BERMUDA MONETARY AUTHORITY

GUIDANCE NOTE

FOR ENTITIES ENGAGED WITH TOKENISATION ACTIVITIES

13 November 2026

1. Introduction

1. The Bermuda Monetary Authority (Authority or BMA) expects that this Guidance Note (GN) will assist entities in understanding how existing legislative, regulatory and supervisory requirements may apply to tokenisation activities, including the assessment of whether an entity is conducting its business prudently under the applicable legislative framework.

2. The overarching aim is to support responsible innovation in tokenised assets while preserving investor protection, market integrity and alignment with international standards.

3. The standards described in the GN are proportionate to the nature, scale, complexity and overall risk profile of the entities' operations and are designed to safeguard the integrity and resilience of the financial ecosystem while ensuring robust investor protection. The framework aims to carefully tailor regulatory developments to support innovation, while adhering to a ‘same risk, same regulatory outcome’ principle.

2. Background Information

4. The Authority issues this GN in the exercise of its functions under the Bermuda Monetary Authority Act 1969 and the sectoral legislation it administers. Entities engaging in tokenisation activities remain subject to the statutory and regulatory requirements of the framework under which they are licensed, authorised or registered.

5. For the purposes of this GN, references to the applicable regulatory framework include, as relevant, the applicable Acts, regulations, rules, codes of conduct, codes of practice, prudential standards, guidance notes, statements of principles, licence conditions, directions and other supervisory requirements applicable to the regulated entity or regulated activity.

6. This GN does not create new statutory or regulatory obligations, establish a separate licensing, registration or approval regime for tokenisation activities, or prescribe a single method by which tokenisation activities must be conducted. Rather, it describes how existing legislative, regulatory and supervisory requirements may apply where entities engage in tokenisation activities and identify illustrative practices that entities may consider when managing tokenisation-related risks.

7. The Authority expects this GN will assist entities in understanding how existing legislative, regulatory and supervisory requirements may apply to tokenisation activities, including relevant prudential, conduct, governance, risk management, investor protection, market integrity, operational resilience, cyber risk, AML/ATF and other supervisory expectations. These expectations should not be interpreted as creating standalone obligations independent of the applicable legal and regulatory framework.

8. Where an applicable Act, regulation, rule, code of conduct or code of practice establishes a specific requirement, that requirement prevails. This GN should be read alongside, and does not amend, replace or supersede, the Authority's existing legislative, regulatory and supervisory frameworks.

9. The standards and practices described in this GN should be applied proportionately, having regard to the nature, scale, complexity and risk profile of the tokenisation activity. Entities may adopt alternative controls, governance arrangements or operational measures where these achieve outcomes consistent with their applicable legal and regulatory obligations.

3. Overview and Scope

10. Asset tokenisation involves the digital representation of rights, interests or claims relating to Real-World Assets (RWAs), whether tangible or intangible, using Distributed Ledger Technology (DLT). The framework outlined in this GN focuses specifically on the asset leg of tokenisation transactions (i.e., the tokenised assets themselves) rather than the settlement leg (i.e., stablecoins, tokenised deposits, Central Bank Digital Currencies or fiat). The Authority maintains a technology-neutral approach to settlement mechanisms, provided that entities implement appropriate systems and controls specific to their chosen method – such as robust smart contract functionality for atomic settlement or secure Application Programming Interface (API) integrations with credit institutions for off-chain fiat settlement. Central Bank Digital Currencies and tokenised deposits fall outside the scope of this GN because their unique characteristics and risk profiles warrant separate regulatory consideration.

11. The framework encompasses a broad range of tokenisable assets, including investments (stocks, bonds, derivatives, investment funds), insurance products (policies, claims, collateral for underwriting, risk pools), real estate, commodities, carbon credits and environmental assets, intellectual property and royalties, and art and collectables.

12. For operational purposes rather than legal definition, the Authority distinguishes between two types of tokenised assets: (i) digital twins and (ii) native tokens. This distinction does not aim to create separate regulatory regimes, but to inform the application of regulatory considerations within a unified framework, allowing proportionate, risk-based oversight that accounts for the unique characteristics of each type of tokenised asset.

13. The Authority reiterates that tokenisation activities are already permissible under existing legislative frameworks that the Authority administers. The distinctions made in this GN between digital twins and native tokens are intended to clarify how existing frameworks apply to different tokenisation approaches, rather than to create new regulatory categories.

14. Digital twins are those tokenised assets which represent existing (off-chain or tokenised) assets on DLT, with their digital token serving as a representation of rights, interests or claims. For the purposes of this framework, digital twins encompass all forms of tokenised representation of assets, including but not limited to tokens that: (a) provide direct legal rights to specific underlying assets on a 1:1 basis; (b) represent economic exposure to underlying assets without direct legal ownership; (c) reference single assets or baskets/pools of assets; (d) derive their value from the price performance of underlying assets; (e) provide conversion rights into underlying assets or their economic equivalent; and (f) pass through economic benefits such as dividends, distributions or other returns from underlying assets. The Authority recognises that digital twins may exhibit different combinations of these characteristics, and the specific regulatory expectations will be applied proportionately based on the actual risk profile and structure of each tokenisation arrangement.

15. Native tokens, conversely, are those tokenised assets that are issued directly and solely in tokenised form, with their entire lifecycle maintained within the DLT environment. Ownership rights are typically enforced primarily through DLT mechanisms, eliminating the need for reconciliation with external systems. While this approach reduces intermediary risk, it presents elevated technical risks and different governance challenges compared to digital twins. Without a reference to an underlying asset, native tokens rely entirely on the integrity of the DLT system and its governance structures, with smart contract vulnerabilities representing a primary risk factor. To date, native tokens have primarily been observed in the context of tokenised investments (i.e., bonds and stocks). Entities engaging in tokenisation activities for these products should ensure compliance with other applicable laws and regulations (e.g., the Companies Act 1981).

16. The Authority's regulatory approach acknowledges these fundamental differences while maintaining consistent regulatory objectives. This enables appropriate adaptation of expectations to address the specific risks of each category while ensuring that core principles of investor protection, market integrity, and financial stability are upheld regardless of the technological implementation.

4. Regulatory Considerations

GENERAL

17. This section outlines the key considerations and supervisory expectations that may be relevant across all tokenised asset classes[1].

18. The framework addresses three key functional roles in the tokenisation ecosystem:

    18.1.1. Primary Tokeniser: An entity that issues tokenised assets and is responsible for the initial tokenisation process, including the legal structuring, technical implementation and ongoing maintenance of the tokenised asset's integrity. This includes entities engaging in issuance activities under the Digital Asset Business Act 2018 (DABA) but specifically excludes service providers that merely assist with the legal, technical or other aspects of the tokenisation process without being the actual issuer of the tokenised asset. The Authority expects Primary Tokenisers to retain overall accountability for the tokenisation arrangement from an investor protection perspective, including maintaining appropriate oversight of material third-party dependencies. The use of service providers or intermediaries would not ordinarily diminish the Authority's expectation that Primary Tokenisers remain able to demonstrate compliance with applicable legal and regulatory requirements.

    18.1.2. Secondary Offeror: An entity that facilitates access to or trading of tokenised assets that have already been created by Primary Tokenisers. This definition includes the following secondary market intermediaries: (i) broker-dealers that facilitate the buying and selling of tokenised assets on behalf of clients; (ii) asset managers that provide investment management services involving tokenised assets[2]; (iii) trading venues that provide platforms for the exchange of tokenised assets, whether through centralised exchanges or Over-the-Counter (OTC) trading facilities; (iv) proprietary trading firms that trade tokenised assets for their own account; and (v) market makers that provide liquidity by continuously quoting bid and offer prices for tokenised assets. Examples include entities that deal in, or arrange the dealing in, investments under the IBA, and digital asset exchanges under DABA.

