulatory codes apply to outsourced functions (such as custody requirements), applicants should provide a detailed gap analysis demonstrating compliance with these codes and explaining how this compliance will be maintained.

34. Applications should identify the specific personnel responsible for managing outsourcing relationships, including both the senior management oversight and operational teams handling day-to-day interactions. This should include information about monitoring protocols, specifying the frequency of reviews, key performance indicators, reporting structures and remediation procedures for addressing service deficiencies. Applicants should demonstrate how they will maintain effective control over outsourced functions while ensuring regulatory compliance and appropriate risk management.

35. All outsourcing and insourcing arrangements should be supported by formal contractual documentation, which should be included in the application package. This includes service level agreements and any other relevant contracts. These documents should clearly define:

    - Service expectations
    - Data access provisions
    - Confidentiality requirements
    - Business continuity arrangements
    - Termination conditions and dispute resolution procedures

    For critical functions, contracts should also specify dedicated resource commitments to the Bermuda entity. Applicants should describe how they will maintain access to timely and accurate records for all outsourced functions, particularly those critical to regulatory compliance and risk management. Additionally, applicants should ensure that the effectiveness of outsourcing arrangements will be subject to review within the entity's audit plan and scope.

36. The Authority will assess outsourcing arrangements in the context of the entity's overall governance framework, with particular attention to whether the arrangements maintain appropriate control and oversight within the Bermuda entity while ensuring operational effectiveness and regulatory compliance.

2.2.5 Insurance

37. Applicants should submit relevant information regarding their proposed insurance coverage as part of their application package. This documentation should detail the specific types of coverage (such as errors and omissions/professional indemnity, directors' and officers' liabilities and crime insurance) and corresponding coverage amounts, supported by either executed insurance contracts or formal quotes. Where insurance has not yet been secured at the time of application, applicants should identify the types of coverage they intend to procure, including estimated coverage amounts and specific timelines for obtaining such insurance. Additionally, applicants should explain how the proposed coverage types and amounts were determined to be adequate and commensurate with their specific business model.

38. While Class T entities are not universally required to maintain insurance coverage, the Authority may determine such coverage necessary based on the nature, scale, complexity and risk profile of the proposed testing activities.

39. For entities utilising group insurance policies, documentation should explicitly identify the Bermuda entity as a named insured party to ensure adequate protection under the policy.

2.2.6 Financial

40. Applicants should provide comprehensive details regarding their funding sources and capital structure. This includes disclosure of all capital contributions, equity investors[7], banking relationships and any loans or debt instruments used to finance operations. For entities with parent company relationships, applicants should disclose any guarantees or financial support commitments from parent or ultimate parent entities. The application should clearly articulate how funding will be deployed to support operational growth, maintain capital adequacy and ensure business continuity.

41. Considering the nature, scale and complexity of the proposed operations, applicants should demonstrate sufficient net assets and an adequate liquidity position to withstand market volatility and operational demands. Class F license applicants are specifically required to propose and justify their capital model, demonstrating how it addresses the full spectrum of risks to which their operations will be exposed –taking into consideration *inter alia* capital requirements for each proposed business line.

42. All applicants should submit detailed financial projections covering a three-year horizon, with quarterly breakdowns for the first 12 months. These projections should include revenue estimates, growth forecasts, cash burn rates and capital adequacy assessments. Projections should be realistic and substantiated by market research, historical data (where available) or comparable business models.

43. Where part of a group, applicants should submit consolidated group financials (audited financial statements and the most recent unaudited management accounts) to allow the Authority to assess the financial standing of supporting entities. For applications involving working capital agreements, convertible notes or any other form of debt instrument, the Authority expects such instruments to be fully subordinated to all other obligations of the applicant. Documentation evidencing this subordination should be included in the application package, along with terms that clearly protect the interests of clients and the overall financial stability of the entity. The subordination arrangements should be legally binding and remain in effect for the duration of the instrument's term.

[7] The capital structure table should be submitted as part of the application package.

III. GOVERNANCE AND THREE LINES OF DEFENCE

44. As part of the application process, all applicants are required to submit documentation outlining their approach to corporate governance, including their proposed 3LOD model. This section specifically addresses these areas, with an emphasis on the second and third lines of defence. In particular, it covers risk management (encompassing operational, credit, liquidity and market risks), compliance, anti-money laundering/anti-terrorist financing (AML/ATF), conduct risk, cyber risk and the internal audit function. The Authority's assessment incorporates a proportional approach, taking into account the class of license being applied for (T, M or F) as well as the nature, scale, complexity and risk profile of the proposed business. The following sub-sections provide detailed information on the Authority's expectations for the applicant's relevant functions, along with specific requirements and guidance designed to ensure compliance with regulatory standards.

3.1 Corporate Governance

45. This section outlines the corporate governance documentation and information required from prospective DAB applicants. All applicants should explain how their proposed governance arrangements reflect the nature, scale, and complexity of their business model, with particular attention to instances where multiple business lines are proposed to be integrated through vertical integration of functions. This approach elevates the applicant's risk profile due to the potential for increased operational complexity and overlaps in responsibilities across business lines. Therefore, applicants pursuing vertical integration should propose a more robust corporate governance framework to mitigate these risks, with a specific focus on managing conflicts of interest that may arise in such integrated structures. Applicants are also expected to outline how governance frameworks will evolve as their business matures.

46. Apart from the documentation and information identified below, all applicants should further provide an organisational chart showing key governance functions, job descriptions for senior management, and an outline of training programs for governance-related roles. For applicants proposing to engage in vertical integration, the organisational chart should clearly outline oversight mechanisms across business lines and detail how governance arrangements will ensure accountability and independence to mitigate potential conflicts of interest. While dual-hatting will not automatically be grounds for refusal during the licensing process, applicants should demonstrate appropriate mitigants to address the heightened risks associated with such arrangements and, more critically, provide a clear plan to reduce or phase out dual-hatting after licensing.

Class-specific documentation requirements

47. Class T licence applicants primarily operate in a testing or innovation stage and are required to submit a simplified corporate governance framework. This includes a basic governance policy detailing the structure of oversight, evidence of at least two qualified directors, and any arrangements with service providers to support governance functions. Board documentation should include a basic charter outlining responsibilities and meeting schedules, along with a simple authority matrix for decision-making. Applicants should also provide an outline for identifying and managing operational risks, alongside planned compliance monitoring activities. Staffing plans should describe key roles, reporting lines and identify individuals performing multiple functions.

As governance limitations are expected during this phase, the submission should acknowledge these constraints and include a timeline for further development as the business matures.

48. Class M licence applicants, which have operations of moderate scale and complexity, are expected to submit a developing corporate governance framework. This includes a comprehensive governance policy, a well-structured board with diversity in skills and experience and detailed descriptions of service provider arrangements. Board documentation should feature a clear charter, outlines of planned committee structures, defined authority matrices for decision-making and established meeting schedules and documentation procedures. A roadmap detailing timelines for advancing governance structures and transitioning to more robust arrangements as the business scales should also be included.

49. Class F licence applicants should demonstrate a mature and sophisticated corporate governance framework. This includes a detailed governance policy, evidence of diverse board composition aligned to a skills matrix, evaluation frameworks for board members, and succession planning for senior management. Board and committee documents should feature charters for both the board and specialised committees (e.g., audit, risk, nomination, HR/governance), detailed authority matrices and methodologies for assessing board effectiveness. Applicants should submit a thorough plan for implementing the 3LOD, including independence safeguards for control functions and resource allocation across each line. Additional requirements include a code of ethics, a conflict of interest policy and procedures for related-party transactions.

3.2 Compliance

50. All applicants should provide a Compliance Policy framework that outlines the objectives and responsibilities of the compliance function, defines the scope of regulations under its purview, and establishes the authority and reporting channels for the function. This document should also clarify the allocation of compliance responsibilities between the compliance function and the first line of defence.

51. Additionally, applicants should outline their methodology for tracking regulatory developments relevant to their business activities, both in Bermuda and in other jurisdictions where they intend to operate. This should include information on how regulatory changes will be identified, assessed and incorporated into the compliance framework.

