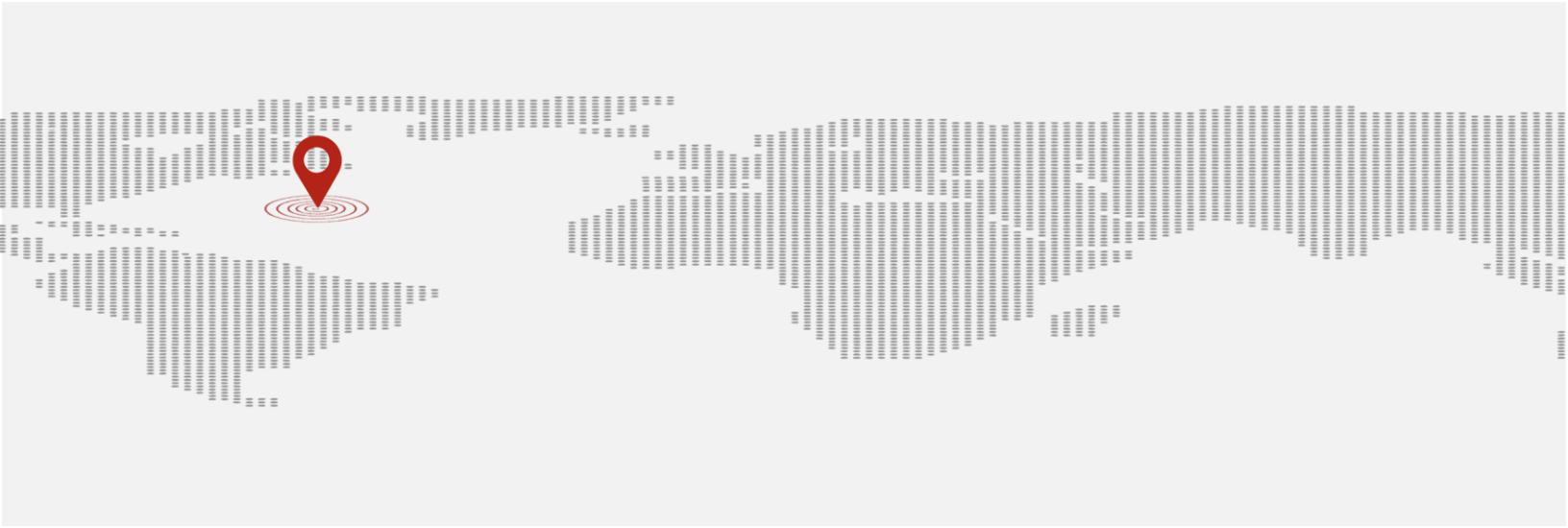
Thursday, 9 April, 2026

BERMUDA MONETARY AUTHORITY

# ASSET TOKENISATION CONSULTATION PAPER

Comments to be received by 30 June 2026



# Contents

## I. INTRODUCTION

1. In November 2025, the Bermuda Monetary Authority (Authority or BMA) released a Discussion Paper (DP) that examined the evolving landscape of asset tokenisation and solicited industry feedback on potential adaptations to Bermuda's regulatory frameworks. The feedback received highlighted several key themes, including the need for clarity on cross-framework interactions, proportionate regulation based on risk profiles and recognition of the distinct characteristics of different tokenisation models.

2. This Consultation Paper (CP) builds upon that foundation by presenting targeted regulatory proposals informed by stakeholder input and international developments. The overarching aim is to promote responsible innovation in tokenised assets while maintaining robust investor protections, market integrity, and alignment with international standards. These proposals seek to provide the legal and regulatory certainty needed for sustainable market development while addressing the unique risk profiles inherent in tokenised structures.

3. It is emphasised that the legislative frameworks that the Authority administer already extend to tokenisation activities. This CP does not propose an entirely new regulatory regime. The proposals outlined aim to enhance regulatory clarity, address specific tokenisation-related risks, and ensure that entities conduct their tokenisation activities in a prudent manner while leveraging existing regulatory structures.

4. The Authority is issuing this CP simultaneously with a Stakeholder Letter that provides additional context and information regarding the proposed regulatory framework for asset tokenisation. Stakeholders are encouraged to read both documents collectively to gain a comprehensive understanding of the proposals outlined herein. The Stakeholder Letter complements this CP by providing further clarification on key aspects of the framework and addressing feedback received on the DP.

5. Considering the significance of revisiting and adapting existing legislative and regulatory frameworks due to asset tokenisation, it is crucial that relevant stakeholders actively engage in the consultation process. This is particularly important given the cross-sectoral implications of certain tokenisation activities, where the aim is to strike a careful balance: avoiding unnecessary or unintended dual licensing requirements while ensuring that all regulatory frameworks remain robust, coherent and fit for purpose in addressing the opportunities and risks associated with this emerging area.

6. The proposed framework is structured into two complementary levels: (1) a legal and regulatory architecture that aims to provide clarity and certainty for each tokenised asset class and (2) bespoke requirements tailored to the various entities engaged in asset tokenisation activities. The proposals described in the CP 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 proposed framework aims to carefully tailor regulatory developments to support innovation, while adhering to a “same risk, same regulatory outcome” principle.

7. Industry and other stakeholders are invited to provide feedback on the proposals outlined in this paper by emailing their comments to fintech@bma.bm by the close of business on **30 June 2026**. The Authority acknowledges that not all sections and questions may be directly relevant to every stakeholder. Accordingly, stakeholders are encouraged to focus their responses on the areas most applicable to their operations and expertise.

## II. OVERVIEW AND SCOPE

8. 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 proposed framework outlined in this CP 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 CP due to their unique characteristics and risk profiles that warrant separate regulatory consideration.

9. The proposed 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.

10. 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 rather to inform the application of regulatory requirements within a unified framework, allowing for proportionate and risk-based oversight that accounts for the unique characteristics of each type of tokenised asset.

11. The Authority reiterates that tokenisation activities are already permissible under existing legislative frameworks that the Authority administers. The distinctions made in this paper 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. This consultation seeks to articulate the proposed approach and overall requirements for entities engaging in tokenisation activities, ensuring they demonstrate prudent business operations in accordance with the minimum criteria for licensing across applicable frameworks.

12. Digital twins are those tokenised assets which represent existing off-chain assets on DLT, with the actual asset remaining outside the blockchain while its digital token serves as a representation of rights, interests or claims. They typically rely on traditional legal frameworks for the enforcement of ownership rights and require ongoing reconciliation between on-chain tokens and off-chain assets. Digital twins introduce intermediary and credit risk due to the separation between the token and underlying asset, with a number of dependencies, including oracles and external data sources for accurate representation. This structure creates the potential for discrepancies between on-chain transfers and off-chain

recognition, necessitating robust legal and governance mechanisms.

13. 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 off-chain 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. It is important to note that, 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).

14. The Authority's regulatory approach acknowledges these fundamental differences while maintaining consistent regulatory objectives. This enables appropriate adaptation of requirements 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.

15. The Authority emphasises that the proposed requirements set out in this CP are supplementary in nature and do not replace or supersede existing requirements applicable to licensees under their respective regulatory frameworks. Entities engaging in tokenisation activities remain fully subject to all existing regulatory obligations relevant to their licensed activities, with these proposed requirements providing additional guidance specific to tokenisation operations. This approach ensures consistent regulatory standards across all activities while addressing the unique aspects of tokenisation.

16. Throughout this CP, the term 'should' is used when describing the proposed framework elements. The Authority wishes to clarify that all instances of this term represent proposals rather than final determinations. The entire framework outlined in this document constitutes the Authority's proposals for public consultation, and no proposal contained herein should be considered finalised until after the conclusion of the consultation period and the Authority's consideration of all feedback received.