> *Note 1: Autonomous protocols and non-custodial software are not, solely by virtue of facilitating transactions, considered Secondary Offerors for the purposes of this framework. The Authority will have regard to the facts and circumstances of the arrangement, including the existence of persons exercising control, governance, administration or decision-making functions in relation to the protocol or its operation.*
>
> *Note 2: Traditional fund distributors facilitating primary issuance and redemption of tokenised fund interests (without secondary market trading capabilities) are not considered Secondary Offerors under this framework.*

    18.1.3. Custodians: Entities responsible for safeguarding both the tokens and, in the case of digital twins, the underlying physical or financial assets to which those tokens relate, serving as a crucial trust anchor

[1] The only asset class separately explored in the next section is tokenised funds, due to certain idiosyncratic features referenced there.

[2] This excludes investment managers of tokenised investment funds addressed in the Investment Funds: Specific Considerations section, who remain subject to their existing investment management regulatory framework without additional tokenisation-specific expectations under this GN.

in tokenisation arrangements[3]. Examples include entities that safeguard and administer investments under the Investment Business Act 2003 (IBA) and custodial wallet providers under the DABA.

19. These terms are operational classifications for the purpose of this GN and should not be construed as new licensable activities or entity types. Rather, they describe functional roles that may be performed by entities already licensed under existing frameworks such as DABA or IBA (as per examples above).

20. The Authority recognises that entities may perform multiple roles within the tokenisation ecosystem, such as combining Primary Tokeniser and Secondary Offeror functions, or operating as both broker-dealer and trading venue provider. Where an entity performs multiple roles within the tokenisation ecosystem, the Authority would generally expect it to consider the expectations associated with each role, applying them proportionately with regard to the nature, scale, complexity and risk profile of the activities performed. Where vertical integration results in the concentration of multiple roles, entities should implement appropriate corporate governance arrangements, including segregation of duties and controls, to identify, monitor and manage potential conflicts of interest and risks associated with such integration. In structures involving multiple regulated entities or where a single entity performs multiple functional roles, the Authority would expect the Primary Tokeniser to retain primary responsibility for: (a) legal structure integrity; (b) reserve asset management and reconciliation; (c) ongoing disclosures; and (d) token minting/burning controls, while the Secondary Offerors remain responsible for proportionate due diligence on the tokenisation structure and compliance with their specific functional requirements.

21. The Authority further recognises that Secondary Offerors operate diverse business models with varying client relationships and service offerings. Accordingly, the depth and frequency of ongoing monitoring and due diligence considerations referenced in this GN should be applied proportionately, considering the entity's business model, the nature and complexity of services provided, the extent of ongoing client relationships, and the degree of discretion exercised, while maintaining consistent baseline standards for investor protection.

22. For clarity, specific expectations applicable to tokenised funds and their service providers are addressed exclusively in the Investment Funds: Specific Considerations section of this GN. These entities are not captured under the terms Primary Tokenisers, Secondary Offerors, or Custodians.

23. Each role carries specific obligations designed to maintain market integrity and protect investor interests, as detailed in the subsequent sections of this GN.

DIGITAL TWIN TOKENISATION: PRIMARY AND SECONDARY MARKET CONSIDERATIONS

24. As established earlier in this GN, digital twins represent existing assets on DLT, with the actual asset typically remaining outside the DLT while its digital token serves as a representation of ownership or rights. Unlike native tokens, which are issued directly and solely in tokenised form, with their entire lifecycle maintained within the DLT environment, digital twins typically rely on traditional legal frameworks to enforce ownership rights and require ongoing reconciliation between on-chain tokens and off-chain assets. This fundamental distinction creates different risk profiles that necessitate tailored regulatory approaches while maintaining consistent regulatory objectives.

25. This sub-section outlines expectations specifically applicable to Primary Tokenisers, Secondary Offerors and Custodians involved in the tokenisation lifecycle of digital twins. These expectations address the unique challenges associated with maintaining alignment between off-chain assets and their on-chain representations, including reserve asset considerations, bankruptcy remoteness provisions, contractual frameworks, and

[3] This excludes the maintenance of tokenised registers for investment funds, which constitutes transfer agent rather than custody functions.

reconciliation processes. The expectations outlined are designed to ensure that entities throughout the digital twin ecosystem implement appropriate safeguards to protect token holder interests, maintain market integrity and provide transparency regarding the relationship between tokens and their underlying assets.

Due Diligence, Asset Verification and Legal Framework

Due Diligence Considerations

26. Primary Tokenisers should perform comprehensive due diligence on the underlying assets to ensure that no legal encumbrances exist (e.g., liens, charges, or other claims) that would prevent a clean transfer of title or rights to token holders and verify directly or through appropriately qualified third parties the quality, value and existence of the underlying assets through appropriate means.

27. For tokenised vaults or nested tokenisation structures, Primary Tokenisers should conduct enhanced due diligence on underlying token issuers, including their reserve backing arrangements and regulatory compliance status. This due diligence should be updated periodically to ensure continued integrity of the nested structure.

28. Secondary Offerors should conduct appropriate due diligence on the Primary Tokeniser and the overall tokenisation structure before offering a tokenised product. However, Secondary Offerors may place reasonable reliance on the due diligence work performed by the Primary Tokeniser and other appropriately qualified third parties in respect of the underlying assets, subject to conducting their own risk-based assessment of the product and the parties involved. Secondary Offerors may leverage existing information (including the Primary Tokeniser's disclosures, third-party audits, and regulatory reports), provided they have taken reasonable steps to satisfy themselves with the general reliability and accuracy of that information.

29. For assets subject to existing transparency measures, such as publicly traded stocks or regulated investments, both Primary Tokenisers and Secondary Offerors may implement proportionate due diligence measures that leverage existing regulatory safeguards. However, the Authority expects both entity types to remain responsible for verifying the accuracy and completeness of this information, particularly regarding any aspects unique to the tokenisation process.

Reserve Asset Considerations

30. The Authority generally expects Primary Tokenisers to maintain reserve assets on a 1:1 basis with issued tokens at all times, unless an alternative arrangement can be demonstrated to achieve equivalent investor protection outcomes. The default expectation is in-kind holding of the exact referenced underlying assets that the tokens purport to represent (e.g., tokenised investments referencing stocks). Cash-equivalent reserves may be used only where in-kind holding is impractical for specific asset classes, subject to enhanced liquidity risk disclosures.

31. Primary Tokenisers of pooled asset structures (e.g., tokenised investment funds, special purpose vehicle structures with underlying real estate, tokenised baskets or indices) should maintain reserve assets such that:

    31.1.1. The total value represented by all tokens issued accurately reflects the aggregate value of all underlying assets in the pool;
    31.1.2. The composition of the underlying asset pool accurately reflects the asset allocation and risk parameters as disclosed to token holders, where relevant; and
    31.1.3. Each token represents a proportional claim on the entire underlying asset pool rather than specific assets within the pool.

Note: For tokenised vaults containing other tokenised assets, Primary Tokenisers should ensure that underlying tokenised assets comply with applicable reserve asset considerations and implement enhanced reconciliation processes to verify the integrity of nested structures.

32. In both cases identified above, the specific underlying assets should be maintained in a manner consistent with the tokenisation structure's legal framework, reinforcing the bankruptcy remoteness provisions (see below).

33. Secondary Offerors should verify that Primary Tokenisers maintain appropriate reserve asset arrangements before offering their tokens to clients. While Secondary Offerors should satisfy themselves that appropriate disclosures, governance arrangements and assurance mechanisms exist, they are not required to conduct independent verification of the Primary Tokeniser's disclosures, third-party audits or regulatory reports in every instance. The scope of ongoing due diligence should remain proportionate to the nature of the product, the risks presented and the Secondary Offeror's role within the distribution chain.