52. Applicants should also detail how they will identify, evaluate and prioritise compliance risks. This should include the frequency of planned compliance risk assessments and how compliance risks will be documented and monitored. They should also describe how compliance information will flow to senior management, relevant committees and the board (including the types of reports that will be produced, their frequency and the escalation procedures for compliance issues). Finally, applicants should describe how they will ensure staff awareness of compliance obligations throughout the organisation.

Class-specific documentation requirements

53. Class T licence applicants should submit essential compliance documentation, including a basic compliance policy that outlines key areas relevant to their testing activities. This policy should be supported by a streamlined process for monitoring regulatory developments, a high-level approach to assessing compliance risks and a reporting structure designed to ensure that critical compliance

issues are effectively communicated to decision-makers. These submissions do not need to be fully developed; conceptual documentation is acceptable, as long as it is accompanied by a clear roadmap for developing more comprehensive compliance capabilities as the business matures.

54. Class M licence applicants are expected to provide a more structured and comprehensive compliance framework, including clearly defined methodologies to guide their efforts. This submission should include documentation outlining how the compliance function will adapt and evolve as the business grows, along with a more detailed approach to assessing compliance risks. Additionally, applicants should present information about their proposed compliance reporting structure, specifying the frequency and content of reports. A roadmap for strengthening compliance capabilities in preparation for transitioning to a Class F license is also required. Applicants may submit well-developed, high-level documentation outlining their policies, accompanied by clear timelines for finalisation and implementation.

55. Class F licence applicants are required to submit comprehensive compliance documentation that reflects a highly developed and mature compliance function. This includes a formal compliance charter, detailed processes for monitoring regulatory developments across all applicable jurisdictions, and a sophisticated methodology for assessing compliance risks. Additionally, applicants should provide structured documentation outlining formal compliance reporting mechanisms, including established schedules, as well as details on how the effectiveness of the compliance function will be evaluated over time. Class F applicants should also demonstrate that their compliance function is adequately resourced with personnel who possess the relevant expertise necessary to support the entity's operational scope. Specifically, compliance personnel are expected to have sufficient knowledge of applicable regulatory frameworks, as well as a thorough understanding of the applicant's products, services and business model to effectively assess and address compliance risks. For larger and more complex businesses within this category, more detailed submissions are expected, such as specialised compliance teams and dedicated compliance committees that oversee compliance efforts at a granular level.

3.3 Risk Management

56. All applicants should submit a documented risk management framework, outlining their approach to risk management. This document should describe the 3LOD methodology, identify all material risk types relevant to the proposed business model (financial and non-financial) and explain how these risks will be identified, assessed, monitored and mitigated. Additionally, applicants should provide a Risk Appetite Statement that articulates the entity's willingness to accept risk, includes both qualitative statements and quantitative metrics and explains how risk appetite will be translated into operational risk limits. This statement should incorporate Key Risk Indicators (KRIs), including early warning indicators, to monitor and assess risk levels effectively. Furthermore, it should outline the use of traffic light systems or similar frameworks to visually represent risk thresholds, providing clear guidance on when action should be taken.

57. Documentation should also outline the Risk Management governance structure, detailing board and senior management responsibilities for risk oversight, reporting lines for risk management functions, and committee structures (if applicable) with terms of reference. Finally, applicants should submit a Risk Register or equivalent document that identifies key risks facing the proposed business, provides an assessment of their likelihood and impact, and outlines planned mitigation measures. This should further specify the assigned risk owner(s) responsible for overseeing the

management of each risk, the identification date of each risk, proposed escalation procedures for material residual risks, and target deadlines for their resolution.

Class-specific documentation requirements

58. Class T licence applicants should submit a basic risk management document that outlines foundational risk management concepts relevant to their testing activities. This should be accompanied by a simplified risk register identifying key risks during the testing phase and a high-level description of how risks will be monitored and reported to senior management. Additionally, Class T applicants should provide a roadmap for developing more comprehensive risk management capabilities as their business matures.

59. Class M licence applicants are expected to submit a more structured risk management framework document with defined methodologies for risk assessment. This should be supported by a comprehensive risk register covering all material risk areas and documentation of proposed risk monitoring tools and reporting procedures. Class M applicants should also include a clear roadmap for enhancing their risk management capabilities before transitioning to a Class F license.

60. Class F licence applicants should submit a sophisticated, comprehensive risk management framework document with detailed methodologies. This should be accompanied by a detailed risk register with quantified assessments and thorough mitigation strategies, as well as documentation of advanced risk monitoring systems and reporting procedures. Class F applicants should also provide evidence of adequate resources, both technological and personnel, to support the risk management function appropriate for a full license holder.

61. Further to the overarching nature of the previously outlined expectations pertaining to an applicant's risk management function, it is important to underscore the need for a deeper understanding of certain critical risk areas. While the foundational principles and frameworks of risk management apply comprehensively to all aspects of a business, the following sub-sections will provide more detailed and specific expectations in relation to certain key risk areas —namely operational, credit, liquidity and market risk management. These more granular expectations aim to ensure that entities not only adhere to the broader risk management standards but also develop focused strategies and mechanisms tailored to effectively address the unique challenges presented by these distinct categories of risk.

Note: It is important to note that the risks outlined in the following sub-sections are intended as an indicative list only. They do not represent or encompass the full spectrum of potential risks. Applicants are therefore encouraged to conduct a thorough assessment of their proposed operations and identify any additional or unique risks specific to their particular circumstances.

3.3.1 Operational Risk Management

62. All applicants, regardless of license class, should provide an Operational Risk policy that outlines their approach to managing risks arising from inadequate or failed internal processes, people, systems or external events. Additionally, applicants should submit information on Business Continuity Planning, detailing how they will ensure business resilience in the face of operational disruptions.

Class-specific documentation requirements

63. Class T licence applicants should submit a basic Operational Risk policy that identifies key operational risks relevant to the testing environment, along with simplified business continuity considerations appropriate for the testing phase.

64. Class M licence applicants are expected to provide a more detailed Operational Risk policy with defined assessment methodologies. This should be accompanied by a business continuity plan outlining recovery strategies for critical functions and documentation of key operational risk indicators that will be monitored.

65. Class F licence applicants should submit comprehensive Operational Risk management documentation with detailed methodologies. This should include fully developed business continuity and disaster recovery plans with defined recovery time objectives, as well as documentation of operational risk monitoring systems and escalation procedures appropriate for a full license holder.

3.3.2 Credit Risk Management

66. Applicants with credit risk exposure should provide a Credit Risk policy document outlining their approach to identifying, assessing and managing credit risk exposures. They should also submit information on their credit approval process, detailing the proposed methodology for evaluating and approving credit exposures. For business models involving collateralised lending, documentation of collateral management is required, including collateral requirements, valuation methodologies and liquidation procedures.

Class-specific documentation requirements

67. Class T licence applicants should submit a basic credit risk policy that identifies key credit risks relevant to the testing phase, along with an overview of proposed credit approval and collateral management processes appropriate for their limited operational scope.

68. Class M licence applicants are expected to provide a more detailed credit risk policy with defined assessment methodologies. This should be accompanied by documentation of credit approval processes with clear decision-making authorities and information on collateral management practices and liquidation procedures.

69. Class F licence applicants should submit comprehensive credit risk management documentation with detailed methodologies, including a defined credit risk appetite and limit framework that translates strategic objectives into practical operational guidelines. This framework should include clearly defined quantitative and qualitative statements providing measurable boundaries and principles for credit risk-taking activities, supported by appropriate early warning indicators. Additionally, Class F licence applicants should provide a sophisticated credit approval framework with multiple approval levels, detailed collateral management procedures including stress testing of collateral values, and documentation of credit risk monitoring systems and reporting procedures appropriate for a full license holder operating at scale.

Note: These requirements are intended to be proportionate to the Class F applicant's actual credit risk exposure, recognising that Class F licence applicants with minimal credit exposure may not

necessitate the same level of sophistication in their credit risk frameworks as those operating at larger scales or with higher levels of credit activity.

3.3.3 Liquidity Risk Management

70. Applicants with liquidity risk exposure should provide a Liquidity Risk Policy document outlining their approach to identifying, assessing and managing liquidity risk. They should also submit information on their funding strategy, detailing proposed funding sources and diversification strategies. Additionally, applicants should provide documentation of how liquidity positions will be monitored and reported.