## III. PROPOSED LEGAL AND REGULATORY ARCHITECTURE

17. This section outlines the Authority's principles-based regulatory framework for asset tokenisation that emphasises substance over form, ensuring assets and activities are regulated according to their economic and functional characteristics rather than their technological implementation. To mitigate potential regulatory overlap and reduce unnecessary compliance burdens within the existing regulatory landscape, the Authority proposes tailored exemptions for entities operating across multiple frameworks, while ensuring comprehensive oversight of risks specific to tokenisation activities. The proposed architecture seeks to provide regulatory clarity and support responsible innovation, while safeguarding market integrity and ensuring robust investor protection.

### *Cross-Regime Exemptions*

18. The Authority recognises that certain tokenised assets may qualify as investments under existing legislation, including those conferring rights or interests in underlying assets listed in the First Schedule of the Investment Business Act 2003 (IBA), those providing exposure to underlying asset values without ownership rights, and native tokens that exist solely on DLT yet possess inherent investment characteristics. Similarly, activities performed by certain tokenisation platform providers, such as facilitating the creation and distribution of tokenised investments or acting as agents for issuers, may qualify as an investment business activity under the IBA. To clarify, tokenised investments are a subset of the broader category of tokenised assets, and like all tokenised assets, they may take the form of either digital twins (representing existing off-chain assets) or native tokens (created and existing solely on DLT). This regulatory overlap necessitates a thoughtful approach to prevent duplicative compliance requirements while ensuring appropriate supervision.

19. To address the potential for duplicate compliance requirements and provide regulatory clarity, the Authority proposes a substance-over-form approach with a harmonised definition of ‘tokenised investments’ to be introduced across multiple regulatory frameworks, encompassing the IBA, the Investment Funds Act 2006 (IFA), the Fund Administration Provider Business Act 2019 (FAPBA), the Digital Asset Business Act 2018 (DABA) and the Digital Asset Issuance Act 2020 (DAIA). This harmonisation is proposed to be achieved by introducing a single definition in the IBA, with all other frameworks cross-referencing it. This approach will ensure consistency across regulatory regimes while providing a clear, authoritative source for the definition, facilitating more efficient updates if refinements become necessary in the future. This definition will apply to both digital twins and native tokens, recognising their underlying technological differences while focusing regulatory treatment on their economic substance and the risks inherent in their structure and use. This harmonised definition will serve as the foundation for the cross-regime exemptions proposed in this section.

**Proposed 'tokenised investment' definition**

'Tokenised investment' means any investment as defined in section 3(1)(a) of the IBA that is represented in digital form using distributed ledger technology, whether as (i) a digital representation of an existing off-chain asset ('digital twin') or (ii) a digital asset created and existing solely on a distributed ledger ('native token').

20. Additionally, the Authority will undertake a review of the investment categories prescribed in Part 1, First Schedule of the IBA to ensure that the definition remains appropriate and reflects developments in the market. For example, stakeholders provided additional examples of investment products being tokenised beyond those outlined in the DP. These include products structured as revenue-sharing arrangements linked to an interest in a pool of assets (e.g., tokenised participations that entitle holders to a proportional share of revenues generated by underlying assets such as real estate, intellectual property, or other pooled resources). Stakeholders also queried whether such products would be regarded as 'investments' under the IBA or as 'investment funds' under the IFA.

    While these products may fall within existing categories in the First Schedule of the IBA, (e.g., 'rights and interests in investments'), the Authority acknowledges that, in certain cases, ambiguity may arise where the structure emphasises revenue participation rather than direct ownership, or where the asset pool operates in a manner akin to an investment fund, potentially falling within the scope of the IFA. The Authority will further assess these arrangements to clarify their appropriate regulatory classification.

21. To address concerns regarding regulatory overlap and dual licensing, the Authority proposes that appropriately tailored exemptions be introduced for entities operating across overlapping frameworks. The Authority recognises that, in certain instances, the risks associated with specific activities involving tokenised investments may be appropriately mitigated within a single regulatory framework, thereby making the imposition of dual licensing requirements both unnecessary and potentially counterproductive. Requiring compliance with multiple frameworks when relevant risks have already been addressed can create complexity and regulatory burden, potentially stifling innovation in the development and adoption of tokenised technologies.

22. The Authority, through industry consultation and market observation, recognises that entities have diverse operational structures and strategic orientations within the financial sector. Requiring entities to operate under a specific regulatory framework that may not align with their established business model could create unintended operational inefficiencies without necessarily enhancing outcomes. For instance, established financial institutions carrying on investment business activities involving tokenised investments (as defined above), as part of their broader service offering, may face additional compliance considerations if required to restructure under DABA, even though they already maintain appropriate risk controls under their IBA licence. Conversely, 'digitally native' entities whose

business models entail tokenised investments may be more appropriately regulated solely under the DABA framework. In pursuit of our regulatory objectives and recognising practical business considerations, the Authority proposes to introduce optional mirrored exemptions for dual-licensing scenarios. This approach ensures comprehensive risk oversight tailored to different business models while allowing entities to operate within a framework aligned with their operational structure and strategic objectives.

23. In addition, to ensure consistency and holistic oversight across all applicable frameworks, the Authority will seek to revisit the relevant legislative and regulatory regimes and, where necessary, introduce targeted amendments to address risks specific to tokenised assets. The BMA will implement several key regulatory extensions to create a comprehensive framework for tokenised assets, including the following:

    a) The DAB Operational Cyber Risk Management Code of Practice is proposed to be extended to all entities engaging in tokenisation activities, regardless of their primary regulatory framework, ensuring consistent cybersecurity standards across the ecosystem;

    b) The DAB Custody Code of Practice is proposed to apply to all entities providing custody services for tokenised assets, establishing uniform standards for safekeeping, key management protocols and operational controls;

    c) The IFA is proposed to be amended to: (1) explicitly allow for a fund register to be tokenised (and exist purely on-chain), providing legal certainty for DLT-based ownership records; and (2) recognise tokenisation-specific service providers as having satisfied principles that underpin traditional service provider appointment requirements. Additionally, the IFA Disclosure Rules are proposed to be amended to include bespoke tokenisation-specific disclosures, such as smart contract functionality, upgrade mechanisms, technological risks, and the allocation of responsibilities among service providers; and

    d) Anti-Money Laundering/Anti-Terrorist Financing (AML/ATF) DAB sector-specific guidance is proposed to apply to all entities leveraging exemptions under DABA, maintaining robust AML/ATF standards regardless of regulatory classification.

24. By aligning and enhancing existing frameworks in response to tokenisation and other DLT-driven activities, the Authority aims to build a unified, forward-looking regulatory environment that supports innovation while maintaining the highest standards of market integrity and investor protection.

*Digital Asset Business and Investment Business*

25. The Authority acknowledges that there may be instances of potential regulatory overlap between the definitions of 'investment business', as set out in First Schedule, Part 2 of the IBA, and 'digital asset business', as set out in section 2(2) of DABA. This overlap arises because the definition of digital asset business under DABA is broader, encompassing a wide range of activities specific to digital assets, including activities related to tokenised investments, and is designed to comprehensively address the associated risks.

26. To address this overlap, the Authority proposes that where DABs engage in activities that fall within the definitional perimeter of 'investment business' under the IBA, and such activities relate *exclusively* to tokenised investments, these DABs be exempted from the dual licensing requirement under the IBA. This exemption will be facilitated by expanding the definition of non-registrable persons pursuant to the Investment Business (Non-Registrable Persons) (Designation) Order 2022.

27. Mirroring the exemption under the IBA contemplated above, it is proposed that an equivalent exemption be introduced under DABA for licensed investment businesses engaging solely in investment business activities (considered narrower in scope than digital asset business activities) *exclusively* related to tokenised investments. This exemption will be included in the Digital Asset Business Exemption Order 2023 (DAB Exemption Order)[1] and would be limited only to licensed investment providers under the IBA. Therefore, the proposed exemption would not be available to investment providers registered as Class A Registered Persons or Class B Registered Persons.