Bankruptcy Remoteness and Token Holder Protection

34. Primary Tokenisers should implement appropriate legal structures such as Incorporated Segregated Accounts Companies (ISACs), Segregated Accounts Companies (SACs), Special Purpose Vehicles (SPVs), trust arrangements or other structures that demonstrably insulate token holders' interests from claims against the issuer or originator of the underlying assets. The selected structure should:

    34.1.1. Clearly establish the nature of token holders' rights in relation to the underlying asset (direct ownership, beneficial interest, contractual claim, or another form of legal entitlement);
    34.1.2. Include explicit provisions addressing token transferability, redemption rights, voting rights (if applicable), and claim priority in the event of issuer insolvency or default; and
    34.1.3. Be tailored to the specific characteristics of the tokenised asset, the jurisdictions involved and the intended distribution model.

35. Secondary Offerors should verify that these structural protections are in place and remain effective before offering tokens for their clients.

Contractual Framework

36. All entity types (Primary Tokenisers, Secondary Offerors and Custodians) should establish a comprehensive contractual framework – to the extent that makes sense and is applicable in relation to the business model of each entity type and the service(s) they offer.

37. Secondary Offerors should establish contractual relationships with Primary Tokenisers that secure their ability to fulfil obligations to their own clients, addressing information sharing, advance notification of material changes, and procedures for managing token events.

Legal Assessment and Cross-Border Considerations

38. Primary, Secondary Offerors and Custodians should conduct and maintain legal assessments appropriate and proportionate to their specific role, business model and operational scale in the tokenisation process. The Authority is not mandating a particular mechanism but may consider such measures as evidence that risks have been appropriately managed:

    38.1.1. Primary Tokenisers should obtain legal assessments focusing on material legal risks relevant to their tokenisation structure and target markets, which may include bankruptcy remoteness considerations, enforceability of token holder rights, and regulatory classification in key jurisdictions where they actively conduct business or where material legal risks arise;

38.1.2. Secondary Offerors should undertake proportionate legal assessments based on their distribution model and client base to confirm the validity of the primary tokenisation structure in jurisdictions material to their operations, and may rely on existing legal opinions and regulatory status of licensed Primary Tokenisers where appropriate;

38.1.3. Custodians should undertake legal assessments commensurate with their custody responsibilities and the value and complexity of assets under custody:

38.1.3.1.1. Custodians of tokens should assess material legal risks related to their custody arrangements and the underlying asset protection framework in relevant jurisdictions; and

38.1.3.1.2. Custodians of underlying assets should focus their legal assessment on material aspects of asset segregation arrangements and their contractual relationship with the Primary Tokeniser taking into account the jurisdictions where assets are held.

39. All entities may take a risk-based approach that considers the materiality of operations, the specific legal risks associated with their functions, and may rely on existing legal opinions, regulatory frameworks and reusable attestations generated by government bodies, regulated entities or qualified service providers where appropriate, avoiding duplicative diligence while maintaining appropriate standards.

40. The Authority expects all entities to review and, where appropriate, refresh legal assessments following material changes to applicable law, underlying facts, operating arrangements or tokenisation structures.

Token Standards and Technical Implementation

41. The Authority recognises that the value proposition of tokenised assets is significantly enhanced through liquidity and accessibility, which often necessitate distribution across multiple blockchain networks and trading venues. Restricting tokenised assets to specific chains or permissioned networks could fragment markets and limit the efficiency and liquidity benefits that tokenisation aims to deliver. Therefore, the Authority does not, in principle, oppose distributing tokenised assets across different DLT environments, including permissionless networks, provided appropriate safeguards are implemented.

42. The Authority recognises that compliance controls can be embedded at different layers of the technology stack. In permissioned networks, controls may be implemented at the protocol level, where the consensus mechanism itself enforces compliance requirements. In permissionless networks, compliance controls are typically applied at the token level through smart contracts. Some implementations may utilise a hybrid approach, with controls distributed across multiple layers of the stack.

43. While subsequent sections make specific reference to token standards as the most prevalent implementation method, the Authority emphasises that the same regulatory expectations apply regardless of where in the technology stack compliance controls are implemented. Any reference to token standard expectations should be construed as applying equally to protocol-level embedded controls or other technical implementations that achieve the same regulatory objectives. The Authority's focus remains on the effectiveness of controls rather than their specific technical implementation.

Compliance-Embedded Token Standards

44. Primary Tokenisers should implement token standards with robust technical specifications that ensure security, compliance, and operational efficiency regardless of the underlying DLT protocol. While the Authority maintains a technology-neutral approach and does not endorse specific token standards, all implemented standards should incorporate essential compliance capabilities. These capabilities should enable the programmatic enforcement of regulatory requirements, including:

44.1.1. Identity verification mechanisms that validate eligibility;

44.1.2. Transfer restrictions based on investor qualifications, AML/ATF sanctions and other jurisdictional limitations;

44.1.3. Configurable compliance rules that can adapt to evolving regulatory requirements through controlled, transparent and auditable governance mechanisms[4]; and

44.1.4. Remediation mechanisms allowing for appropriate regulatory intervention when necessary.

45. Secondary Offerors and Custodians should conduct appropriate due diligence to verify that tokens they offer or safeguard implement the necessary compliance capabilities outlined above.

Cross-Chain and Composability Risk Mitigation

46. The Authority acknowledges that bridges, wrappers, cross-chain messaging layers, and integration with composite financial structures introduce additional risk vectors and may potentially degrade embedded compliance controls as tokens move between environments or become components in larger protocols.

47. Primary Tokenisers should implement appropriate risk management measures for cross-chain operations and composability scenarios that could affect compliance controls, including: a) assessment of compliance control preservation across different environments and composite structures; b) implementation of equivalent controls through alternative means where original controls may be impaired; and c) monitoring and response procedures for unauthorised activities or compliance degradation.

48. Secondary Offerors and Custodians should verify that Primary Tokenisers have implemented appropriate cross-chain and composability risk mitigation measures for tokens they offer or safeguard.

Risk Management Framework

49. All entities (Primary Tokenisers, Secondary Offerors and Custodians) should implement a documented risk management framework appropriate to their role and proportionate to their activities in the tokenisation ecosystem, addressing key risks while protecting investors and market integrity. This framework should undergo regular reviews, especially after significant changes to tokenisation structures or market conditions.

50. While this framework addresses the primary risk categories associated with tokenisation activities, entities should also consider other risks relevant to their specific circumstances, including valuation risk (particularly for illiquid or complex underlying assets), concentration risk and regulatory change risk.

Counterparty Risk Management

51. Primary Tokenisers should conduct appropriate due diligence on all relevant service providers in their tokenisation structure, with particular attention to entities exercising control over critical functions including token supply management (minting or burning), transferability controls (whitelisting, freezing or restrictions), ownership records, smart contract upgrades, and key management. Oracle providers warrant particular attention given their direct influence on token functionality, pricing, collateralisation, and investor outcomes.

52. Secondary Offerors and Custodians should implement appropriate oversight of their own service providers, including oracles and technology vendors that they directly engage (and in the case of Custodians, also sub-custodians), with enhanced attention to interoperability-related service providers such as bridge operators or cross-chain infrastructure that may alter token risk profiles or introduce exposure to vulnerabilities outside the original tokenisation environment. Additionally, before offering or safeguarding tokens, they should conduct due diligence on Primary Tokenisers based on available information, contractually provided documentation, and direct inquiries, where appropriate, while being permitted to place reasonable reliance on work performed by

[4] 'Configurability' refers to the ability to update compliance parameters through structured governance processes, including appropriate approvals, testing and stakeholder communication, rather than unrestricted or real-time modification.