Class-specific documentation requirements

71. Class T licence applicants should submit a basic liquidity risk policy that identifies key liquidity considerations during the testing phase, along with a simple funding plan appropriate for the testing environment.

72. Class M licence applicants are expected to provide a more detailed liquidity risk policy with defined assessment methodologies. This should be accompanied by documentation of the funding strategies with consideration given to diversification and information on liquidity monitoring tools and reporting procedures.

73. Class F licence applicants should submit comprehensive liquidity risk management documentation with detailed methodologies. This should include a well-defined liquidity risk appetite and limit framework[8], sophisticated funding strategy with multiple contingency options, documentation of advanced liquidity monitoring systems, and stress testing scenarios specifically designed to address digital asset market liquidity conditions.

3.3.4 Market Risk Management

74. Applicants with market risk exposure should provide a Market Risk Policy document outlining their approach to identifying, assessing and managing risks arising from market movements. They should also submit information on Market Risk Measurement, detailing the methodologies used to measure market risk exposures. For applicants planning to engage in hedging activities, documentation of proposed hedging strategies and effectiveness assessment is also required.

Class-specific documentation requirements

75. Class T licence applicants should submit a basic market risk policy that identifies key market risks during the testing phase, along with a simple market risk measurement approach appropriate for testing activities.

[8] The liquidity risk appetite and limit framework represent a critical component of the applicant's overall strategy and should be operationalised through both quantitative statements (such as by indicating specific metrics and thresholds) and qualitative statements (such as creating principles and guidelines) supported by appropriate indicators that enable effective monitoring. The framework should not operate in isolation but should be informed by stress testing outcomes.

76. Class M licence applicants are expected to provide a more detailed market risk policy with defined assessment methodologies. This should be accompanied by documentation of market risk measurement approaches that consider digital asset volatility and information on proposed hedging strategies, if applicable.

77. Class F licence applicants, particularly those with significant proposed trading activities or proprietary positions, should submit comprehensive market risk management documentation with detailed methodologies. This should include a well-defined market risk appetite (expressed through quantitative limits and qualitative statements that define acceptable levels of market risk exposure), sophisticated market risk measurement approaches potentially incorporating Value at Risk (VaR) or Expected Shortfall methodologies[9], documentation of advanced market risk monitoring systems (including early warning indicators) and stress testing scenarios specifically designed to address digital asset market conditions.

3.4 AML/ATF

78. To assist Regulated Financial Institutions (RFIs) in understanding and complying with Bermuda's Anti-Money Laundering (AML) and Anti-Terrorist Financing (ATF) acts and regulations, the Authority issued comprehensive General Guidance Notes in 2023[10], which replace and supersede earlier guidance notes. Sector-specific guidance notes are issued by the Authority relevant to the sector.

79. Applicants should provide AML/ATF and Sanctions policies and procedures that comply with Bermuda's regulatory framework. These policies and procedures should outline, among others:

- The responsibilities of senior management and internal controls (Chapter 1)
- The risk-based approach (Chapter 2)
- The application of standard and non-standard Customer Due Diligence (CDD) measures (Chapters 3, 4 and 5)
- Sanctions regimes (Chapter 6)
- Ongoing monitoring (Chapter 7)
- Wire transfers (Chapter 8)
- Suspicious activity reporting (Chapter 9)
- Employee training and awareness (Chapter 10)

[9] These methodologies should capture all material sources of market risk, including price risk, interest rate risk, foreign exchange risk and basis risk where applicable.

[10] https://www.bma.bm/viewPDF/documents/2024-06-13-13-28-45-2023-06-12-15-17-06-General-Guidance-Notes-for-AMLATF-Regulated-Entities-Revised.pdf

- Record-keeping (Chapter 11)

80. Applicants' AML/ATF frameworks are expected to demonstrate the applicant's compliance with each regulatory and/or legislative requirement in the AML/ATF regulations. The policies and procedures should be tailored to the applicant's business plan and take into consideration the specific ML/TF risks that the applicant will incur and which should be assessed using the Business ML/TF and Sanctions Risk Assessment (BRA) and be submitted. Applicants can refer to the *Guidance Notes for AML/ATF Regulated Financial Institutions on Anti-Money Laundering and Anti-Terrorist Financing 2023* (AML/ATF RFI Guidance), and the sector-specific Guidance Note for DABs, for further clarification or assistance.

81. As further elaborated upon in a previous Section of this Guidance, applicants should confirm, as part of their application, whether or not they intend to migrate existing clients into the Bermuda RFI, either upon licensure or at a later stage. In the affirmative, they should also provide the relevant details (as outlined above in this Guidance).

82. To the extent the applicant does intend to migrate existing customers into the Bermuda RFI, the following AML bespoke requirements should be in place:

    - A comprehensive Remediation Action Plan/Roadmap for the total customer base that the Company proposes to transfer and detailed customer breakdown (retail and/or institutional)

    - Quarterly Remediation Status/Progress Tracker

    - An assurance of remediated customer files to be performed prior to migration evidencing compliance with the Proceeds of Crime Act 1997

83. In line with the AML/ATF RFI Guidance – applicants should submit a comprehensive BRA. This should include the identification of the applicant's inherent risks of ML/TF and sanctions violations against the relevant ML/TF risk factors (i.e., associated with the products/services offered, the types of customers and associated risks, the delivery channel risk, and the geographical risk associated with the customer base and jurisdictions the applicant intend on operating in considering the specific business model), and should take into consideration the results of Bermuda's National Risk Assessment. The BRA should also document the impact of the applicant's mitigation measures and the consequent residual risks.

84. Individuals appointed as Compliance Officer (CO) and/or Reporting Officer (RO) should possess the necessary competence and expertise with an in-depth understanding Bermuda's AML/ATF Framework evidenced prior to operationalisation of the entity (Section 1.47 of the AML/ATF RFI Guidance). To allow the Authority to assess the competency, fitness and propriety of a CO and/or RO, the applicant should submit:

    - A CV outlining the CO/RO's skills and experience that also highlights the specific AML/ATF roles and responsibilities they have had for which the CO/RO will be responsible

    - Evidence of knowledge of the Bermuda AML/ATF and Sanctions requirements (or information indicating how this will be developed prior to operationalisation)

- Evidence of knowledge and proficiency in a Blockchain Analytics Tool

85. To better understand the Bermuda AML/ATF and Sanctions requirements, the Authority recommends that the applicant's (i) senior management, (ii) CO and (iii) RO undergo the Standard Service Provider Training offered (free of cost) by the Authority, which can be accessed via the following link: https://www.bma.bm/viewPDF/documents/2021-11-05-13-37-50-FAQ---Service-Provider- Training.pdf

    To the extent an applicant intends to outsource the AML/ATF compliance function for the Bermuda RFI:

    - Per the applicant's obligations under section 14A of the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008 (POCR), the applicant should name a senior individual responsible to monitor and manage the outsourcing program and provide appropriate evidence to the Authority of their experience and competence to fulfil this responsibility. It is the Authority's preference that this senior individual is based in Bermuda

    - This guidance would equally apply to cases where the provider is insourced vs. outsourced

86. In line with the AML/ATF RFI Guidance, applicants should develop a Customer ML/TF Risk Assessment (CRA) Methodology and the accompanying form/tool for new and ongoing business relationships. The CRA should adequately assess the ML/TF risks (including but not limited to customer, geography, delivery channel and products/services) in order to determine each customer's risk rating, which in turn will determine the level of customer due diligence and ongoing monitoring required. The methodology should include consideration of events that would trigger a potential re-rating or *ad hoc* customer review. In order to fully assess the CRA tool/system and associated data integration points and methodology, the Authority may request a demonstration. The applicant should provide further evidence of integration with appropriate transaction monitoring tools, including fiat and blockchain analytics and results.

87. The following tables provide an overview of the application requirements for DAB applicants, and for Class M and T applicants, they additionally outline the information and documentation that must be prepared after license issuance but prior to the commencement of operations or client onboarding.