***Fund Service Providers: Investment Manager and Self-Custody***

*Investment Manager*

The Authority recognises that tokenisation in the context of investment funds can occur at two distinct levels: (i) at the fund register level, where ownership interests in the fund are tokenised or (ii) at the portfolio level, where the fund invests in tokenised assets. Importantly, the investment manager's core function remains unchanged in either scenario, as they do not typically directly custody, transfer or process these tokenised assets, but rather direct qualified custodians and administrators to execute transactions based on their investment decisions.

Accordingly, the exemption contemplated in this illustrative example is proposed to apply to investment managers (licensed under the IBA) engaged in:

[1] The broader nature of digital asset business activities (which includes the 'digital asset services vendor' definition, capturing any type of intermediary activity in relation to digital assets), in combination with the broad 'digital asset definition', renders DABA a conducive platform-centric framework to address instances of platform convergence.

i. Managing investment funds where ownership interests are tokenised (i.e., tokenised fund shares/units);
ii. Managing investment funds that hold tokenised assets within their portfolios; or
iii. Managing investment funds that involve a combination of both tokenised fund shares/units and tokenised asset portfolios.

This proposed approach recognises that the introduction of tokenisation does not alter the fundamental nature or responsibilities of the investment fund manager's role.

*Note: This example illustrates the case of traditional investment managers licensed under the IBA who engage with tokenised investments, reflecting the current market landscape. The Authority notes that the proposed mirrored exemption principle would also apply in reverse scenarios. 'Digitally native' entities primarily licensed under DABA that engage in activities which might otherwise require IBA licensing when involving management of tokenised investment funds would similarly benefit from appropriate IBA exemptions.*

*Self-Custody*

Based on feedback received and market observations, the Authority acknowledges that in certain instances, and in view of the convergence of roles, the investment manager may be conducting self-custody of tokenised fund units and/or tokenised assets forming part of an investment fund's portfolio (for and on behalf of the investment fund). Given the risks that may be associated with these arrangements, particularly conflicts of interest, they will be assessed on a case-by-case basis, ensuring that the investment manager has the appropriate systems and controls in place to mitigate them.

The Authority notes that, as it stands, the operator of a fund may request a waiver of the requirement to appoint a third-party custodian under the IFA; therefore, no additional statutory amendments are currently contemplated. Where, based on the above, the Authority determines that self-custody is acceptable, and noting the mirrored exemption route referenced above, the investment manager responsible for self-custody is proposed to be exempted from a DABA licensing requirement (for the reason already stated).

However, the Authority emphasises that this exemption will be accompanied by enhanced requirements specific to tokenised activities, such as compliance with applicable custody standards (including those derived from DABA's Custody Code of Practice). These standards will endeavour to ensure that risks associated with the custody of tokenised assets, including cybersecurity and operational risks, are appropriately managed.

*Tokenised Funds and Fund Administrators*

28. The Authority proposes that tokenised funds be explicitly exempted from the requirements of DAIA in cases where the tokenisation of fund units or shares is involved. Based on the

Authority's experience, the way such funds have been structured to date generally allows them to benefit from one or more of the other exemptions already contemplated under DAIA. However, introducing an explicit exemption specifically for tokenised funds would provide further legal and regulatory clarity.

29. The Authority also intends to streamline and align key definitions across regulatory frameworks. Specifically, the Authority proposes to review and harmonise the definitions of 'qualified participants' under Section 9 of the IFA and 'qualified acquirers' under Section 6 of DAIA. Codifying aligned and consistent definitions will help eliminate any ambiguity, promote cross-regime clarity and provide certainty for stakeholders.

30. Beyond aligning 'qualified participants' and 'qualified acquirers', the Authority proposes to undertake a comprehensive harmonisation of investor qualification definitions across all relevant regulatory frameworks (IFA, IBA, DABA, DAIA). This will establish a unified approach to investor categorisation, ensuring consistent investor protection standards regardless of the specific framework under which a tokenised investment is offered.

31. It is further proposed that **fund administrators** conducting activities associated with tokenised funds, such as maintaining tokenised registers or managing smart contracts for the minting and burning of tokens, be exempted from licensing requirements under DABA. As fund administrators are already subject to regulation under FAPBA, the risks arising from such activities are largely addressed within the existing regulatory framework. However, to ensure consistency in risk management and to mitigate potential regulatory gaps, the Authority will assess the feasibility of applying relevant standards under DABA, such as those pertaining to operational resilience and smart contract governance, or introducing related safeguards under the FAPB framework, to fund administration providers engaging in such activities.

***Question 1***

***Do you agree with the Authority's proposed approach to definitions and harmonisation across regulatory frameworks, including the harmonised definition of 'tokenised investment', the review of investment categories, and the alignment of qualified investor definitions? Are there any aspects that require modification or additional clarification?***

***Question 2***

***Do you agree with the Authority's proposed cross-regime exemption approach, including the substance-over-form principle and optional mirrored exemptions?***

***Question 3***

***What transitional measures or arrangements should the Authority consider implementing until the enactment of the proposed legislative amendments?***

***<u>Question 4</u>***

***Are there any additional areas within the proposed legal and regulatory architecture that have not been adequately addressed in this section of the CP?***

## IV. PROPOSED FRAMEWORK: REGULATORY REQUIREMENTS

### GENERAL

32. This section outlines the Authority's proposed regulatory framework establishing overarching requirements applicable across all tokenised asset classes. Unlike the DP, this section does not include dedicated subsections on tokenised investments (outside of funds), tokenisation in (re)insurance, precious metals, real estate or energy efficiency certificates, or other forms of alternative assets (e.g., art or intellectual property) as the Authority's assessment indicates that the comprehensive overarching requirements established in this section adequately address the regulatory needs of these sectors. The only asset class separately explored in the next section is tokenised funds, due to certain idiosyncratic features referenced there.

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

    a) **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 DABA as well as operators of tokenised investment funds under the IFA. Primary Tokenisers may issue tokens directly to clients. This 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.

    b) **Secondary Offeror**: An entity that facilitates access to or trading of tokenised assets that have already been created by Primary Tokenisers. This definition is limited to the following secondary market intermediaries: (i) broker-dealers that facilitate the buying and selling of tokenised assets on behalf of clients; (ii) asset managers; and (iii) trading venues that provide platforms for the exchange of tokenised assets, whether through centralised exchanges or Over-the-Counter (OTC) trading facilities. Examples include entities dealing or arranging the dealing in investments under the IBA, and digital asset exchanges under DABA.

    c) **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 in tokenisation arrangements. Examples include entities that safeguard and administer investments under the IBA and custodial wallet providers under the DABA.

34. These terms are operational classifications for the purpose of this CP 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).

35. The Authority recognises that in some cases, entities may perform multiple roles within the tokenisation ecosystem. For example, an entity might combine the roles of a Primary Tokeniser and a Secondary Offeror, effectively creating and managing both primary and secondary markets for tokenised assets on a single platform. Another scenario could involve a Secondary Offeror operating as both a broker-dealer and providing a trading venue, thereby facilitating trades while also maintaining the marketplace where those trades occur. In such cases of role convergence, the entity should satisfy the requirements applicable to all roles it performs, while maintaining appropriate segregation of duties and controls to manage potential conflicts of interest.

36. For clarity, specific requirements applicable to fund administrators/transfer agents in relation to tokenised investment funds are addressed exclusively in the *Investment Funds: Specific Considerations* section of this CP. These service providers are not captured under the terms Primary Tokenisers, Secondary Offerors, or Custodians[2].

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

***Question 5***

***(a) Are there any aspects of the proposed Primary Tokeniser, Secondary Offeror, and Custodian roles that require further clarification?***

***(b) Is there an additional role or type of activity in the tokenisation lifecycle that has not been captured by these classifications?***

## DIGITAL TWIN TOKENISATION: PRIMARY AND SECONDARY MARKET REQUIREMENTS

38. As established earlier in this CP, digital twins represent existing off-chain assets on DLT, with the actual asset remaining outside the blockchain 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.