Primary Tokenisers and other appropriately qualified third parties regarding underlying assets. This due diligence should:

52.1.1. Assess whether the Primary Tokeniser's risk management practices meet minimum standards appropriate for the tokenised assets in question;
52.1.2. Identify any material gaps that could impact their clients' interests; and
52.1.3. Determine whether to proceed with offering or safeguarding the tokens, potentially with additional disclosures to clients or enhanced internal controls to mitigate identified risks.

53. Risk management frameworks should explicitly account for cross-environment dynamics where activity in one environment can influence outcomes in another, including valuation processes, collateral thresholds, liquidation events, and redemption mechanisms.

54. All entities (Primary Tokenisers, Secondary Offerors and Custodians) should maintain monitoring systems tracking key risk indicators with clear escalation procedures, paying particular attention to jurisdictional risks in cross-border operations, and ongoing reassessment of service providers rather than treating outsourcing as static relationships.

Liquidity Risk Management

55. Primary Tokenisers should provide clear and appropriate disclosures to token holders and maintain transparent communication regarding their liquidity management practices, including regular reporting on liquidity metrics appropriate to the asset class[5]. For tokenised assets with limited secondary markets, entities should clearly disclose liquidity constraints and implement appropriate mitigation measures, including transparent secondary venue arrangements where appropriate.

56. Liquidity risk management should address three identifiable areas: (a) secondary market liquidity where holders seeking to exit before maturity depend on functioning secondary markets; (b) settlement asset liquidity when settlement uses stablecoins or other digital assets, including depeg risk and redemption suspension risk; and (c) concentration risk where small holder bases may create market impact from large holder exits.

57. Primary Tokenisers should generally refrain from making guarantees about the liquidity of their tokens. Where liquidity guarantees are offered, Primary Tokenisers should establish and implement redemption frameworks that align token liquidity with underlying asset liquidity. Such frameworks should incorporate appropriate mechanisms based on asset type (e.g., notice periods, redemption windows, or queuing mechanisms for illiquid assets or efficient processes) and account for settlement timeframes in traditional markets for liquid assets. In these instances, Primary Tokenisers should further maintain suitable liquidity buffers.

58. Secondary Offerors should, before offering tokens to clients, conduct appropriate due diligence in Primary Tokenisers' liquidity management practices based on available information and documentation provided by the Primary Tokeniser, proportionate to their business model and the nature of services provided. They should provide clear disclosures to clients about liquidity characteristics and potential constraints at the point of sale.

59. Secondary Offerors (excluding brokers) should monitor liquidity across trading venues where the tokens they trade or list are active and have procedures to address significant price dislocations or liquidity fragmentation. Additionally, Secondary Offerors operating trading venues should implement appropriate trading interruption mechanisms for extreme market conditions, aligned with established standards for similar traditional assets (e.g., circuit breakers or trading halts).

Operational Risk Management

[5] The Authority considers it acceptable practice to publish liquidity profiles that categorise assets by time to liquidation under normal and stressed conditions.

60. Primary Tokenisers should establish controls covering the full tokenisation lifecycle that mitigate process failures, human error, and system malfunctions specific to DLT environments, with particular attention to governance and control risks associated with smart contracts and administrative privileges where entities have the ability to upgrade contracts, pause functionality, or alter token behaviour. Where tokenised assets are designed for use in composite structures (such as collateral for other tokenised products), Primary Tokenisers should assess compliance control preservation to ensure embedded controls are not bypassed when tokens interact with other protocols or financial structures.

61. Secondary Offerors should implement controls specific to token trading, order management, and trade execution. At the same time, Custodians should establish comprehensive reconciliation processes, asset segregation protocols, secure key management systems, and appropriate backup and recovery procedures, with enhanced focus on key-management and custody-related technology provider risk.

62. All entities (Primary Tokenisers, Secondary Offerors and Custodians) should document stress testing results proportionate to the nature, scale, complexity and overall risk profile of their operations, report them to senior management and the board and use the findings to strengthen risk management practices, capital planning and operational resilience.

Recovery and Wind-Down Planning

63. Primary Tokenisers should establish recovery plans addressing severe distress scenarios that could affect token functionality or value, with clear governance mechanisms for activation. They should also develop wind-down plans that prioritise token holder protection when recovery is not feasible, address the technical challenges of winding down tokenised assets and establish procedures for transferring essential functions to successor entities where appropriate.

64. Secondary Offerors should focus recovery planning on maintaining client services and protecting client assets during distress, including contingencies for Primary Tokeniser disruptions. Their wind-down plans should emphasise the orderly transfer of client positions to alternative providers or the direct return of tokens to clients, while maintaining records in a format that facilitates efficient transfers.

65. Custodians should develop comprehensive recovery plans that address scenarios threatening their ability to safeguard tokenised assets, including private key compromise, severe cyber incidents, and operational failures. Their wind-down plans should detail mechanisms for the secure and orderly transfer of tokenised assets to alternative custodians, with specific attention to maintaining security and asset verification throughout the transfer process.

66. All entities (Primary Tokenisers, Secondary Offerors and Custodians) should establish clear triggers for activating these measures, develop stakeholder communication protocols and regularly review and update their plans to reflect changes in their business model or tokenisation structure.

Nested Tokenisation Structures

67. Entities involved in nested tokenisation structures (where tokenised assets are backed by other tokenised assets) should implement enhanced risk management measures including: assessment of counterparty risks associated with underlying token issuers; monitoring of the reserve backing integrity throughout the nested structure; and contingency planning for scenarios where underlying tokenisation arrangements fail or are compromised.

Outsourcing and Vendor Management

68. All entities engaging in tokenisation activities should follow the requirements set out in the BMA's Operational Resilience and Outsourcing Code of Conduct[6]. In addition to these standard requirements, entities should pay particular attention to service providers that play critical roles specific to tokenisation, including technology infrastructure providers unique to tokenisation activities (e.g., oracles, smart contract developers, tokenisation platform providers) and asset-specific service providers appropriate to the underlying tokenised assets (e.g., physical vault providers for tokenised precious metals, property managers for tokenised real estate, and specialised valuation experts).

69. Primary Tokenisers, Secondary Offerors and Custodians should ensure (to the extent applicable, based on their business model) that their vendor management programmes address the unique risks associated with these tokenisation-specific service providers while maintaining compliance with the established Operational Resilience and Outsourcing Code. This approach ensures appropriate oversight of the specialised service providers essential to tokenisation operations without duplicating existing regulatory requirements.

Reconciliations, Attestations and Proof of Reserve

70. Primary Tokenisers[7] should maintain a tiered verification framework. Examples may include:

    70.1.1. Daily internal reconciliations ensuring tokens match underlying assets;
    70.1.2. Regular external attestations by qualified independent parties conducted proportionately based on risk and operational factors (see below)[8]; and
    70.1.3. Comprehensive 'Proof of Reserve' (PoR) audits verifying the entire reserve structure[9] .

    The Authority does not mandate a particular mechanism but may consider such measures as evidence that risks have been appropriately managed.

    Note: Attestations should, where applicable and to the extent possible, address not only asset existence but also ownership, encumbrance status, custody chain, and uniqueness, particularly for real-world assets where the risks of duplication, substitution, or undisclosed claims may arise.

71. Attestation frequency should be determined proportionately based on risk and operational factors, including but not limited to the nature of underlying assets, transaction volumes, structural complexity and overall risk profile. Primary Tokenisers should document their frequency determination methodology and provide clear justification for the selected attestation intervals based on these proportionate factors.