Table 1 – Requirements for DABA Class M and T applicants

Requirement Category	***Pre-Licensing Requirements***	***Post-Licensing Requirements (Pre-Commencement of Operations)[11]***
Business Plan	Comprehensive plan detailing nature and scale of proposed business activities	N/A – Approved during licensing phase
BRA	Identification of inherent ML/TF risks based on relevant risk factors; Appropriately reflect findings of Bermuda's National Risk Assessment; Outline mitigation measures; Assess residual risks	N/A – Approved during licensing phase
Compliance Personnel	Details of appointed CO and/or RO; Comprehensive CV demonstrating skills, experience, and AML/ATF expertise; Evidence of knowledge of Bermuda's requirements or development plan	N/A – Approved during licensing phase
CRA	Initial methodology outline for assessing customer risk; Considerations for customer profiles, geographical exposure, delivery channels, and products/services	Comprehensive methodology, with corresponding assessment form or tool, which should include: Evaluation of the ML/TF risks associated with customers, geographical exposure, delivery channels, and products/services to determine customer risk ratings; Dictating the level of customer due diligence and monitoring required; Specific triggers for customer risk reassessment or *ad hoc* reviews
Outsourcing/ Insourcing	Confirmation whether any AML/ATF or Sanctions-related functions will be outsourced/ insourced	Written confirmation of all outsourcing arrangements; Service Level Agreements (SLAs) detailing specific functions and responsibilities; Documentation on monitoring and management of outsourced functions; Documentation evidencing that ultimate responsibility remains with licensee

[11] Information/documentation that Class T and M applicants will be required to develop and submit to the Authority before commencing operations, onboarding customers or conducting testing.

AML/ATF Policies and Procedures	Initial policies aligned with business plan; Address specific ML/TF risks in BRA	Updated policies demonstrating full compliance with all relevant legislative and regulatory requirements outlined in the POCR, including: Alignment with approved business plan; Integration of identified ML/TF risks; Compliance with Part 4 of the POCR (e.g., Travel Rule)[12]

Table 2 – Requirements for DABA Class F applicants

Requirement Category	***Application Requirements***
Business Plan	Comprehensive plan outlining nature, scale, and scope of proposed business activities
BRA	Comprehensive assessment identifying, evaluating inherent risks; Detailed mitigation strategies; Assessment of residual risks
Compliance Personnel	Qualified CO and/or RO; Detailed CVs demonstrating relevant expertise and experience; Evidence of familiarity with Bermuda's AML/ATF and Sanctions framework
CRA	Comprehensive methodology for evaluating customer risk; Assessment framework for customer relationships
Outsourcing/ Insourcing	Confirmation of any outsourcing/insourcing of AML/ATF or Sanctions-related functions; Supporting documentation detailing these arrangements, including SLAs and details on oversight mechanisms to ensure the outsourced activities are effectively monitored and managed
AML/ATF Policies and Procedures	Comprehensive policies reflecting business plan; Address specific risks identified in BRA[13]

[12] Applicants are encouraged to refer to the AML/ATF RFI Guidance and the Sector-Specific Guidance Notes for DABs to ensure alignment with regulatory expectations.
[13] Applicants are encouraged to refer to the AML/ATF RFI Guidance and the Sector-Specific Guidance Notes for DABs to ensure alignment with regulatory expectations.

Corporate Governance Framework	Governance structures supporting effective oversight; Mechanisms for compliance risk management; Clear lines of responsibility and accountability

3.5 Conduct, Disclosures and Client Engagement

88. Applicants should submit a conduct risk policy document that demonstrates their approach to identifying, assessing and mitigating conduct risks. This submission should clearly outline the governance structure for conduct oversight, including roles and responsibilities of board members and senior management in supervising conduct-related matters.

89. Applicants targeting sophisticated (non-retail) and retail clients are expected to outline their client suitability assessment methodology, detailing how they will collect and validate client information regarding financial circumstances, objectives, risk tolerance and knowledge levels. This should include specific provisions for identifying and accommodating vulnerable clients. Marketing plans/processes should also be explained, demonstrating compliance with requirements for clear, fair and non-misleading communications.

90. Applicants intending to offer complex products (e.g., leveraged products or derivatives) to retail clients should also describe any additional disclosures they intend to make available to their (prospective) clients, including gain/loss ratios, margin requirements and liquidation mechanisms.

91. For applicants operating as part of a group structure where multiple entities use the same or similar trade names, documentation should demonstrate how clients will be clearly informed about which specific entity they are interacting with. This should include examples of entity-specific disclosures, distinctive user interface elements, separate branding components and clear communication protocols to eliminate potential confusion about the regulated entity providing the service.

92. The application package should further describe any planned client education resources and explain how these will be made accessible.

93. Draft terms and conditions should also be provided as part of the application package, demonstrating clear articulation of:

    - Fee structures (including any hidden or contingent charges)
    - Detailed rights and obligations of all parties
    - The specific risks associated with the proposed business model
    - Explicit statements regarding legal and beneficial title over custodied assets
    - Transparent explanations of proposed arrangements, particularly where critical functions are outsourced

- Dispute resolution mechanisms
- Applicable governing laws and jurisdiction

94. Applicants should also provide details of their proposed complaints handling process, as well as any market abuse prevention systems and controls that will be in place, including surveillance methodologies and reporting protocols.

95. Whereas all applicants are expected to provide well-developed policies, the depth and level of detail required in the documentation will vary depending on the license class being applied for. Class F applicants should submit comprehensive, fully implemented frameworks. Class M applicants are required to provide robust implementation plans with clear timelines, while Class T applicants should submit foundational frameworks that demonstrate a solid understanding of core principles. In all cases, the documentation should reflect a conduct risk approach that is proportionate to the applicant's anticipated business model, scale and complexity.

3.6 Cyber Risk

96. From a cyber risk perspective, there are different requirements in relation to the application types (T, M and F). Specifically for the maturity and development of policies for the different licence classes, which can be found within the DAB application form(s). Policies and procedures can be categorised in the following ways:

    - Fully Developed (F) – Fully documented and approved by the board
    - Advanced Draft (M) – Fully documented, but not yet approved by the board
    - Draft (T) – General Outline with certain sections still requiring refinements

97. The Authority requires applicants to document a top level Cyber Risk Policy that is reviewed and approved annually by the Board.

    The Cyber Risk Policy should include the IT control categories listed below (alternatively these topics can be documented in separate stand alone policies).

    - Cyber Risk Governance
    - IT Asset Management
    - Change Management
    - Configuration Management
    - Capacity and Performance Management
    - Business Continuity Planning
    - Disaster Recovery

- Secure Software Development Life Cycle (SSDLC)
- IT Security Operations
- Security Testing

98. The IT Roadmap should outline any major releases to support both IT and business-related services. Security Testing dates of new production services should be referenced. This allows the Authority to understand the context of the current and planned environment. The roadmap should also include an estimated timeline.

99. Applicants should provide a detailed description of their 3LOD framework. A summary of each line of defence is outlined below for reference:

- Operational (IT Security) Controls (First Line): Measures focused on IT security, including policies, procedures and technical safeguards to protect systems, data and infrastructure
- IT Risk Identification (Second Line): Processes for identifying, assessing and managing risks related to information technology and cybersecurity
- Independent Cyber Risk Audit (Third Line): An impartial evaluation of cyber risk management practices and controls to ensure compliance, effectiveness and alignment with organisational objectives

100. The IT Risk Register provides an opportunity to identify, prioritise and control cyber risks. Applicants should have a fully developed IT Risk Register (to be submitted as part of the application package), which should include the below elements:

- Risk Identification: risk name or ID
- Risk Description: a brief overview of risk
- Risk Likelihood: how likely it is the risk will happen
- Risk Impact: the potential impact of risk
- Risk Mitigation: the risk response plan
- Risk Priority: the level of risk compared to other risks
- Risk Ownership: the person or team responsible for the risk
- Risk Status: the progress of the risk mitigation plan

101. Applicants should provide a list of all international IT and data privacy-related regulations that should be met in each jurisdiction that the applicant operates, or intends to operate in. Examples

include the European Union's General Data Protection Regulation[14] and Bermuda's Personal Information Protection Act 2016. This can be included in the entities Data Protection/Privacy policy.