[2] Unless they engage in any of these activities, in which case the relevant requirements outlined in this section would also be applicable, as per above.

39. This sub-section outlines the proposed requirements specifically applicable to Primary Tokenisers, Secondary Offerors and Custodians involved in the tokenisation lifecycle of digital twins. These requirements address the unique challenges associated with maintaining alignment between off-chain assets and their on-chain representations, including reserve asset requirements, bankruptcy remoteness provisions, contractual frameworks, and reconciliation processes. The requirements are designed to ensure that entities throughout the digital twin ecosystem implement appropriate safeguards to protect tokenholder 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 Requirements*

40. 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.

41. Secondary Offerors should conduct appropriate due diligence on both the underlying assets and the tokenisation structure and 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 of the general reliability and accuracy of that information.

42. 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, both entity types remain responsible for verifying the accuracy and completeness of this information, particularly regarding any aspects unique to the tokenisation process.

*Reserve Asset Requirements*

43. Primary Tokenisers should maintain reserve assets on a 1:1 basis with issued tokens at all times, where such reserve assets should be the exact referenced underlying assets that the tokens purport to represent (e.g., tokenised stocks).

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

a) The total value represented by all tokens issued accurately reflects the aggregate value of all underlying assets in the pool;

b) The composition of the underlying asset pool accurately reflects the asset allocation and risk parameters as disclosed to tokenholders, where relevant; and

c) Each token represents a proportional claim on the entire underlying asset pool rather than specific assets within the pool.

45. 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).

46. Secondary Offerors should verify that Primary Tokenisers maintain appropriate reserve asset requirements before offering their tokens for clients and should conduct ongoing due diligence to ensure continued compliance with these requirements.

*Bankruptcy Remoteness and Tokenholder Protection*

47. 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 tokenholders' interests from claims against the issuer or originator of the underlying assets. The selected structure should:

a) Clearly establish the nature of tokenholders' rights in relation to the underlying asset (direct ownership, beneficial interest, contractual claim, or another form of legal entitlement);

b) Include explicit provisions addressing token transferability, redemption rights, voting rights (if applicable), and claim priority in the event of issuer insolvency or default; and

c) Be tailored to the specific characteristics of the tokenised asset, the jurisdictions involved and the intended distribution model.

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

*Comprehensive Contractual Framework*

49. 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 – that

includes:

a) Master service agreements and operational Service Level Agreements (SLAs) that define the rights and obligations of each party;

b) Clear delineation of responsibilities for key tokenisation functions (e.g., asset custody[3], token issuance, compliance monitoring, technical maintenance and investor services);

c) Performance expectations and accountability mechanisms with defined remediation processes;

d) Provisions granting the Authority access to relevant information necessary for effective supervision;

e) Clear dispute resolution mechanisms addressing jurisdiction, governing law, escalation procedures, and alternative dispute resolution options; and

f) Specific provisions for token lifecycle events (i.e., issuance, redemption, fork management, protocol upgrades, and potential wind-down scenarios).

50. 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*

51. Primary Tokenisers, Secondary Offerors and Custodians should conduct and maintain comprehensive legal assessments appropriate to their role in the tokenisation process:

a) Primary Tokenisers should obtain assessments covering bankruptcy remoteness across jurisdictions, private international law considerations, legal status of smart contracts and underlying assets, enforceability of tokenholder rights, and regulatory classification in key distribution jurisdictions;

b) Secondary Offerors should undertake independent legal assessments to confirm the validity and enforceability of the primary tokenisation structure in their distribution jurisdictions; and

c) Custodians should undertake legal assessments appropriate to their specific custody role:

[3] Where multiple custodians are responsible for different layers of the custody structure (e.g., one custodian safeguarding the tokenised assets and another custodian responsible for the underlying real-world assets), the contractual framework should clearly define the allocation of responsibilities, liabilities and operational procedures between these custodians.

i. Custodians responsible for the safeguarding of tokens should focus on the proposed custodial arrangements for the underlying assets, including the bankruptcy remoteness provisions and the legal arrangements that protect tokenholder rights across relevant jurisdictions; and

ii. Custodians responsible for safeguarding the underlying RWAs should conduct legal assessments focused on the arrangements established between themselves and the Primary Tokeniser, including the legal structure for asset segregation, the contractual protections in place, and their role in supporting the overall bankruptcy remoteness of the Primary Tokeniser's tokenisation structure.

In both cases, Custodians should assess the enforceability of their rights and obligations with respect to the assets under custody as well as the legal implications of the custody chain across all relevant jurisdictions.

52. All entities are expected to regularly review and update their legal assessments following material changes to applicable laws, regulations or the tokenisation structure.

***Question 6***

***(a) Do you support the Authority's proposed approach to due diligence, asset verification and legal frameworks for tokenised assets?***

***(b) Do you agree with the specific requirements outlined for each entity type (Primary Tokenisers, Secondary Offerors and Custodians)?***

***(c) Are there additional considerations that should be addressed to ensure robust asset validation and token holder protection in the context of these distinct roles?***

**Token Standards and Technical Implementation**

53. 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 lead to market fragmentation, limiting the efficiency and liquidity benefits that tokenisation aims to deliver. Therefore, the Authority does not, in principle, oppose the distribution of tokenised assets across different blockchain environments, including permissionless networks, provided appropriate safeguards are implemented.

54. 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.

55. 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 requirements 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*

56. Primary Tokenisers should implement token standards with robust technical specifications that ensure security, compliance, and operational efficiency regardless of the underlying blockchain 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:

    a) Identity verification mechanisms that validate eligibility;

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

    c) Configurable compliance rules that can adapt to evolving regulatory requirements; and

    d) Remediation mechanisms allowing for appropriate regulatory intervention when necessary.

57. 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 Risk Mitigation*

58. The Authority acknowledges that bridges, wrappers and cross-chain messaging layers introduce additional risk vectors and may potentially degrade embedded compliance controls as tokens move between environments. In cases where bridging or wrapping

mechanisms remove or impair embedded compliance controls and safeguards, Primary Tokenisers should demonstrate that equivalent controls can be applied through alternative means (e.g., off-chain compliance verification systems, mandatory gateway processes for cross-chain transfers, supplementary smart contracts that restore compliance functionality in the destination environment).

59. Primary Tokenisers should implement appropriate risk management measures for cross-chain operations that could affect compliance controls. These measures should include identifying key risks, monitoring for unauthorised cross-chain activities and having procedures in place to address compliance issues if they arise.

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

***Question 7***

***(a) Do you agree with the Authority's proposed requirements for token standards and technical implementation, including the approach to cross-chain distribution and compliance controls?***

***(b) Are there any technical aspects that require further consideration?***

**Risk Management Framework**

61. 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.

*Counterparty Risk Management*

62. Primary Tokenisers should conduct appropriate due diligence on all relevant service providers in their tokenisation structure. For traditional intermediary models, this may include assessing custodians, technology providers and oracles. For non-custodial or smart contract-based models, the focus may be on technical safeguards, including smart contract audits, governance controls and continuous monitoring.

63. 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). 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. This due diligence should:

a) Assess whether the Primary Tokeniser's risk management practices meet minimum standards appropriate for the tokenised assets in question;

b) Identify any material gaps that could impact their clients' interests; and

c) Determine whether to proceed with offering or safeguarding the tokens, potentially with additional disclosures to clients or enhanced internal controls to mitigate identified risks.

64. 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.

*Liquidity Risk Management*

65. Primary Tokenisers should provide clear and appropriate disclosures to tokenholders and maintain transparent communication regarding their liquidity management practices, including regular reporting on liquidity metrics appropriate to the asset class[4].

66. 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.

67. Secondary Offerors should, before offering tokens to clients, conduct appropriate due diligence on Primary Tokenisers' liquidity management practices based on available information and documentation provided by the Primary Tokeniser. They should provide clear disclosures to clients about liquidity characteristics and potential constraints at the point of sales.