72. These processes should be tailored to asset characteristics and risk profiles as determined above, with verification confirming alignment between smart contract functionality and legal documentation. This verification should be performed following any material update to either the code or legal documentation and should explicitly assess whether token behaviour accurately reflects token holder rights as defined in legal documentation.

---

[6] https://www.bma.bm/viewPDF/documents/2025-09-15-16-10-28-Operational-Resilience-and-Outsourcing---Code.pdf
[7] For tokenised investment funds, different considerations apply, as set out in section 'Investment Funds: Specific Considerations' of this GN.
[8] And made available in standardised, reusable form on-chain where feasible.
[9] For physical assets such as precious metals or commodities, PoR audits should include physical verification of the underlying assets, including sampling methodologies, unannounced audit components, serial-number documentation addressing substitution risks, where appropriate to the asset class. For financial assets, audits should verify ownership records through independent sources and assess valuation methodologies.

73. Secondary Offerors should implement risk-based measures to verify Primary Tokenisers before offering their tokens. Secondary Offerors may rely on:

    73.1.1. Existing regulatory oversight for licensed Primary Tokenisers, while conducting proportionate business due diligence focused on the tokenisation structure and parties involved; and
    73.1.2. Work performed by qualified parties, including standardised reusable attestations, Proof of Reserves (PoR) reports, third-party audits, and regulatory reports produced by Primary Tokenisers or independent qualified parties, provided they take reasonable steps to verify the authenticity, currency and reliability of such information.

    For unlicensed Primary Tokenisers, more comprehensive due diligence would be appropriate, though the reliance mechanisms above remain available where suitable.

74. Custodians should implement robust reconciliation processes to ensure accurate accounting of tokenised assets under their custody. These reconciliations should occur daily, with real-time reconciliation implemented where technologically feasible. Custodians should also maintain the appropriate documentation to demonstrate that they have properly segregated and accounted for client assets. However, the Authority would expect the responsibility for PoR attestations regarding the backing of tokenised assets by underlying assets to remain primarily with the Primary Tokeniser. Custodians may rely on reusable attestations and PoR outputs produced by Primary Tokenisers or qualified third parties in standardised form to satisfy their verification obligations regarding reserve asset arrangements.

75. All entities (Primary Tokenisers, Secondary Offerors and Custodians) should establish clear procedures for addressing and reporting discrepancies, with appropriate disclosure to token holders of material issues affecting token value or holder rights. Where entities rely on reusable attestations, they should establish procedures for verifying the continued validity and authenticity of such attestations and for addressing situations where attestations become outdated or where material concerns arise regarding their accuracy or reliability.

76. Where an entity acts in multiple roles (e.g., Primary Tokeniser and Custodian), functional separation should be maintained with independent reconciliation and attestation teams to preserve verification integrity.

Secondary Market Operations

77. Secondary Offerors (excluding brokers) should establish a token listing policy that maintains market integrity and protects investor interests through risk-based and proportionate criteria. Token listing eligibility should consider market capitalisation and trading volume alongside compliance, disclosure quality, legal and structural integrity, with appropriate recognition that insufficient market depth in new issuances or infrequently traded tokenised products should not be an automatic exclusion criterion (provided other risk factors are adequately addressed). The policy should address token-level factors, underlying asset characteristics, blockchain infrastructure quality, Primary Tokeniser assessment, and legal compliance, with criteria tailored to the specific characteristics and risks of each tokenisation arrangement. These criteria should be applied flexibly to accommodate innovative tokenisation structures while maintaining investor protection objectives.

78. Secondary Offerors should implement governance arrangements for listing decisions that are appropriate to their scale and operations, including reasonable measures to identify and manage material conflicts of interest, ensure listing decisions prioritise investor protection and market integrity and maintain appropriate documentation of decision rationale.

79. The policy should establish ongoing monitoring procedures to ensure continued compliance with eligibility criteria, transparent delisting procedures with graduated responses proportionate to compliance failures, and specific provisions for managing client positions in affected tokens. Secondary Offerors should consider both traditional triggers (such as regulatory concerns and material adverse changes) and tokenisation-specific events

(such as technical vulnerabilities, loss of oracle integrity or reserve discrepancies) when developing delisting criteria, with appropriate stakeholder notification processes.

80. Secondary Offerors (excluding brokers) should implement formal governance mechanisms for reviewing and updating the policy, with appropriate documentation of all aspects, including the rationale for specific criteria and thresholds.

81. For brokers, the following distinction applies:

    81.1.1. Brokers who provide advice or recommend tokens to clients should establish an asset eligibility policy with criteria similar to those outlined above, tailored to their advisory role and the types of clients they serve.

    81.1.2. Execution-only brokers who merely facilitate transactions without providing advice should implement reasonable measures to ensure they only offer tokens from reputable Primary Tokenisers, which may include reviewing publicly available information about the tokens and avoiding tokens with widely reported critical issues.

Note: Secondary Offerors are not expected to independently verify reserve composition, ownership of underlying assets, valuation methodologies, legal enforceability, or the continuing financial condition of third-party issuers where those matters remain under the Primary Tokeniser's responsibility. Their focus should remain on maintaining objective listing and delisting policies and monitoring publicly available material information. Secondary Offerors' role is to ensure clients receive clear, fair and non-misleading information together with appropriate risk disclosures to enable informed decision-making.

NATIVE TOKENS: PRIMARY AND SECONDARY MARKET CONSIDERATIONS

82. This sub-section outlines the expectations specifically applicable to entities involved in the lifecycle of native tokens[10]. While the fundamental roles and responsibilities of Primary Tokenisers, Secondary Offerors and Custodians remain consistent with those established for digital twins, the specific requirements are tailored to address the unique characteristics of native tokens.

Due Diligence, Asset Verification and Legal Framework

83. For native tokens, similar expectations outlined in the relevant sub-section for digital twins also apply to Primary Tokenisers, Secondary Offerors and Custodians – but with certain important modifications reflecting their unique characteristics. Since native tokens exist solely on-chain without referencing any underlying assets, considerations related to asset verification, reconciliation with off-chain assets, reserve asset arrangements and bankruptcy remoteness of underlying assets should not be applicable. However, entities should still establish comprehensive contractual frameworks that define token holder rights and maintain appropriate legal assessments.

84. Compliance-embedded token standards and cross-chain risk mitigation take on heightened importance for native tokens, as there is no off-chain record or process to rectify erroneous transfers. Primary Tokenisers should implement appropriate governance mechanisms to address potential compliance issues or erroneous transactions, including documented remediation processes that specify the legal basis for any on-chain intervention and the governance controls governing such actions. Primary Tokenisers should maintain accurate and current registers of token holders as these records serve as the sole authoritative source of ownership information.

[10] As referenced elsewhere in this paper, native tokens have predominantly been observed in tokenised investment products (e.g., bonds and stocks).

85. For Custodians, bankruptcy remoteness considerations remain relevant to the custody of the native tokens themselves, including appropriate legal structures to protect client assets from the Custodian's insolvency.

Risk Management

86. Native tokens require a different risk management approach compared to digital twins. While digital twins focus on reconciling on-chain and off-chain elements, native tokens require a stronger focus on smart contracts and token-centric risk management that prioritises technical integrity at the application layer. Primary Issuers, Secondary Offerors and Custodians should implement risk frameworks that address the unique characteristics of native tokens.

    86.1.1. Smart Contract and Token-Level Risk Management: Unlike digital twins, where risk management focuses on underlying asset verification and bankruptcy remoteness, native token risk management should focus on smart contract security, token functionality, and application-level governance mechanisms. All entities should prioritise comprehensive smart contract audits and transparent disclosure of findings, as technical vulnerabilities at the token implementation level represent the primary risk vector rather than off-chain asset concerns.