102. Applicants should document their IT operational security control procedures, to include;

- Logging and monitoring
- Malicious code detection/prevention
- Network perimeter controls
- Encryption of data
- Logical access management

103. Applicants intending to operate as custodians should provide a detailed gap analysis demonstrating how they currently comply or plan to comply (with timelines) with the Digital Asset Custody Code of Practice 2024 (as amended). This requirement applies even if custodial services are outsourced to a third-party provider, as applicants will still be regarded as custodians and are expected to conduct the same gap analysis to ensure compliance with the said code.

104. Applicants should understand the security testing requirements as outlined in the following sections of the DAB Operational Cyber Risk Management Code of Practice (DAB Cyber Risk Code) and provide adequate documentation in this regard.

DAB Cyber Risk Code Section 5.17 – Penetration Testing and Vulnerability Assessments

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

i. Regular penetration testing of internet-facing services by an independent and qualified testing company (minimum annual frequency);

ii. 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;

iii. Internal vulnerability scanning (minimum six-month frequency);

iv. External vulnerability scanning (minimum monthly frequency); and

v. Baseline standards to document secure configuration baselines of all network devices.

[14] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data

The expectation is that any internet-facing services are penetration tested before they go live (i.e., before they become internet-facing). The summary outcome of the penetration test should be presented to the Authority as a part of the licensing process.

DAB Cyber Risk Code Section 5.22 – Secure Application Development

A SSDLC should be in place to embed secure development practices.

DAB Cyber Risk Code Section 5.23 – Smart Contracts

An assessment of the security testing requirement should be completed before any new smart contracts are deployed. The expectation is that smart contracts should be subject to a security audit before they are used as a part of any production service. The summary outcome of the security audit should be presented to the Authority as part of the licencing process.

105. Applicants should provide details around their third-party risk assessment and management process. It should outline how the applicant intends to identify and manage cyber risk relevant to third party services.

3.7 Internal Audit

106. As part of their application package, applicants should submit documentation demonstrating their approach to internal audit. The level of detail required is proportionate to the license class sought and the complexity of the proposed operations.

107. All applicants should provide information on how their proposed internal audit function will operate as an effective 3LOD. This should include a documented Internal Audit framework outlining the proposed approach to internal audit, including how the function will maintain independence from operational activities. Additionally, applicants should submit information detailing how the internal audit function will report to the board or relevant committee, ensuring appropriate oversight and independence. Information should also include audit planning methodology and how audit findings will be tracked, remediated and reported to senior management and the board.

108. Where the internal audit function is outsourced to a group entity, applicants should also provide additional details regarding the structure and capacity of the outsourced team. These details should include the number of staff involved in delivering the internal audit services, along with their qualifications, relevant expertise and experience.

Class-specific documentation requirements

109. Class T licence applicants should submit a basic description of their proposed internal audit arrangements, which may include outsourcing to qualified third parties, along with a simplified outline of key risk areas to be covered by internal audit activities. They should provide a high-level roadmap for developing more comprehensive internal audit capabilities as the business matures. If planning to outsource the internal audit function, information on how the board will maintain

oversight of these activities should be included. Class T applicants may provide conceptual documentation, accompanied by a clear roadmap for implementation.

110. Class M licence applicants are expected to provide a more structured internal audit framework document with defined methodologies and documentation showing how the internal audit function will evolve as the business grows. They should include information on audit frequency and coverage based on risk assessment. If relying on a group internal audit function, information on whether this will adequately cover the applicant's operations with appropriate local focus should be provided, along with a clear roadmap for enhancing internal audit capabilities before transitioning to a Class F licence. Class M applicants may provide draft documentation with implementation timelines.

111. Class F licence applicants should submit comprehensive internal audit documentation, including a formal internal audit charter, evidence of planned audit committee structure and reporting lines, and a detailed audit planning methodology and risk assessment approach. They should provide documentation of formal reporting structures and remediation tracking processes, as well as information on how the effectiveness of the internal audit function itself will be assessed. If outsourcing is planned, comprehensive details on service provider selection criteria, oversight mechanisms, and board responsibility should be included. Class F applicants should demonstrate that their internal audit function will be appropriately resourced with personnel possessing relevant expertise for their proposed operations.

IV. BUSINESS MODEL-SPECIFIC CONSIDERATIONS

112. This sub-section supplements the core requirements outlined elsewhere in this GN by providing additional, activity-specific guidance regarding certain DAB activities under the Act. While the preceding sections establish the foundational regulatory expectations applicable to all applicants, as they pertain to their proposed business operations, this section outlines the specialised expectations for specific business models. It highlights common areas where the Authority typically requests further clarification during the application review process. Applicants should ensure they address both the general requirements and the activity-specific expectations relevant to their business model described in this part.

113. Where an applicant seeks to provide multiple services, it is important to note that, for the purposes of the application, they should ensure that they address all information and documentation requirements referenced under the following Sections of this GN. Examples include custodial exchange operations, spot and derivative exchange operations, and exchanges offering staking, among others. Applicants are expected to review each applicable subsection comprehensively and provide the necessary information and documentation for every service they intend to offer, as each service may have distinct compliance and operational requirements.

114. In such instances, where there is vertical integration of functions, applicants should also consider the elevated corporate governance requirements referenced under Section 3.1 of this GN. Particular emphasis should be placed on ensuring the robustness of the conflicts of interest framework, as well as other governance measures necessary to mitigate risks associated with vertically integrated operations.

Note: The Authority applies a tiered approach to the requirements outlined below and will assess the adequacy of the proposed measures relative to the nature, scale and complexity of the proposed business, allowing smaller operations to implement proportionate controls while ensuring that larger platforms maintain robust systems commensurate with their systemic importance and risk profile.

4.1 Spot Trading (exchange platform or proprietary)

115. Prospective applicants seeking to offer spot trading, whether through an exchange platform or Over-The-Counter (OTC) operations, should provide comprehensive information and documentation as outlined below.

Exchange platform

116. Applicants proposing to operate an exchange platform with an order book and matching engine should detail their asset (de)listing policies, outlining the processes and governance structures for the admission, monitoring and removal of digital assets from the platform. Specifically, applicants should include the following:

- A comprehensive list of all digital assets that will be available for trading at launch
- Clearly defined, objective criteria for both the admission of new assets and the continued listing of existing ones

- Documentation identifying the governance body responsible for asset listing decisions
- Policies regarding listing of proprietary tokens (if applicable)
- Disclosure of material interests in listed digital assets
- Procedures for managing conflicts in primary market activities
- Controls to prevent misuse of information regarding new listings

Additionally, applicants should specify how and when periodic reviews of asset admission criteria will occur, describing any triggers that prompt reviews. Protocols for suspending or delisting assets should be explained, particularly in cases where the asset's characteristics, regulatory status or risk profile undergo material changes.

117. A comprehensive description of the exchange's microstructure should be provided, covering *inter alia* the following elements:

- Order typology and execution logic
- Matching engine architecture (e.g., priority rules, batch versus continuous, latency characteristics)
- Pricing and quotation mechanics (e.g., tick size, spread governance)
- Market integrity controls (e.g., pre-trade risk filters, volatility controls, order cancellation policies)
- Liquidity incentives model (e.g., maker/taker fee model)
- Market Data and transparency (e.g., data feeds, post-trade transparency)
- Access and connectivity (e.g., API, direct market access)

118. If present, applicants should specify how mechanisms such as circuit breakers and trading halts will function, how they will be tested and the conditions under which they will be triggered to protect market integrity during periods of high volatility.

119. Applicants should clearly define whether the exchange will operate as an independent order book or connect to other liquidity venues. Further, they should address:

- The sources of liquidity, ensuring a minimum number of diversified liquidity providers
- Minimum depth requirements for the order book to maintain adequate market liquidity
- Selection and monitoring processes for liquidity providers, including key performance metrics

- Whether liquidity providers will commit to supporting the market in times of stress, and any incentives for continuous liquidity provision during volatile periods
- A range of supported order types, including market orders, limit orders, and advanced options

120. Applicants should document order handling procedures, including:

- Client order handling policy
- Best execution policy
- Order prioritisation rules
- Front-running prevention controls
- Procedures for handling large orders
- Disclosure of order routing arrangements
- Payment for order flow arrangements (if applicable)

121. To ensure fair trading practices and prevent abuse, applicants should articulate a market surveillance framework. They should outline the tools and systems used to monitor trading activities, along with processes for identifying and investigating suspicious patterns. Measures to promote fairness and transparency, as well as dedicated resources for market surveillance, should be detailed. Additionally, applicants should describe the protocols in place for addressing market abuse once identified, ensuring a robust and responsive system.