68. 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

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

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*

69. Primary Tokenisers should establish controls covering the full tokenisation lifecycle that mitigate process failures, human error, and system malfunctions specific to DLT environments.

70. 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.

71. All entities (Primary Tokenisers, Secondary Offerors and Custodians) should document stress testing results, report them to senior management and the board, and use findings to strengthen risk management practices, capital planning and operational resilience.

*Recovery and Wind-Down Planning*

72. 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, addressing the technical challenges of winding down tokenised assets and establishing procedures for essential function transfers to successor entities where appropriate.

73. 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.

74. 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.

75. 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.

***Question 8***

***(a) Do you agree with the Authority's proposed risk management framework for tokenisation activities (including counterparty, liquidity and operational risk management, stress testing and recovery and wind down planning)?***

***(b) Are there additional risk factors specific to tokenisation that should be addressed?***

**Outsourcing and Vendor Management**

76. All entities engaging in tokenisation activities should follow the requirements set out in the BMA's Operational Resilience and Outsourcing Code of Conduct[5]. 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).

77. 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.

***Question 9***

***(a) Do you agree with the proposal to align tokenisation outsourcing and vendor management requirements with the existing Operational Resilience and Outsourcing Code, while emphasising specific considerations for tokenisation-specific service providers that Primary Tokenisers, Secondary Offerors, and Custodians should address?***

[5] https://www.bma.bm/viewPDF/documents/2025-09-15-16-10-28-Operational-Resilience-and-Outsourcing---Code.pdf

***(b) Are there specific aspects of the tokenisation value chain that warrant additional safeguards?***

**Reconciliations, Attestations and Proof of Reserve**

78. Primary Tokenisers[6] should maintain a tiered verification framework, including:

    a) Daily internal reconciliations ensuring tokens match underlying assets;
    b) Regular external attestations by qualified independent parties[7]; and
    c) Comprehensive 'Proof of Reserve' (PoR) audits verifying the entire reserve structure[8].

79. These processes should be tailored to asset characteristics, with real-time verification where feasible and appropriate frequency adjustments for less liquid assets. Verification should confirm alignment between smart contract functionality and legal documentation[9].

80. Secondary Offerors should implement reasonable measures to verify the regulatory status of Primary Tokenisers before offering their tokens. For licensed Primary Tokenisers operating under appropriate regulatory oversight, Secondary Offerors may rely on this existing regulatory framework while conducting standard business due diligence. For other Primary Tokenisers, more comprehensive due diligence on their tokens would be appropriate.

81. 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 responsibility for PoR attestations regarding the backing of tokenised assets by underlying assets remains primarily with the Primary Tokeniser.

82. All entities (Primary Tokenisers, Secondary Offerors and Custodians) should establish clear

[6] For tokenised investment funds, different considerations apply, as set out in section 'INVESTMENT FUNDS: SPECIFIC CONSIDERATIONS' of this CP.

[7] At minimum, attestations should occur monthly for liquid financial assets and semi-annually for less liquid assets such as real estate or private equity.

[8] For physical assets such as precious metals or commodities, PoR audits should include physical verification of the underlying assets, including sampling methodologies appropriate to the asset class. For financial assets, audits should include verification of ownership records through independent sources and assessment of valuation methodologies.

[9] 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.

procedures for addressing and reporting discrepancies, with appropriate disclosure to token holders of material issues affecting token value or holder rights.

***Question 10***

***(a) Do you support the Authority's proposed approach to reconciliations, attestations, and PoR requirements?***

***(b) Do you agree with the specific verification responsibilities assigned to Primary Tokenisers, Secondary Offerors, and Custodians?***

***(c) Are the proposed frequencies and verification methods appropriate for different asset classes?***

**Secondary Market Operations**

83. Secondary Offerors (excluding brokers) should establish a token listing policy that maintains market integrity and protects investor interests. The policy should include clear eligibility criteria at both token level (market capitalisation, trading volume, liquidity) and underlying asset level (appropriate standards for each asset class[10]), with a comprehensive legal and regulatory assessment framework evaluating the token's compliance with relevant jurisdictions.

84. Qualitative criteria should assess the Primary Tokeniser's operational history, regulatory standing, governance, and technical infrastructure, with differentiated requirements based on token type[11] and appropriate diversification thresholds.

85. 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[12].

86. Secondary Offerors (excluding brokers) should implement formal governance mechanisms for reviewing and updating the policy, with appropriate documentation of all aspects,

[10] E.g., such as minimum market capitalisation for tokenised equities (even for publicly traded stocks that may be thinly traded), credit ratings for tokenised debt instruments, or independent valuation requirements for tokenised real assets.

[11] E.g., more stringent requirements for tokens representing less liquid underlying assets or employing more complex tokenisation structures.

[12] Including reasonable (and statutory) notice periods, options for orderly exit, and procedures for handling tokens that cannot be transferred or redeemed through normal channels.

including the rationale for specific criteria and thresholds. For brokers, the following distinction applies:

a) Brokers who provide investment 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.

b) Execution-only brokers who merely facilitate transactions without providing investment 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.

***Question 11***

***(a) Do you agree with the proposed requirements for secondary market operations and token listing policies?***

***(b) Do you support the specific responsibilities assigned to Primary Tokenisers, Secondary Offerors (including the differentiated approach for brokers) and Custodians?***

***(c) Are there additional criteria that should be considered for each entity type to ensure market integrity in the secondary trading of tokenised assets?***

## NATIVE TOKENS: PRIMARY AND SECONDARY MARKET REQUIREMENTS

87. This sub-section outlines the proposed requirements specifically applicable to entities involved in the lifecycle of native tokens[13]. 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

88. For native tokens, similar requirements 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

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

solely on-chain without underlying assets, requirements related to asset verification, reconciliation with off-chain assets, reserve asset requirements and bankruptcy remoteness of underlying assets are not applicable. However, entities should still establish comprehensive contractual frameworks that define token holder rights and maintain legal assessments focused on inter alia transfer of legal title through the token itself, compliance with relevant applicable laws and cross-jurisdictional enforceability.

89. 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 place particular emphasis on maintaining accurate and current registers of token holders as these records serve as the sole authoritative source of ownership information.

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

**Risk Management**

91. 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 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.

    a) **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.

    b) **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, while Secondary Offerors and Custodians should understand these dependencies and evaluate whether appropriate controls are in place to mitigate risks from these critical technology counterparties.

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

d) **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 the 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 Reconciliations Considerations**

92. For native tokens, outsourcing and vendor management requirements 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 requirements 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.

93. Similarly, secondary trading requirements 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.

94. In contrast, reconciliation, attestation, and PoR requirements 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 for maintaining the integrity of digital twins.

***Question 12***

***(a) Do you support the Authority's proposed approach to regulating native tokens, including the modified requirements for due diligence, risk management and operational controls that reflect their purely on-chain nature?***

***(b) Do you agree with the specific responsibilities assigned to Primary Tokenisers, Secondary Offerors and Custodians?***

***(c) Are there additional considerations specific to native tokens that should be addressed in the regulatory framework?***

## CONDUCT AND CYBER RISK REQUIREMENTS FOR DIGITAL TWINS AND NATIVE TOKENS

95. This section outlines the proposed conduct and cyber risk requirements 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 specific to each token type, the requirements 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 that remain constant regardless of token structure.

### Conduct

96. The proposed conduct requirements outlined below are founded on core principles, including fair treatment, responsible business practices, transparency, asset protection, accessible dispute resolution and customer education. All entities (Primary Tokenisers, Secondary Offerors and Custodians) should implement these requirements in proportion to their respective business models and customer compositions (with enhanced measures for retail clients).

*Disclosure and Transparency*

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

    a) Token Structure and Design: Clear definition of what the token represents, rights

afforded to holders, and key features including compliance mechanisms and governance capabilities.

b) 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.

c) Settlement Finality: Definition of when transfers become legally final[14] and explanation of any jurisdictional variations in finality recognition, especially in cross-border contexts.