    86.1.2. Counterparty Risk Management: For native tokens, counterparty risk management shifts focus from traditional intermediaries associated with underlying assets to technical service providers critical to token functionality. Entities should conduct thorough due diligence on tokenisation platforms, smart contract developers, oracle providers, and infrastructure services that support token operations. Primary Issuers should establish robust governance over these relationships. At the same time, Secondary Offerors and Custodians should understand these dependencies and evaluate whether appropriate controls are in place to mitigate risks from these critical technology counterparties.

    86.1.3. Operational Risk Management: Operational controls for native tokens should emphasise smart contract interaction vulnerabilities rather than reconciliation with off-chain systems.

    86.1.4. Recovery Planning: Recovery and wind-down planning remain applicable for native tokens, but with a different focus. Recovery and wind-down plans should address scenarios such as critical smart contract vulnerabilities, governance attacks, or severe market disruptions that affect token functionality. The emphasis should be on token infrastructure and protecting token holder interests through technological safeguards rather than focusing on underlying asset concerns relevant to digital twins.

Outsourcing, Secondary Trading and Reconciliation Considerations

87. For native tokens, outsourcing and vendor management expectations remain applicable, but with a modified scope that reflects their purely on-chain nature. Vendor management programmes should focus on technology service providers and DLT infrastructure partners, without the need to address service providers related to underlying assets (e.g., custodians of underlying investments, vault providers for precious metals, or property managers for real estate). The core considerations for due diligence, contractual safeguards and contingency planning remain essential but should be tailored to address the specific operational and technical risks associated with token-level service providers.

88. Similarly, secondary trading expectations for native tokens follow the same fundamental principles as those for digital twins, but with important modifications to listing criteria and monitoring approaches. Token listing policies should focus on technical robustness and smart contract security, rather than underlying asset characteristics. Market monitoring should focus on on-chain trading patterns and token-specific metrics rather than correlations with underlying asset markets.

89. In contrast, reconciliation, attestation and PoR expectations that apply to digital twins are not applicable to native tokens. Since native tokens exist solely on-chain and do not represent external assets, there is generally no need for synchronisation between off-chain and on-chain systems, independent verification of underlying assets, or attestations regarding reserve backing. The token ledger itself serves as the definitive record of ownership and existence, eliminating the need for the reconciliation frameworks that are essential to maintain the integrity of digital twins.

CONDUCT AND CYBER RISK CONSIDERATIONS FOR DIGITAL TWINS AND NATIVE TOKENS

90. This section outlines the conduct and cyber risk expectations applicable to entities involved in the tokenisation lifecycle of both digital twins and native tokens. While previous sections address the distinct operational and structural characteristics of each token type, the expectations presented here establish overarching standards that apply universally across the tokenisation ecosystem. These standards reflect the Authority's recognition that although digital twins and native tokens differ significantly in their technical implementation, the fundamental obligations to protect market integrity, ensure fair treatment of clients and maintain robust cybersecurity safeguards remain constant regardless of token structure.

Conduct

91. The conduct expectations outlined below are founded on core principles, including fair treatment, responsible business practices, transparency, asset protection, accessible dispute resolution and client education. All expectations should be applied proportionately, having regard to the entity's business model, nature, size and complexity, the type of clients served (retail, institutional, or sophisticated), product complexity and the specific activities undertaken (whether advisory, execution-only, primary issuance, secondary trading, or custody). The Authority recognises that different business models present varying risk profiles and accordingly, the depth and sophistication of systems and controls required may differ, while maintaining consistent baseline standards for investor protection and market integrity.

Disclosure and Transparency

92. All entities should provide clear and concise disclosures across several key areas to ensure transparency, investor protection and market confidence:

    92.1.1. Token Structure and Design: Clear definition of what the token represents, rights afforded to holders, key features including compliance mechanisms and governance capabilities, and how corporate actions or other lifecycle events affecting underlying assets (such as stock splits, dividend distributions, mergers or other adjustments) will be reflected in token balances or entitlements.

    92.1.2. On-chain and Off-chain Relationship (for digital twins): Identification of which record is legally authoritative, how discrepancies are resolved, and explanation of dual-layer custody arrangements and title transfer mechanisms.

    92.1.3. Settlement Finality: Definition of when transfers become legally final[11] and explanation of any jurisdictional variations in finality recognition, especially in cross-border contexts.

    92.1.4. Smart Contract Governance: Details of upgrade authority, conditions for changes, and emergency powers, including clear parameters for when and how changes can be implemented.

[11] Issuers should specify which process determines legal finality, particularly where technical finality (on-chain immutability) and legal finality may differ, and under what conditions finality might be challenged or reversed.

92.1.5. Oracle Dependencies: Disclosure of any oracle dependencies in the tokenisation structure, including contingency plans for oracle failures or manipulations and data integrity measures.

92.1.6. Market Characteristics: Explanation of unique market characteristics, including 24/7 trading possibilities, fragmented liquidity and potential limitations during stressed conditions.

92.1.7. Interoperability Risks: Clear disclosure of risks when tokens move across different blockchain environments, including potential impacts on compliance controls and token holder protections[12].

92.1.8. DeFi Integration Risks (where applicable): When a token is designed to interact with DeFi protocols (whether entity-deployed or external), entities should provide: (i) a clear explanation of the nature and purpose of these integrations; (ii) potential risks to token functionality, value and token holder rights; (iii) governance mechanisms specific to these integrations; and (iv) how these integrations might affect market dynamics and liquidity.

92.1.9. Dispute resolution processes.

93. Primary Tokenisers of nested tokenisation structures should provide clear disclosure to token holders regarding: the layered nature of the tokenisation structure; the identity and regulatory status of underlying token issuers; associated risks including potential amplification of operational, technical, and counterparty risks; and the reconciliation processes implemented to verify nested backing arrangements.

94. Primary Tokenisers should include this information in offering documents and ongoing disclosures, while Secondary Offerors and Custodians should either incorporate this information directly into their client communications and risk disclosures or, where appropriate, provide clear references (such as links) to the Primary Issuer's token documentation, provided that such referenced information is readily accessible to clients and contains all material disclosures required for informed decision-making. Where the Primary Tokeniser is not based in Bermuda, Secondary Offerors and Custodians should ensure equivalent disclosure standards are met, either through obtaining appropriate representations from the foreign Primary Tokeniser or by supplementing disclosures to meet the considerations outlined in this section. Secondary Offerors may rely on risk disclosures provided by Primary Tokenisers where such disclosures meet the required standards, avoiding duplicative disclosure obligations.

Suitability Assessment

95. Those Secondary Offerors that provide discretionary portfolio management or advice relating to tokenised assets (i.e., brokers) should require those clients to provide sufficient information to demonstrate their knowledge, experience and understanding of the risks associated with the specific products and/or services requested, in order to assess their suitability for such products and/or services. The knowledge verification mechanism should be proportionate to the entity's business model and client base. Where clients are limited to institutional or sophisticated investors, the fact that the client meets the relevant eligibility criteria may be sufficient. For retail clients, more comprehensive suitability assessments would be expected, including verification of understanding of tokenised asset characteristics and associated risks.

Market Abuse Systems and Controls

96. Both Primary Tokenisers and Secondary Offerors should establish appropriate systems and controls to prevent insider trading, front running and market manipulation[13]. They should further periodically assess market abuse

[12] All entities should notify investors of material changes to the risk profile or client rights when interoperability significantly alters the structure, security or behaviour of the token. This includes scenarios where the token's governance, operational features or legal enforceability are affected, such as when interoperability introduces new intermediaries, reduces transparency or creates potential jurisdictional conflicts that may impact investor protections or enforceability.