OTC spot trading operations

122. Applicants intending to offer OTC spot trading services should provide a breakdown of how these transactions will be executed, such as via telephone, messaging systems or electronic platforms. These details should include:

- Settlement methods, including pre-funded, Delivery-versus-Payment (DvP), or Free-of-Payment (FoP) options
- Exposure management methods for proprietary trading, including any hedging strategies employed
- Sources of liquidity with requirements for the minimum number and diversification of providers
- Constraints on the volume of unsettled positions and time limits for settlement with liquidity providers
- Metrics for assessing counterparty credit risk and associated post-trade settlement practices

- Monitoring processes for portfolio risk management

4.2 Derivatives/Margin Trading

123. Applicants offering derivatives or margin trading should provide a detailed description of all derivative products proposed to be offered on their exchange, including perpetual futures, options, swaps or Contracts-For-Difference (CFDs). Each product description should outline the underlying digital assets referenced, explain the pricing mechanisms used[15], and indicate whether offerings are standardised or customisable. The documentation should explain how potential price discovery disruptions are mitigated, including specific processes for handling situations where price sources become unreliable or discontinued. The frequency of mark-to-market calculations should be clearly specified. Similarly, for margin trading, the interest rate calculation methodology should be explained, along with the sources of funding for margin loan issuance.

124. Applicants should document relevant client vulnerability and suitability assessment methodologies, along with any resulting limitations on product access. If applicable, these assessments should align with any restrictions on trading certain products based on client segmentation or specific regulatory requirements.

Derivatives exchange structure and liquidity

125. Applicants should clarify whether their derivatives exchange will operate as a standalone order book or connect to other liquidity sources. The application should specify the liquidity sources for the order book, including minimum number and diversification requirements for liquidity providers, as well as minimum order book depth requirements. Applicants should provide the details of any liquidity provider and monitoring process and clarify whether liquidity providers will have any commitment to support liquidity during market stress or other incentives to ensure continuous liquidity provision during volatile periods.

126. A comprehensive description of the exchange's microstructure should be provided, covering inter alia the following elements:

- Order typology and execution logic
- Matching engine architecture (e.g., priority rules, batch versus continuous, latency characteristics)
- Pricing and Quotation mechanics (e.g., tick size, spread governance)
- Market integrity controls (e.g., pre-trade risk filters, volatility controls, order cancellation policies)
- Liquidity incentives model (e.g., maker/taker fee model)
- Market Data and transparency (e.g., data feeds, post-trade transparency)
- Access and connectivity (e.g., API, direct market access)

[15] For perpetual futures contracts, applicants should provide detailed information on the funding rate calculation methodology, including its calculation formula, payment frequency, and where available, recent historical data.

Margin requirements and leverage controls

127. Applicants should document their requirements for initial and maintenance margin based on position size and the volatility of the underlying asset. The documentation should explain how the adequacy of margin requirements is monitored on an ongoing basis to ensure client protection and platform stability. Leverage limits should be clearly defined, including maximum permissible levels for various client categories or product types, as well as any controls in place to prevent excessive leveraging or systemic risk. Applicants should specify whether margin calls or margin warnings are implemented, whether these processes are automated, and if push notifications are used to alert clients. Additionally, applicants should specify whether they will offer negative balance protection to limit client losses to their deposited funds.

128. Applicants should further detail their collateral framework, including allowed collateral types and any restrictions. The collateral valuation and revaluation methodology should be clearly explained, along with the frequency of revaluation. Applicants should specify collateral haircut levels at launch and provide the calculation methodology, including considerations for cross-denomination risks. The application should address collateral management and safekeeping procedures, with particular emphasis on segregation practices and bankruptcy remoteness to protect client assets in the event of insolvency.

Liquidation processes, risk management and loss socialisation

129. Applicants should provide a step-by-step explanation of how forced liquidations are carried out—whether they involve partial or full position closures—and how clients are notified. The application should explain the approach to handling large-scale forced liquidations during periods of heightened market volatility, including any 'waterfall' processes designed to resolve shortfalls. Applications should include details of any proposed backstop liquidity providers, describing their roles, obligations, and the funding available during extreme events.

130. If the derivatives exchange will operate a reserve fund, applicants should provide its operational framework, including the pre-funded volume and target minimum amount to be maintained at all times. The application should detail how the reserve fund will remain adequately funded and outline replenishment mechanisms to restore fund adequacy after activation.

131. Where Automated Deleveraging (ADL) or other loss socialisation mechanisms will be employed, applicants should provide a comprehensive methodology explaining how these systems will function to distribute losses. Where losses exceed the collateral posted by clients and available liquidity mechanisms, applicants should clarify whether residual losses will be absorbed by the applicant or socialised among clients. Applicants should also specify whether they will implement negative balance protection measures for their non-retail clients as part of their proposed services or risk management framework.

4.3 Stablecoin and Token Issuers

132. Applicants should provide a clear description of their proposed stablecoin(s) or tokenised asset(s), detailing *inter alia* whether they will be yield-bearing or non-yield-bearing. For tokenised assets, applicants should specify if the token represents a 'digital twin' of an existing asset or if it is a native digital token. They should include comprehensive details about the reserve assets or Real-World Assets (RWA) being tokenised. If their stablecoin or tokenised asset will generate

yield, dividends or other distributions, applicants should explain the mechanisms for yield generation, the frequency and manner of accrual, and the distribution methodology to token holders.

133. For stablecoins and certain tokenised assets, such as tokenised funds, applicants should submit a comprehensive investment policy detailing the composition of their reserve asset portfolio. This policy should clearly outline measures to ensure both the sufficiency and quality of backing assets, guaranteeing that their value equals or exceeds the total stablecoins or tokens in circulation.

Note: The investment policy should emphasise a commitment to holding high-quality, liquid assets, including short-term government securities, cash deposits with commercial banks, and, where applicable, public money-market funds. Applicants should also address their approach to diversification to mitigate concentration risks, as well as their liquidity management strategy to ensure sufficient daily liquidity for redeeming assets at par value.

134. Applicants should detail their approach to blockchain selection, including the due diligence process used to evaluate blockchain networks. If deploying across multiple blockchains, they should clarify whether stablecoins/tokens will be bridged or natively issued on each chain. For bridged stablecoins/tokens, applicants should provide details of the bridge mechanism (centralised, wrapping, etc.). They should outline their approach to interoperability across blockchain networks and with traditional financial systems, including technical standards adopted, bridge technologies for cross-chain functionality, and integration with payment systems. Applicants should explain how they manage risks associated with cross-chain transactions, including smart contract vulnerabilities and consensus mechanism differences.

135. Applicants should document the complete end-to-end lifecycle for stablecoin/token issuance and redemption, including any market liquidity considerations and timelines. For cross-chain transactions, they should detail the specific redemption processes and provide information on how proof of reserves will be maintained.

136. Applicants should ensure that their application package includes detailed information on the following:

- A thorough description of the procedures for reconciling backing assets, including identification of the teams responsible for these tasks
- Documentation of their attestation processes, along with the identification of the third-party firm responsible for the attestation
- An outline of audit procedures, as well as the identification of the third-party firm responsible for conducting audits

137. Applicants' draft terms and conditions should clearly define customer rights, particularly regarding stablecoin/token redemption, bankruptcy scenarios and issuer liquidation. They should detail the legal title to the underlying assets and any recourse available to stablecoin/token holders. For example, if the applicant will be operating a B2B2C model where direct recourse against the issuer is limited, this should be clearly articulated in the applicant's draft terms and conditions.

138. Applicants should include, as part of their submission, all agreements with staking validators and market makers/liquidity providers. They should further provide documentation of their bankruptcy remote structure, ensuring proper segregation and protection of client assets.