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

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

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

g) Interoperability Risks: Clear disclosure of risks when tokens move across different blockchain environments, including potential impacts on compliance controls and token holder protections[15].

h) 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 integration; and (iv) how these integrations might affect market dynamics and liquidity.

[14] For hybrid systems with both on-chain and off-chain components, issuers should specify which process determines legal finality and under what conditions finality might be challenged or reversed. This is particularly important where smart contracts include functionality for administrative intervention or where legal frameworks may impose different standards of finality than those enforced by the underlying technology.

[15] All entities should notify investors of material changes to the risk profile or customer 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.

98. 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.

*Suitability Assessment*

99. Those Secondary Offerors that provide advice relating to tokenised assets (i.e., brokers) should require those clients to provide sufficient information to demonstrate their knowledge and experience in relation to the specific products and/or services requested, in order to assess their suitability for such products and/or services. For higher-risk products, Secondary Offerors should provide such services only after determining that the client has the requisite experience and knowledge to understand the risks associated with the requested products and services.

*Market Abuse Systems and Controls*

100. Both Primary Tokenisers and Secondary Offerors should establish appropriate systems and controls to prevent insider trading, front running and market manipulation[16]. They should further periodically assess market abuse 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.

101. Secondary Offerors operating trading venues should monitor trading activities. Monitoring could range from periodic reviews to real-time surveillance, incorporating both on-chain indicators (transaction patterns and liquidity movements) and off-chain signals relevant to their operations.

102. Secondary Offerors operating trading venues across multiple markets, venues or chains should consider cross-market impacts in their oversight approach, where applicable. In these instances, they should tailor their methodologies to the specific interconnections present in their business model.

*User Interface Design*

103. Primary Tokenisers and Secondary Offerors should design user interfaces that promote responsible engagement and informed decision-making. These entities should consider how

[16] 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.

interface design elements, notifications and reward structures might influence user behaviour, particularly for retail participants. User interfaces should present balanced information about both opportunities and risks, with appropriate safeguards that reflect the target audience's level of sophistication.

*Customer Education and Awareness*

104. All entities (Primary Tokenisers, Secondary Offerors and Custodians) should establish comprehensive customer education programmes as a fundamental conduct safeguard. They should ensure clients have ready access to appropriate educational resources that clearly explain the unique characteristics, benefits and risks associated with tokenised assets (including phishing and social engineering risks), and that make individuals aware of their responsibilities within the business relationship. These resources should:

a) Be presented in standardised, plain language that is accessible to the intended audience; and

b) Clearly differentiate between digital twins and native tokens, explaining the distinct legal and risk profiles of each token type.

105. All entities 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.

106. 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.

107. 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.

***Question 13***

***(a) Do you support the Authority's proposed conduct requirements for entities involved in tokenisation activities?***

***(b) Do you agree with the specific responsibilities assigned to Primary Tokenisers, Secondary Offerors (including the differentiated requirements between execution-only brokers and those operating trading venues) and Custodians across the key areas of disclosure and transparency, suitability assessment, market abuse prevention, user interface design and customer education?***

***(c) Should market manipulation systems and controls be required only for Secondary Offerors operating trading venues, or should they apply to other types of Secondary Offerors as well?***

**Cyber Risk**

108. The proposed 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.

*On-Chain Cyber Risk Governance*

109. Primary Tokenisers should implement robust on-chain governance mechanisms enforced directly by code. These entities should deploy mandatory time-locks of at least 48 hours for all non-emergency upgrades, ensuring sufficient time for security review before implementation. For critical functions including minting, treasury management, and protocol upgrades, Primary Tokenisers should implement high-threshold multi-signature schemes requiring a minimum of 4-of-6 or 5-of-7 approvals using hardware-backed keys (HSMs/MPC).

110. Secondary Offerors should confirm that Primary Tokenisers have implemented appropriate on-chain governance controls before offering tokens to their clients. They should conduct due diligence specifically on the governance mechanisms controlling upgradability and maintain documentation of these controls for regulatory review.

111. All entities should implement formal requirements for independent security audits before deploying any protocol changes. When controlling any aspect of token functionality, they should establish minimum voting quorums for governance decisions and maintain transparent records of all governance actions.

*Off-Chain Governance Requirements*

112. 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 role-based permissions for critical infrastructure access, and hardware-backed key custody solutions that prevent single-individual access to minting keys. Primary Tokenisers should implement mainnet shadow forking to test incident responses on private clones of the live chain, providing deterministic

validation that is superior to theoretical exercises.

113. 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.

114. Custodians should secure private keys using hardware-backed solutions (HSMs/MPC) and high-threshold multi-signature arrangements to prevent single-individual access to critical functions, such as minting keys.

115. 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 multi-signature approval mechanisms.

*Tokenisation Lifecycle Security*

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

*Stage 1: Asset Selection And Structuring*

117. 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*

118. Primary Tokenisers should implement pre-minting attestation from independent third-party custodians and protect minting functions with multi-signature schemes (minimum 4-of-6 or 5-of-7) using hardware-backed keys.

119. 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*

120. Primary Tokenisers should obtain independent audits from specialist security testing companies, implement reproducible builds with cryptographic verification, pin dependencies to specific versions, and deploy circuit-breakers for critical functions.

121. 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.

122. All entities should implement appropriate governance mechanisms for any contract functionality they control, including mandatory time-locks for upgrades and multi-signature requirements for administrative functions.

*Stage 4: Token Issuance And Distribution*

123. Where appropriate, Primary Tokenisers should implement fair launch technology controls to reduce risks of front-running and deploy technical controls, such as Domain Name System Security Extensions, to prevent domain and front-end hijacking.

124. Primary Tokenisers should implement authenticated communication channels with digital signatures for all offering-related information and verify the Primary Tokeniser's security controls.

*Stage 5: Post-Issuance Trading And Management*

125. Primary Tokenisers should restrict tokenised assets to approved integrations, protocols, platforms and counterparties, with such restrictions implemented through enforceable on-chain controls where appropriate. They should set defined exposure limits for each approved integration, calibrated to the relevant operational, market, counterparty and technology risks. Where pricing or reference data is derived from oracles, Primary Tokenisers should ensure that such mechanisms properly account for market liquidity and trading depth and assign reduced or no weight to prices from illiquid venues that may be vulnerable to distortion, manipulation, or unreliable price formation.

126. Secondary Offerors and Custodians should conduct due diligence on the interoperability risks of the tokens they offer and appropriately disclose these risks to investors.

127. All entities should monitor cross-chain bridges used by their tokens, prioritising those that may carry higher risks, such as those with zero-knowledge verification over multi-sig-only bridges, and implement appropriate risk controls for DeFi integrations.

*Stage 6: Redemption And Realization*

128. Primary Tokenisers should implement queue throttling and per-address caps to prevent denial-of-service attacks and provide cryptographic attestations confirming off-chain asset release.

*Stage 7: Token Destruction And Burning*

129. 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.
130. Secondary Offerors should verify that appropriate burn mechanisms are in place and monitor burn events for compliance with stated schedules.

131. Both entities (Primary Tokenisers and Secondary Offerors) should maintain transparent records of all burn events.

***Question 14***

***The Authority has proposed specific baseline technical controls (e.g., multi-signature thresholds, timelocks, continuous proof-of-reserve, and mainnet shadow forking) to address the unique velocity of cyber risks in tokenisation.***

***(a) Do you consider these baseline technical controls proportionate for Primary Tokenisers?***

***(b) If you disagree with a specific prescriptive mandate, are there any alternative cryptographic, automated or deterministic controls that you believe should be considered (particularly concerning high-risk vectors such as cross-chain bridges and external oracles)?***

***(c) Are there operational challenges in the proposed allocation of cyber responsibilities between Primary Tokenisers, Secondary Offerors and Custodians? If so, please describe any anticipated operational challenges.***

***(d) Additionally, what transitional lead times would be required for the industry to implement this framework?***

**INVESTMENT FUNDS: SPECIFIC CONSIDERATIONS**

132. This section addresses regulatory requirements tailored to tokenised investment funds, which warrant distinct consideration within the tokenisation taxonomy. Even where the token register is maintained solely on DLT, with no parallel traditional register, tokenised fund units would typically be classified as native tokens under this CP. However, their NAV remains derived from the underlying portfolio assets, which are generally held off-chain. Tokenised investment funds, therefore, raise regulatory considerations associated with both native tokens and digital twins. This warrants a tailored regulatory approach within the unified framework while preserving the core investor protection principles applicable to investment funds generally.