[13] Custodians are not referenced in this section as they typically do not facilitate trading activities or operate trading venues. Their primary function of safeguarding assets does not involve the execution or matching of trades that could give rise to market manipulation concerns.

risks specific to their business activities and adapt their control frameworks to address emerging threats and changing market conditions in a manner appropriate to their operations.

97. The Authority expects Secondary Offerors operating trading venues to bear primary responsibility for comprehensive market surveillance and detection of abusive trading patterns across their markets. Monitoring should incorporate both on-chain indicators (transaction patterns and liquidity movements) and off-chain signals relevant to their operations, ranging from periodic reviews to real-time surveillance as appropriate to their market impact and complexity. Entities operating across multiple markets, venues or chains should consider cross-market impacts in their oversight approach, tailoring their methodologies to the specific interconnections present in their business model. Execution-only brokers and distributors should maintain appropriate controls to identify suspicious activity within their own business, escalate concerns where appropriate and cooperate with trading venues and competent authorities.

User Interface Design

98. Primary Tokenisers and Secondary Offerors should design user interfaces that promote responsible engagement and informed decision-making. These entities should consider how interface design elements, notifications and reward structures might influence user behaviour, particularly for retail participants. User interfaces should present balanced information about opportunities and risks, with safeguards appropriate to the target audience's level of sophistication.

Client Education and Awareness

99. All entities (Primary Tokenisers, Secondary Offerors and Custodians[14]) should establish client education programmes as a fundamental conduct safeguard, proportionate to their business model, the services provided and the type of clients serviced. They should make these educational resources publicly accessible through appropriate channels and ensure clients can easily locate and access them prior to and throughout their engagement with tokenised assets.

100. Where appropriate, based on client type and product complexity, entities should implement knowledge verification mechanisms that are proportionate to their product risk profiles. Entities dealing with retail clients should implement more robust verification processes than those serving only institutional investors.

101. All entities should adopt an iterative approach to investor education, regularly reviewing and refreshing content to reflect evolving market conditions, technological developments, custody practices and educational effectiveness metrics.

Cyber Risk

102. The cyber risk framework applicable to entities engaged in tokenisation activities recognises that, while Primary Tokenisers bear the principal responsibility for implementing core security controls, Secondary Offerors and Custodians should conduct appropriate due diligence and implement complementary controls to protect their clients and, in the case of Secondary Offerors, maintain market integrity. Responsibilities should follow the functions each entity performs and the systems it controls. The Authority's focus is on the effectiveness of controls rather than their specific technical implementation. This section sets out the security outcomes to be achieved. Entities may choose the controls through which they achieve those outcomes, provided they can demonstrate that the controls are effective.

On-Chain Cyber Risk Governance

[14] Pure custody providers that solely offer custodial wallet services (without exchange, advisory, distribution etc. activities) may limit educational considerations to custody-specific risks and security practices.

103. Primary Tokenisers should implement robust on-chain governance mechanisms enforced directly by code. Non-emergency upgrades should be subject to a delay, such as a time-lock, that allows sufficient time for security review before implementation. For critical functions, including minting, treasury management and protocol upgrades, Primary Tokenisers should ensure that no single individual can act unilaterally and that the keys controlling those functions are held securely.

104. Secondary Offerors should confirm that Primary Tokenisers have implemented appropriate on-chain governance controls before offering tokens to their clients and maintain documentation of these controls for regulatory review. This confirmation may rely on information or attestations provided by the Primary Tokeniser. Secondary Offerors are not expected to verify independently matters within the Primary Tokeniser's control.

105. All entities should obtain an independent security assessment, proportionate to the risk, before deploying material changes to protocols they control. When controlling any aspect of token functionality, they should maintain transparent records of all governance actions.

Off-Chain Governance

106. Primary Tokenisers should develop comprehensive off-chain governance frameworks addressing the human and process layers of security. These should include clearly documented incident response playbooks, strict controls over access to critical infrastructure, and secure key custody arrangements that prevent single-individual access to minting keys. Primary Tokenisers should test their incident response capability in a way that gives reliable assurance that it would work in a live incident.

107. Secondary Offerors should establish clear procedures for responding to security incidents affecting tokens they offer, including communication protocols with Primary Tokenisers and procedures for protecting client interests during incidents.

108. Custodians should secure private keys with controls that prevent single-individual access to critical functions, such as minting keys.

109. All entities (Primary Tokenisers, Secondary Offerors and Custodians) should implement transparent oversight mechanisms for major security decisions and regular security training programmes for staff with access to critical systems. They should implement appropriate controls to mitigate security risks associated with human and process failures. Where self-custody arrangements are utilised, independent administrators should be involved in the approval mechanisms.

Tokenisation Lifecycle Security

110. The tokenisation process involves multiple stages during which different security controls should be implemented.

Stage 1: Asset Selection and Structuring

111. Primary Tokenisers should maintain documented migration plans for cryptographic standards to address emerging threats, such as quantum computing vulnerabilities.

Stage 2: Token Creation and Minting

112. Primary Tokenisers should implement pre-minting attestation from independent third-party custodians and protect minting functions with governance controls that prevent a single individual from accessing critical functions.

113. Custodians should provide the independent, auditable attestations of reserve assets that Primary Tokenisers require before executing minting functions.

Stage 3: Smart Contract Development and Deployment

114. Primary Tokenisers should obtain independent security audits before deployment, have verifiable controls to ensure the deployed code matches the audited code, and maintain the ability to contain the effects of failures in critical functions.

115. Secondary Offerors and Custodians should seek confirmation that smart contracts have been independently audited and that appropriate governance controls are in place for upgradable contracts.

116. All entities should implement appropriate governance mechanisms for any contract functionality they control, consistent with the on-chain governance expectations set out above.

Stage 4: Token Issuance and Distribution

117. Where appropriate, Primary Tokenisers should implement controls to prevent domain and front-end hijacking.

118. Primary Tokenisers should implement authenticated communication channels for all offering-related information. Secondary Offerors should confirm the Primary Tokeniser's security controls.

Stage 5: Post-Issuance Trading and Management

119. Primary Tokenisers should manage their exposure to integrations, protocols, platforms and counterparties within defined limits calibrated to the relevant operational, market, counterparty and technology risks, enforced through on-chain controls where appropriate. Where pricing or reference data is derived from oracles, Primary Tokenisers should ensure that such mechanisms account for market liquidity and are resistant to distortion and manipulation.

120. Entities should implement cross-chain bridge and DeFi integration risk management appropriate to their role and degree of control over token transfers.

Stage 6: Redemption And Realisation

121. Primary Tokenisers should implement controls that keep redemption processes orderly and resilient to denial-of-service attacks and provide verifiable confirmation of off-chain asset release.

Stage 7: Token Destruction and Burning

122. Primary Tokenisers should use well-tested, industry-standard code for burn functionality and conduct regular audits to verify that on-chain supply accurately reflects all burn events.

123. Secondary Offerors should confirm that appropriate burn mechanisms are in place and monitor burn events for compliance with stated schedules.

124. Primary Tokenisers should maintain transparent records of all burn events. Secondary Offerors should maintain records of burn events relevant to the tokens they offer.

5. Investment Funds: Specific Considerations

125. This section addresses the regulatory expectations applicable to tokenised investment funds where only the fund register is tokenised. This represents the tokenisation of fund units/shares themselves, creating digital representations of investor interests in the fund on DLT. This section does not address funds that hold tokenised assets in their investment portfolios. Where only the register is tokenised, the Authority adopts an outcomes-based approach to tokenised investment funds, ensuring regulatory outcomes equivalent to traditional funds while recognising the operational efficiencies that tokenisation can provide.