139. Specifically, regarding commodity-backed tokens, applicants should provide a clear description of the underlying RWA and the overall supply management ecosystem. For example, in the case of gold-backed tokens, applicants should provide comprehensive details about the gold sourcing, including adherence to industry standards[16]. They should document their vaulting arrangements, including the security measures, insurance coverage and the jurisdictional location of vaults. Applicants should detail their audit procedures for physical gold reserves, including the frequency of audits, the independent third-party auditors responsible, and the verification methodologies employed. They should also provide information on secure transportation agreements, chain of custody protocols, and how they will manage and mitigate risks during the physical movement of gold.

4.4 Custodians

140. Applicants should specify the types of digital and fiat assets to be held in custody and the way client assets will be segregated from proprietary fund. They should also identify any third parties involved in sub-custody relationships.

141. Applicants should also provide clear documentation of the legal framework governing client assets under custody[17]. This documentation should explicitly define the legal and beneficial ownership rights of clients over their assets and specify how these rights are protected. Draft custody agreements should also be submitted as part of the application package, clearly articulating the terms under which assets will be held, including any limitations on the custodian's use of those assets, jurisdictional considerations for asset protection and the procedures for returning assets to clients in various scenarios (e.g., business wind-down or insolvency proceedings).

142. For digital assets, applicants should provide a detailed description of their wallet infrastructure, including their approach to hot, warm and cold wallet solutions, and whether they implement client-level or omnibus custody arrangements. Any applicable caps for holding clients' funds in hot/warm wallets should be specified and justified based on operational needs and security considerations.

143. As pertains to fiat assets, applicants should clearly explain how they ensure segregation and bankruptcy remoteness of clients' fiat funds. This should include details on the financial institutions where funds will be held, the legal structures in place to protect client assets and the governance framework for managing these arrangements.

[16] Such as London Bullion Market Association (LBMA) Good Delivery standards or equivalently recognised benchmarks.
[17] Applicants should also refer to the 'Legal vehicle design and contractual relationships' section of this GN.

144. When utilising third-party custodians, applicants should detail their ongoing monitoring and due diligence measures. This should include the governance process for selecting custodians, performance metrics for evaluating their services and procedures for addressing service failures[18].

145. The application should outline internal reconciliation procedures, any proof of reserves methodologies and any frameworks for external independent attestation of clients' funds. Additionally, the transaction authorisation policy[19], with respect to custodied assets, should be clearly documented and aligned with the risk profile of the business.

4.5 Lending and Borrowing

Lending

146. When applying for a licence to offer lending services, applicants should provide a comprehensive description of their lending business model. They are required to specify whether their lending activities are collateralised or uncollateralised and identify their target client segments, such as retail or non-retail (institutional and/or sophisticated clients). Applications should include a complete list of the digital and fiat assets that will be accepted as collateral, as well as those available for lending. Additionally, applicants should disclose their funding sources for loans and clearly define their operational role as direct lenders, intermediaries or peer-to-peer platforms.

147. Applicants should detail their loan issuance process, including the approval workflow and underwriting criteria. They should explain their methodology for determining Loan-To-Value (LTV) ratios for varying collateral types and specify any minimum or maximum loan amounts and tenors. Information on how interest rates are set (i.e., fixed, variable or algorithmic) should be provided, along with details outlining their credit risk assessment and ongoing borrower monitoring processes. Applicants are also required to clearly state whether rehypothecation of client collateral is allowed, including the specific conditions for such practices.

148. Applicants should describe their approach to collateral management, including how collateral is held (e.g., cold wallets or hot wallets, segregated or omnibus accounts, or third-party custodians), with emphasis on segregation practices and bankruptcy remoteness measures. Terms governing the use, pledging or rehypothecation of client assets should be included in the application. Additionally, applicants should explain the frequency and methodology for collateral revaluation and LTV monitoring, as well as the triggers, procedures and systems implemented for collateral liquidation. Applicants are required to describe any automated mechanisms for managing liquidations during periods of market volatility and specify whether they maintain reserves or reserve funds to address potential shortfalls or defaults.

149. Applications should specify portfolio concentration limits in terms of counterparty, asset type and jurisdictional exposure. Stress-testing methodology for the loan portfolio under adverse market conditions should be detailed, as well as procedures for managing defaults, including the

[18] Applicants should also refer to the requirement for gap assessment against the DAB Custody Code of Practice, as further detailed in the 'Cyber Risk' section of this GN.
[19] *Inter alia* indicating responsible persons/positions and delegation/approval levels.

enforcement of collateral rights. Comprehensive approaches to loan loss provisioning should also be outlined, including specific triggers and timelines.

150. Applicants should describe the governance structures and oversight mechanisms for their lending operations. They should explain how conflicts of interest are identified and mitigated, particularly those involving related-party borrowers or affiliated entities.

Borrowing

151. For borrowing activities, applicants should provide a detailed description of their borrowing operations, including the nature of the borrowing activity (e.g., term loans, revolving credit facilities, flash loans etc.) and whether borrowing is conducted via fixed-term, open-term or demand-based agreements. They should specify the types of digital assets and/or fiat assets they plan to borrow from clients and indicate any minimum or maximum amounts per lender. Applicants should clearly articulate the intended use of loan proceeds, noting any applicable limitations or restrictions. Additionally, they should describe the methodology used to determine interest rates (e.g., fixed, floating or performance-linked) and specify if acceleration clauses apply, along with the triggers for such clauses.

152. Applicants should address how risks related to the use or investment of borrowed assets are managed, including mitigation strategies for liquidity mismatches, counterparty risk and market risk. The application should confirm whether portfolio concentration limits or exposure thresholds are applied to the use of borrowed funds. Applicants should also disclose whether borrowed funds might be used to finance related parties and describe how potential conflicts of interest would be identified and mitigated.

153. Applicants should provide information on liquidity buffers, reserves or capital allocated to ensure sufficient resources for client redemption requests. They should specify whether redemption requests are subject to gating, queuing or *pro rata* allocation mechanisms during periods of market stress. The application should include procedures for the suspension of withdrawals, detailing how such actions are communicated to clients. Furthermore, applicants should confirm the frequency of liquidity stress tests and describe the scenarios analysed during these assessments.

154. Applicants should clearly outline the frequency and scope of client reporting on the use of assets, their performance and associated risks to ensure clients remain adequately informed.

4.6 Staking

155. Applicants should provide a detailed description of their proposed staking business model, specifying the type(s) of staking services they intend to offer. Applicants should include, for all staking types, a complete list of blockchain networks supported at launch and any networks planned for future integration. All eligible digital assets for staking should be listed, along with their respective lock-up, bonding and un-bonding periods. The application should specify eligibility requirements for client participation, such as minimum staking amounts or geographic restrictions. Applicants should clearly detail the distribution process for staking rewards (e.g., native tokens, yield), including frequency, and identify if fees will be deducted prior to distribution.

Direct Staking

156. Applicants should indicate whether they will operate their own nodes (validators) and manage the staking infrastructure in-house. Applications should include details regarding the node setup process, hardware security measures, and redundancy protocols to ensure validator uptime. The applicant should disclose how it intends to manage the concentration risk of relying on a single validator or a small group of validators.

157. Applicants should detail the governance process for selecting their validators, including performance metrics, uptime requirements and penalties for errors or slashing incidents. More specifically, the application should confirm whether penalties will be absorbed by the applicant or passed on to clients and describe reserve funds or insurance policies designed to cover slashing liabilities. Applications should further explain the oversight mechanisms to ensure compliance with blockchain-specific staking requirements.

158. Applicants that will be engaging in direct staking should describe how staked assets will be held securely, whether in hot wallets, cold storage, multi-signature wallets or other setups. The application should address measures to ensure the security and integrity of client assets during validator operations, such as redundancy protocols, cyber risk protections and fallback mechanisms.

159. Applicants should disclose how they communicate the risks and rewards of staking to clients, including the potential for hardware failures, slashing penalties or network-specific risks. Reporting would typically be expected to include periodic summaries of staked amounts, accrued rewards, performance metrics of validators operated by the applicant, and any applicable fees deducted prior to reward distribution.

Delegated staking

160. For delegated staking services, applicants should specify whether clients will select their preferred validators or whether the applicant will make these selections. The application should describe the process by which clients delegate their assets for staking and the mechanisms for returning those assets to clients, including details on immediate withdrawal options (where no lock-in or un-bonding period exists), as well as the procedures for assets subject to any applicable un-bonding periods.