133. This section specifically addresses the primary offering of tokenised investment funds and the regulatory requirements applicable to operators of tokenised funds and their service providers in that context. It does not encompass secondary trading of tokenised fund units on secondary markets. Where tokenised fund units are traded on secondary markets, the applicable requirements for Secondary Offerors outlined in the preceding section of this CP would apply to those entities facilitating such secondary trading.

134. It is important to emphasise that operators of tokenised funds bear the ultimate responsibility for ensuring that all service providers appointed to the fund meet the requirements 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 CP as part of their obligations under the Minimum Licensing Criteria of the IFA.

**Tokenised Investment Funds**

135. The Authority recognises that many of the overarching requirements outlined in the previous section apply to operators of tokenised funds, while others require modification to address the specific characteristics of fund structures. The following clarifies how the general requirements apply to operators of tokenised funds:

*Due Diligence, Asset Verification and Legal Framework*

136. For tokenised investment funds, the relevant requirements outlined in the preceding section remain broadly applicable, with the following distinctions:

a) Operators of tokenised funds should ensure that fund custody and asset segregation requirements already provide appropriate protections regarding reserve assets and bankruptcy remoteness, and no additional requirements beyond existing fund regulations are necessary in this regard.

b) Operators of tokenised funds should ensure that legal assessment requirements require differentiation, as follows:

i. Where only the fund register is tokenised while underlying assets remain traditional, operators should ensure that legal assessment focuses primarily on ensuring the tokenised register conforms with laws and regulations of targeted jurisdictions, particularly regarding recognition of ownership rights and transfer mechanisms.

ii. Where the fund's portfolio includes tokenised assets, operators should ensure that the legal assessment requirement also encompasses the portfolio level, to ensure valid ownership and control of those tokenised assets within the fund structure.

*Risk Management Framework*

137. Operators of tokenised funds should ensure that the relevant requirements outlined in the preceding section remain broadly applicable, with the following distinctions:

a) Service Provider Risk: Fully applicable, with additional consideration required for fund-specific functionaries, including investment managers and fund administrators/transfer agents. Operators are responsible for assessing and monitoring these counterparty risks as part of their due diligence and ongoing oversight of service providers.

b) The stress testing, recovery and wind down planning requirements outlined in the preceding section are not applicable to tokenised investment funds, where tokenisation does not fundamentally alter the risk profile of the fund in a manner that would necessitate specialised stress testing, recovery, or wind down planning beyond what is already required for traditional funds.

*Outsourcing and Vendor Management*

138. Operators of tokenised funds should ensure that outsourcing and vendor management requirements outlined in the preceding section are fully applicable to tokenised investment funds. Beyond the technological considerations applicable to all tokenised assets, operators must ensure that investment funds also incorporate their various fund service providers within their outsourcing and vendor management programme.

*Reconciliations, Attestations and PoR - Modified Approach*

139. The requirements for reconciliations, attestations, and PoR outlined in the preceding section of this CP do not apply to tokenised investment funds. Given that tokenised funds maintain traditional NAV calculation methodologies and established fund accounting practices, these specialised verification requirements would be duplicative and unnecessary.

140. Instead, operators of tokenised funds should ensure that fund administrators 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.

*Conduct and Investor Protection*

141. For tokenised investment funds, the existing fund regulatory framework already provides robust investor protections. While the general conduct requirements apply to Primary Tokenisers, tokenised funds should primarily focus on transparency and disclosures, incorporating relevant tokenisation information into their standard offering documentation. Other requirements, such as market monitoring and customer education, may not be necessary given the existing fund regulations.

142. The Authority emphasises that tokenisation should not alter the fund's fundamental investor protection framework. Specifically, operators of tokenised funds should ensure that tokenised fund units maintain the same investor eligibility restrictions as their traditional counterparts. Tokenisation technology should not be used to circumvent established investor classification requirements – for example, by fractionalising units of a fund restricted to qualified participants to make them accessible to retail investors. Fund operators should implement appropriate technological controls within the tokenised register to enforce these restrictions and prevent unauthorised transfers.

*Cyber Risk*

143. All cyber risk requirements outlined in the preceding section that are applicable to Primary Tokenisers also apply to tokenised investment funds. Operators of tokenised funds should ensure that these requirements are properly implemented, either directly or through appropriate oversight of service providers. 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 requirements 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*

144. Investment managers of tokenised funds should conduct comprehensive due diligence on tokenisation platforms beyond standard financial assessments, examining technical capabilities, security protocols and compliance infrastructure. When selecting tokenisation infrastructure, managers should ensure alignment with both the fund's classification and

investor profile, implementing safeguards specifically designed for tokenised assets[17].

*Fund Administrators/Transfer Agents*

145. Fund administrators should adapt their processes to the tokenised environment by developing specialised NAV calculation methodologies (e.g., intraday or windowed NAV calculation) as disclosed in the fund's offering memorandum. Administrators should implement reconciliation processes bridging on-chain and off-chain records. For tokenised registers, administrators should ensure equivalent regulatory outcomes to traditional registers while leveraging DLT capabilities, explicitly designating in fund documentation which register constitutes the authoritative legal record[18]. As transfer agents, administrators should implement transfer restrictions, investor verification, and compliance controls directly within the register infrastructure, while establishing technical safeguards that ensure token transfers reflect legal ownership transfers and are documented with clear settlement finality across all relevant jurisdictions.

*Custodians*

146. Tokenised investment funds present distinct considerations regarding responsibilities across different tokenisation layers. For native-only registers, 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.

147. For tokenised assets held in the fund's investment portfolio, custodians should comply with all requirements referenced in the preceding section of the CP.

148. The Authority emphasises that while this subsection outlines specific requirements applicable to various service providers, the ultimate responsibility for ensuring compliance with these requirements rests with the operators of tokenised funds. Operators should conduct appropriate due diligence when appointing service providers, establish effective oversight mechanisms to monitor ongoing compliance, and take prompt action to replace any service provider that fails to meet these requirements. This responsibility aligns with the operators' broader obligations under the IFA to ensure that all fund service providers remain fit and proper at all times.

[17] For example, a tokenised fund marketed to sophisticated institutional investors may employ more complex smart contract structures than one designed for retail investors, who may require additional protections and simplified interfaces.

[18] Hybrid registers require continuous reconciliation mechanisms with near-real-time synchronisation and comprehensive audit trails that document all discrepancies and their resolutions.

***Question 15***

***(a) Do you support the Authority's proposed tailored approach to regulating tokenised investment funds, recognising their hybrid nature within the tokenisation taxonomy?***

***(b) Do you agree with the modified requirements for fund operators and service providers (investment managers, fund administrators/transfer agents, and custodians) that acknowledge the existing fund regulatory framework while addressing tokenisation-specific considerations?***

***(c) Are there additional fund-specific aspects that should be addressed in the regulatory framework for tokenised investment funds?***

## V. CONCLUSION AND NEXT STEPS

149. The Authority has undertaken a comprehensive examination of asset tokenisation through this CP, proposing a regulatory framework that balances innovation with effective regulation and supervision. This framework addresses the unique characteristics and risks of tokenised assets while maintaining proportionate, principles-based regulation.