126. This section specifically addresses the primary offering of tokenised investment funds and the regulatory expectations applicable to operators of tokenised funds and their service providers in that context. It does not encompass secondary trading of tokenised fund units. Fund operators should clearly define in fund documentation the conditions under which tokenised fund units may become available for secondary market trading. Where tokenised fund units are traded on secondary markets, the applicable Secondary Offeror expectations outlined in the preceding section apply to those entities, platforms or venues that actively facilitate or conduct such secondary trading, not to the funds themselves[15].

127. It is important to emphasise that the Authority would expect the operators of tokenised funds to bear the ultimate responsibility for ensuring that all service providers appointed to the fund meet the considerations outlined in this section. As required under the IFA, operators should ensure that service providers remain fit and proper at all times, including their ability to fulfil tokenisation-specific obligations. When assessing the suitability of service providers for appointment, fund operators should conduct thorough due diligence to verify that these providers can meet the standards described in this GN as part of their obligations under the Minimum Licensing Criteria of the IFA.

Tokenised Investment Funds

128. Operators remain responsible for ensuring that each appointed service provider is fit and proper, and able to carry out its activities in line with this GN, both at appointment and on an ongoing basis. References in this section to operators ensuring, assessing or monitoring a matter should be read as accountability for the outcome, supported by appropriate oversight of service providers and the ability to demonstrate to the Authority that the expected outcome has been achieved.

129. Operators are accountable for ensuring, through the service providers they appoint and oversee, that tokenising a fund's register does not affect the fund's established valuation methodology; net asset value (NAV) calculation processes and timing; pricing controls and validation procedures; or compliance with financial reporting standards. Tokenisation may enhance but should not compromise the accuracy, timeliness or transparency of fund valuation processes. It is reiterated that no additional reserve asset, bankruptcy remoteness, specialised stress testing or PoR expectations apply merely because the register is tokenised.

130. For tokenised registers where DLT serves as the authoritative source of truth, fund documentation should specify which register constitutes the authoritative legal record and ensure compliance with the fund's governing law.

Risk Management Framework

131. Operators of funds are accountable for ensuring that risks specific to register tokenisation are assessed and monitored as part of their risk management framework, whether by the operator or by the service providers they appoint. These include counterparty risks associated with both fund-specific functionaries (such as investment

[15] A fund that merely enables peer-to-peer secondary trading or collateralised lending or borrowing of its tokenised units is not automatically considered a Secondary Offeror.

managers and fund administrators) and tokenisation-specific service providers, alongside technology and operational risks related to DLT infrastructure, legal risks related to register authority, and cyber risks specific to tokenised register operations. Operators should be able to demonstrate that appointed service providers remain fit and proper to carry out these activities in line with this GN.

Note: The stress testing, recovery and wind-down planning expectations outlined in the general tokenisation section are not applicable to tokenised investment funds where tokenisation does not fundamentally alter the fund's risk profile beyond what is already required for traditional funds.

Outsourcing and Vendor Management

132. Operators of tokenised funds are accountable for ensuring that the vendor management expectations outlined in the preceding section are applied in full, incorporating both general tokenisation service providers and fund-specific service providers (such as administrators, custodians, and transfer agents) within their comprehensive vendor management programme. This includes satisfying themselves, at appointment and on an ongoing basis, that each service provider is fit and proper and able to meet those expectations in respect of the activities it performs.

Reconciliations, Attestations and PoR - Modified Approach

133. The expectations for reconciliations, attestations and PoR outlined in the preceding section of this GN do not apply to tokenised investment funds. Given that tokenised funds typically maintain traditional NAV calculation methodologies and established fund accounting practices, these specialised verification expectations would be redundant and unnecessary. Operators nevertheless remain accountable for ensuring that the service providers they appoint continue to maintain those established practices, and for being able to demonstrate that these providers remain fit and proper to do so.

134. Instead, operators of tokenised funds are accountable for ensuring that the fund administrators they appoint maintain standard NAV calculation and unit reconciliation processes in accordance with existing fund regulations and best practices, with specific tokenisation-related considerations addressed in the 'Fund Administrators/Transfer Agents' subsection below. The operator remains responsible for verifying that these processes are appropriate and effectively implemented, and that the administrator remains fit and proper to perform them.

Conduct and Investor Protection

135. For tokenised investment funds, the existing fund regulatory framework already provides robust investor protections. While the general conduct considerations apply to Primary Tokenisers, operators of tokenised funds should primarily focus on ensuring transparency and disclosures, incorporating relevant tokenisation information into the fund's standard offering documentation (whether prepared by the operator or by service providers they appoint), including, at a minimum, which register constitutes the authoritative legal record, how tokenisation affects investor rights and redemption processes, technology risks specific to the tokenised register, settlement finality and transfer mechanisms, and any limitations on secondary market trading. Other considerations, such as market monitoring and client education, may not be necessary given the existing fund regulations.

Note: Operators should consider making current NAV per share and outstanding capital commitments publicly available via website or on-chain publication to facilitate informed secondary market trading, particularly where peer-to-peer trading occurs independently of fund operations.

136. The Authority emphasises that tokenisation should not alter the fund's fundamental investor protection framework. Operators are accountable for ensuring that tokenised fund units maintain the same investor eligibility restrictions as their traditional counterparts, and that appropriate technological controls are implemented within the tokenised register, whether by the operator or by the transfer agent or other service provider they have appointed, to enforce these restrictions and prevent unauthorised transfers.

137. Operators are accountable for ensuring, whether directly or through the service providers they appoint and oversee, that tokenised funds do not use tokenisation arrangements to create liquidity or transferability that circumvents or is inconsistent with the fund's disclosed redemption terms, established liquidity management procedures, or applicable regulatory requirements. Token transferability should reflect the underlying fund's liquidity profile and redemption constraints.

Cyber Risk

138. All cyber risk expectations outlined in the preceding section that are applicable to Primary Tokenisers also apply to tokenised investment funds. Operators of tokenised funds are accountable for ensuring that these expectations are properly implemented, either directly or through the service providers they appoint, and for maintaining appropriate oversight of those providers, including ensuring that they remain fit and proper to implement them. However, the Authority recognises that the risk profile of tokenised fund units differs significantly from other tokenised asset classes, particularly when only the register is tokenised. Given these differences, the Authority will approach the application of cyber risk expectations in a proportionate manner, focusing on the specific technological risks introduced by the tokenisation of fund units rather than applying a one-size-fits-all approach.

Fund Service Providers

Investment Managers

139. Investment managers retain due diligence obligations commensurate with their actual function and operational interaction with tokenisation infrastructure. Investment managers whose role is limited to investment selection and monitoring, without direct DLT infrastructure interaction, are not required to conduct platform-level technical due diligence on tokenisation platforms. Where investment managers only manage funds with tokenised interests, standard investment management due diligence processes apply without additional tokenisation-specific considerations. Comprehensive due diligence on tokenisation platforms remains the responsibility of fund operators.

Fund Administrators/Transfer Agents

140. For tokenised registers, administrators should ensure equivalent regulatory outcomes to traditional registers while leveraging DLT capabilities. Fund documentation should explicitly designate which register constitutes the authoritative legal record. As transfer agents, administrators should implement transfer restrictions, investor verification and compliance controls directly within register infrastructure, ensuring token transfers reflect legal ownership transfers with clear settlement finality.

Custodians

141. For tokenised investment funds (where effectively only the register is being tokenised), the Authority does not view the maintenance and security of token records as a custody function, but rather as an extension of the transfer

agent's traditional role in maintaining the register of unitholders. While appropriate cyber risk controls remain applicable to these activities, they do not constitute custody services for regulatory purposes[16].

[16] Consequently, investors may hold tokenised fund units in self-custody arrangements without triggering additional custody service requirements, though fund operators should provide appropriate guidance on security responsibilities and technological risks.