161. Applicants should describe their due diligence on external validators, including criteria used to assess performance (e.g., uptime, slashing history, reputation). They should outline how validator alignment with network-specific security and decentralisation principles are ensured. If any validators are affiliated with the applicant, this relationship should be disclosed.

162. Applications should further explain if slashing penalties will be borne by the validators, shared proportionally among pool participants, or covered by the applicant itself. Applicants should indicate whether slashing protections or guarantees will be offered to clients—including insurance mechanisms or fund reserves—and detail any measures to prevent operational errors or validator misconduct that could lead to slashing events.

163. Applicants should clearly outline how client assets will be securely delegated to external validators without compromising beneficial ownership. They should describe custody

arrangements and whether private keys, staking rights or control over assets are transferred to third-party validators. Measures for monitoring and safeguarding delegated assets during the staking and un-bonding processes should also be detailed.

164. Applicants should describe how they will inform clients about the due diligence process for validator selection, the distribution of rewards (e.g., whether they are auto-compounded or distributed at specific intervals), and the potential risks associated with third-party validators. Transparency around slashing risk (e.g., what happens if the delegate's validator is penalised) is essential, as is clarity regarding whether any fees or commissions are deducted from staking rewards.

Pooled staking

165. Applicants offering pooled staking should explain how client assets are combined into a staking pool and how rewards will be distributed among participants. This includes a clear explanation of how pooling impacts clients' control and ownership of their staked assets. The application should also detail how the applicant will ensure fair and proportional distribution of staking rewards across all participants, along with any mechanisms to mitigate over-concentration in specific validators. For pooled staking models, the application should further explain how validator selection minimises concentration risks and safeguards client funds.

166. Like delegated staking, pooled staking-related applications should explain if slashing penalties will be borne by the validators, shared proportionally among pool participants, or covered by the applicant itself. Applicants should indicate whether slashing protections or guarantees will be offered to clients and detail any measures to prevent operational errors or validator misconduct that could lead to slashing events.

167. Applicants should explain how client funds will be aggregated and stored, ensuring proper segregation or tracking mechanisms to maintain beneficial ownership for each client. They should also describe measures to prevent misappropriation or risks arising from significant pooling concentration on specific validators.

168. In pooled staking arrangements, applicants should explain how client contributions and rewards will be reported. They should clarify how clients will be made aware of pooling risks, such as over-concentration on a single validator or unequal reward distribution. Clear reporting of staking fees, pool performance metrics and validator activity should be outlined.

Liquid staking

169. For liquid staking services, applicants should describe how staked assets will be tokenised to allow liquidity while remaining staked. They should provide details about the issuance of derivative tokens, their redeemability for underlying assets, and any risks associated with these tokens (e.g., de-pegging risk). Additionally, the application should specify whether these derivative tokens will be used in secondary markets or Decentralised Finance (DeFi) platforms and explain how risks related to liquidity or counterparty exposure will be mitigated.

170. For liquid staking services, applicants should disclose the criteria for selecting validators that secure the staked assets backing the derivative tokens. They should explain how validator performance impacts the value and security of the derivative tokens and describe safeguards against

slashing or downtimes that may affect liquidity or token holders' redemption rights. Additionally, applicants should specify whether validator slashing risks or failures will impact the derivative token holders directly and detail insurance or risk mitigation mechanisms in place to address such occurrences.

171. Applicants should articulate whether slashing events affecting staked assets will impact derivative token holders directly or indirectly. The application should describe the measures implemented to safeguard derivative token value, including the use of slashing reserves, insurance policies or external monitoring mechanisms. Additionally, applicants should outline protocols, if any, for compensating token holders in the event of slashing-related losses.

172. Applicants should further describe the safeguards in place to protect staked assets from being misused or compromised during the tokenisation and delegation processes. This includes outlining security mechanisms within the smart contracts used for liquid staking, such as audited codebases, fail-safes, or multi-signature authorisation to prevent unauthorised transactions. Furthermore, the application should specify whether token holders retain ultimate ownership rights to staked assets and how redemption requests for derivative tokens will be processed, including mechanisms to align the liquidity of derivative tokens with the availability of underlying staked assets, particularly during high-demand periods.

173. Applicants offering liquid staking should describe how derivative token holders will be kept informed about the relationship between the derivative token and the underlying staked assets. They should disclose all risks inherent to liquid staking, including potential liquidity mismatches, market volatility that affects derivative token prices, and de-pegging events. Disclosures should also include any fees deducted for liquid staking services or secondary-market usage of derivative tokens.

APPENDIX: CORE REQUIREMENTS COMPARISON TABLE

Requirement Area	*Class T (Testing)*	*Class M (Modified)*	*Class F (Full)*
Corporate Governance	Simplified framework with basic governance policy, at least two qualified directors, simple authority matrix	Developing framework with comprehensive governance policy, well-structured board with diverse skills and planned committee structures	Mature framework with detailed governance policy, diverse board aligned to skills matrix, specialised committees and succession planning
Risk Management	Basic document with foundational concepts, simplified risk register and high-level monitoring description	Structured framework with defined methodologies, comprehensive risk register covering all material risks and documented monitoring tools	Sophisticated framework with detailed methodologies, quantified risk assessments, advanced monitoring systems, stress testing scenarios
Compliance	Basic policy covering key testing areas, streamlined regulatory monitoring process and high-level risk assessment approach	Structured framework with defined methodologies, detailed approach to compliance risks, evolving framework as business grows	Comprehensive documentation with formal compliance charter, sophisticated risk assessment methodology, specialised compliance teams
AML/ATF	Basic policy for testing activities, simplified customer risk assessment and fundamental monitoring	More detailed policy with defined methodologies, comprehensive customer risk assessment and structured monitoring	Comprehensive policy with advanced methodologies, sophisticated customer risk assessment and automated monitoring systems
Operational Risk	Basic policy identifying key operational risks, simplified business continuity considerations	Detailed policy with defined assessment methodologies, business continuity plan for critical functions	Comprehensive documentation with detailed methodologies, fully developed BCP/DR plans with recovery time objectives
Credit Risk	Basic policy with overview of approval and collateral processes	Detailed policy with clear decision-making authorities, defined collateral management	Comprehensive framework with defined risk appetite and limits, sophisticated approval framework and stress testing of collateral values
Liquidity Risk	Basic policy with simple funding plan	Detailed policy with diversification considerations, defined monitoring tools	Comprehensive documentation with defined risk appetite/ limits, sophisticated funding

			strategy, advanced monitoring, stress testing
Market Risk	Basic policy with simple measurement approach	Detailed policy considering digital asset volatility, defined hedging strategies	Comprehensive documentation with defined risk appetite, sophisticated measurement (VaR/Expected Shortfall) and advanced monitoring
Cyber Risk	Basic policy documentation, IT risk register	Advanced draft policies, more detailed IT risk register and defined security testing	Fully developed policies approved by board, comprehensive IT risk register and an advanced security testing regime
Internal Audit	Basic description of arrangements may be outsourced	Structured framework with defined methodologies, evolving as business grows	Comprehensive documentation with formal audit charter, detailed planning methodology and formal reporting structures
Conduct Risk	Basic framework with core principles	Clear implementation plans with timelines	Fully developed framework with sophisticated controls
Senior Representative	Required; may maintain office outside Bermuda	Required; must maintain office in Bermuda	Required; must maintain office in Bermuda
Head Office	Exempt (roadmap for future compliance)	Required (proportionate to business scale/complexity)	Required (full compliance with Head Office Guidance)
Insurance	Not universally required (case-by-case)	Required (appropriate to business model)	Required (comprehensive coverage)
Wind-Down Plan	Conceptual approach to orderly cessation	More detailed approach with timeline and communication strategy	Comprehensive plan with triggering events, detailed sequence and resource requirements
Financial Projections	Three-year horizon (quarterly breakdowns for first year)	Three-year horizon with more detailed analysis	Three-year horizon with sophisticated analysis and stress scenarios

Documentation Level	Basic/conceptual with roadmap for development	Advanced draft with implementation timelines	Fully developed and board-approved
Graduation Plan	Required (testing objectives, milestones, metrics)	Required (development objectives, milestones, metrics)	Not applicable