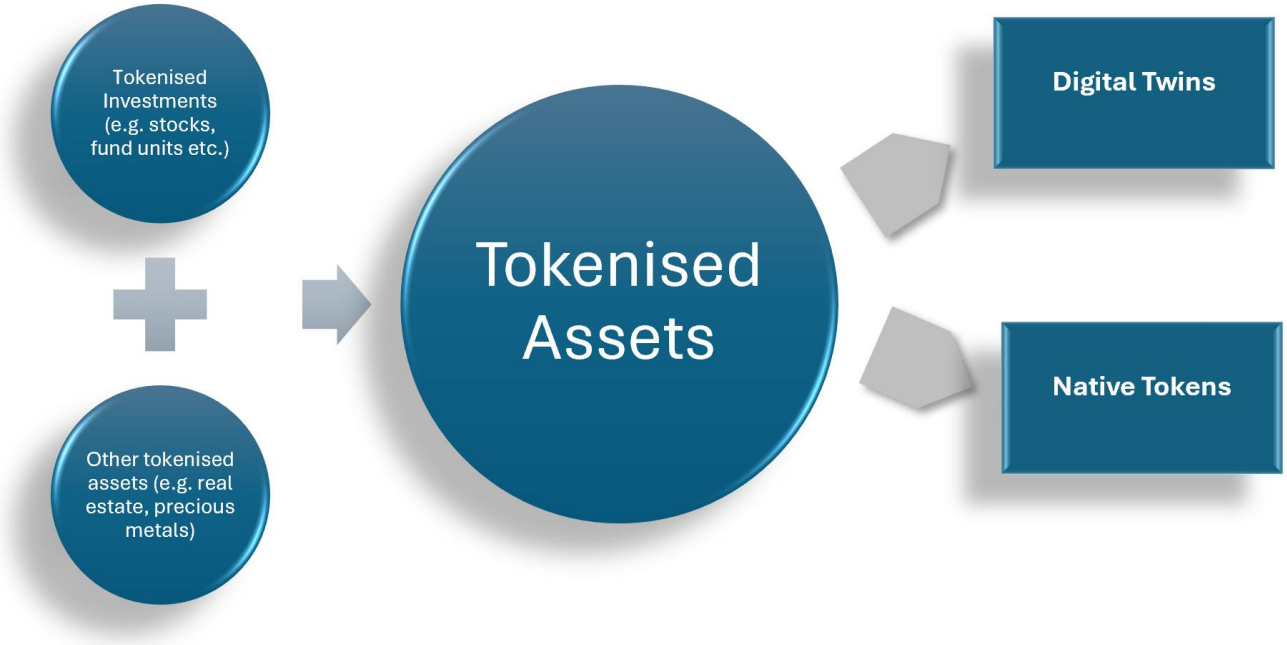
150. The proposed two-tiered approach, which combines a legal and regulatory architecture with entity-specific requirements, provides a comprehensive foundation for the tokenisation ecosystem. By distinguishing between Primary Tokenisers, Secondary Offerors and Custodians, and recognising the operational differences between digital twins and native tokens, the framework acknowledges the diverse business models and risk profiles within this emerging sector.

151. The Authority welcomes feedback on all aspects of this CP **by the close of business on 30 June 2026**. This input will be crucial to refining the proposed framework to ensure it remains effective and fit for purpose, and to foster an environment that supports responsible innovation in financial services while adhering to international standards and best practices.

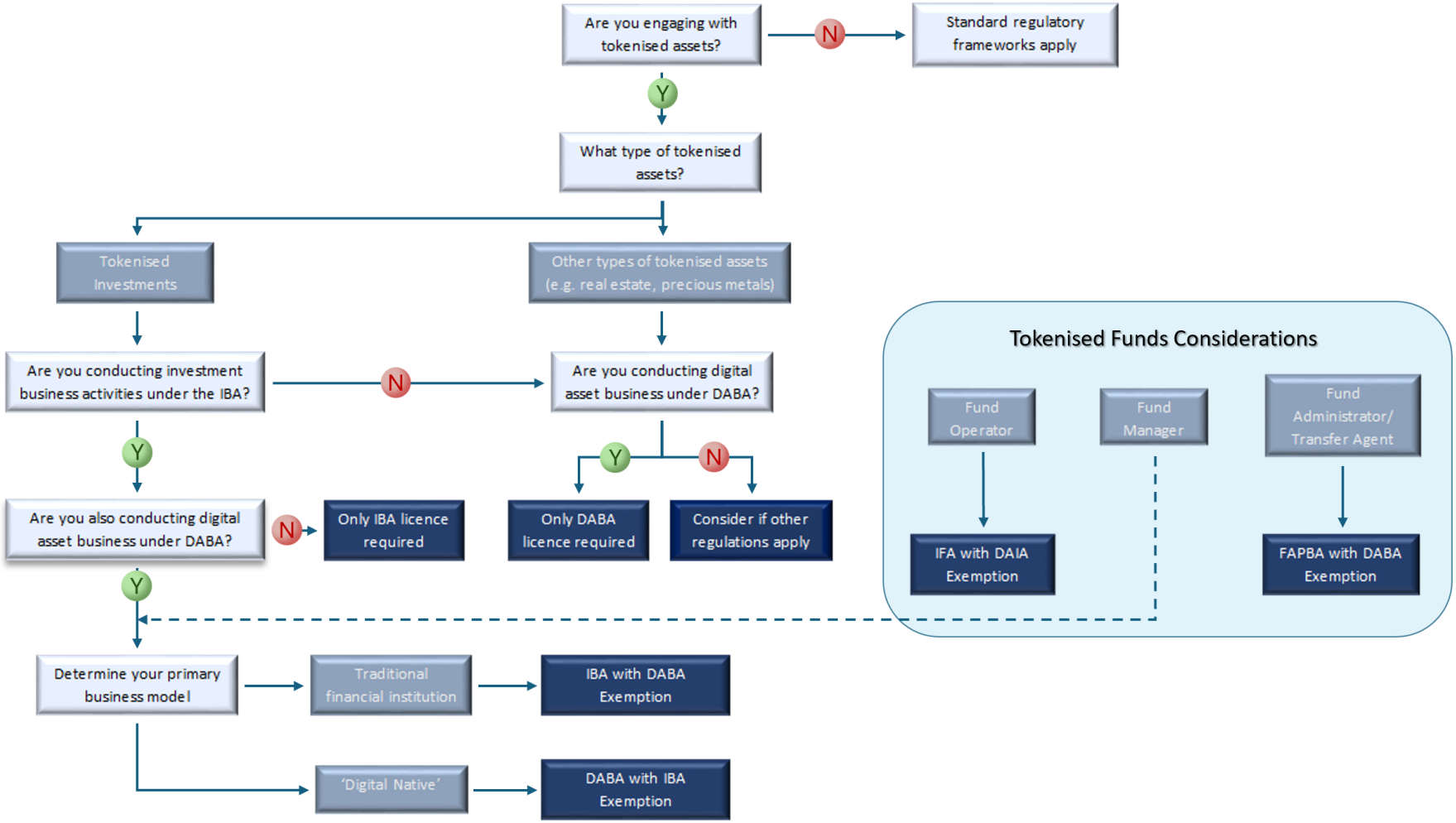
152. Following the consultation period, the Authority will analyse the feedback received and determine appropriate next steps, which may include legislative amendments, issuance of guidance notes, or other regulatory actions to implement the finalised framework.

**Annex 1: Tokenised Assets Taxonomy**

The following diagram illustrates the taxonomy of tokenised assets as described in this CP, highlighting their subdivision into two main categories based on asset classes that are being tokenised – tokenised investments (referencing investments as defined under the IBA) and other non-financial asset classes (e.g., real estate, precious metals) – as well as two categories based on the tokenisation approach: digital twin and native token.



## Annex 2: Regulatory Framework Decision Matrix for Token Assets



Bermuda Monetary Authority

BMA House

43 Victoria Street

Hamilton HM 12

Bermuda

Tel: (441) 295 5278

Fax: (441) 292 7471

Website: https://www.bma.bm