16 June 2025

ripple

Securities Commission Malaysia
3, Persiaran Bukit Kiara,
Bukit Kiara, 50490
Kuala Lumpur, Malaysia

Public Consultation Paper No. 1/2025: Proposed Regulatory Framework for Offering and Dealing in Tokenised Capital Market Products

Email: aFINity@seccom.com.my

Dear Sir/Madam,

Ripple Labs Inc. ("Ripple") welcomes the opportunity to provide feedback and comments on the Securities Commission Malaysia ("SC"s) consultation paper on a proposed regulatory framework for offering and dealing in tokenised capital market products ("Consultation").[1]

Ripple would like to thank the SC for the comprehensive efforts that have been undertaken in producing this Consultation, as well as for the opportunity to provide our comments. We respectfully request that you consider them as you consider the policy direction and development of a regulatory framework for tokenised capital market products.

Ripple, in partnership with the Boston Consulting Group, recently published a report on tokenisation,[2] which highlights that the financial industry is undergoing a significant transformation as tokenisation reshapes traditional asset management.

By converting assets into programmable, interoperable digital tokens recorded on shared ledgers, financial systems are becoming more efficient, accessible, and responsive to modern market demands.

The policy implications of this transformation are critical, and will need

[1] See https://www.sc.com.my/api/documentms/download.ashx?id=5a9a10e2-5872-4b48-9ea3-5b9635cc5179, *Public Consultation Paper No. 1/2025: Proposed Regulatory Framework for Offering and Dealing in Tokenised Capital Market Products.*
[2] See https://ripple.com/reports/approaching-tokenization-at-the-tipping-point.pdf, *Approaching the Tokenization Tipping Point.*

regulators and policymakers to develop regulatory frameworks that:

- Support Regulatory Harmonisation – Developing clear and consistent regulations across jurisdictions is crucial to facilitate the growth of tokenised markets.
- Infrastructure Development – Investing in robust digital infrastructures, including custody solutions and interoperable platforms, will support the scalability of tokenisation.
- Public-Private Collaboration – Engaging with industry stakeholders to establish standards and best practices will ensure the secure and efficient implementation of tokenisation technologies.

In developing a regulatory framework for tokenisation, Ripple recommends that the SC draw clear distinctions between three categories of tokenised assets:

1. Native Real-World Asset ("RWA") Tokens – Assets that originate and are issued directly on-chain, representing a legally enforceable claim without reliance on off-chain records.
2. Digital Twin Representation Tokens ("DTRTs") – Tokens that digitally represent off-chain real-world assets, such as capital market products issued off-chain. These tokens rely on a digital twin model, where the legal rights and obligations are still governed by off-chain frameworks.
3. Native Blockchain Tokens – Tokens that are native to public blockchains and are not backed by or linked to are not backed by or linked to legally enforceable claims (e.g., cryptocurrencies).

These distinctions are essential for tailoring regulatory requirements and applying appropriate safeguards to each asset type. Ripple encourages the SC to establish a clear regulatory roadmap that supports progression from digital representation tokens to native RWA tokens, thereby unlocking the full benefits of RWA tokenisation, including efficiency, transparency, and programmability.

In responding to this Consultation, we wish to bring to the attention of the SC the following key themes:

1. Embracing a flexible, forward-looking regulatory approach

As regulators globally continue to develop their capacity to regulate the tokenisation lifecycle, it is essential that regulators allow for a flexible, forward-thinking approach to the tokenisation of capital market products.

Ripple believes that limitations to the tokenisation process, be it on the class of underlying assets permitted or technology, would adversely affect the growth of the industry. Ripple also believes that a functional and risk-based approach that leverages regulatory sandboxes would serve to spur innovation and growth

of the sector.

2. **Enabling market growth and development**

Ripple firmly believes that institutional markets play a key role in scaling the tokenisation of capital market products. A clear pathway for this growth can be established through a combination of targeted short-term reforms and a longer-term regulatory assessment.

3. **Scaling tokenisation through institutional engagement**

Institutional participation is key to scaling tokenised markets, supported by short-term sandbox enhancements and long-term alignment of Distributed Ledger Technology ("DLT") with existing legal and regulatory structures.

In the short term, enhancing sandbox initiatives can create a practical testing environment for regulatory modifications that support tokenisation in capital markets. Over the longer term, a comprehensive evaluation of the alignment of DLT with existing regulatory frameworks – including securities laws, property and ownership rights, contract law, and clearing and settlement mechanisms – can help ensure scalability, regulatory clarity, and the sustainable development of tokenised capital markets.

4. **Need for clarity on native RWA tokens**

We welcome the SC's phased approach, beginning with digital twin representation tokens (on-chain tokens mirroring off-chain traditional assets), and a regulatory framework for native RWA tokens at a later time. However, we believe it is important to highlight the strategic trade-offs of this method.

While we acknowledge the rationale for prioritising digital twins based on regulatory readiness, we would encourage the SC to provide greater roadmap visibility for the treatment of native RWA tokens. This will be critical as regional capital markets begin to interoperate more closely, ensuring Malaysia remains well-positioned to capitalise on cross-border opportunities and maintain regulatory coherence with emerging international standards.

5. **Stablecoins as a key enabler in the tokenisation ecosystem**

Finally, Ripple believes that a tokenisation ecosystem will require several regulated and unregulated market players, including exchanges, on-chain analytic tools, insurance, etc. While Ripple understands that this consultation paper doesn't seek to regulate cryptocurrencies and stablecoins, Ripple believes that fiat-backed stablecoins would offer a low-risk enabler to capitalise on the full potential of tokenisation technology, by providing an

effective means of settlement for tokenised capital market products.

***

With this overview, Ripple respectfully submits the following responses to the questions outlined in the Consultation in the attached Appendix. We also welcome the opportunity for ongoing engagement with the SC on the development of a regulatory framework for tokenised capital market products.

Should the SC wish to discuss any of the points raised as part of this feedback to the Consultation, please do not hesitate to contact Rahul Advani (Global Co-Head of Policy) at radvani@ripple.com and Caren Tso (Policy Manager, APAC) at ctso@ripple.com.

Sincerely,
Ripple Labs Inc.

APPENDIX

Ripple respectfully submits the following responses to the proposals in the Consultation.

Q1: Please provide your comments and views on the proposed phased approach, i.e., the SC's current focus on digital twin representation tokens, and to only consider the introduction of a regulatory framework for native tokens in the future. Do you agree or disagree with this approach? Please elaborate your comments.

Ripple acknowledges the benefits of using a phased approach when introducing a regulatory framework, particularly in the area of asset tokenisation.

By focusing only on DTRTs, the regulatory framework can keep potentially complex issues such as legal finality and collateral management within traditional systems. These processes become particularly challenging from a regulatory and legal perspective when moved on-chain. This approach allows for a simpler framework that can be integrated more easily into the existing financial system and can act as a type of sandbox, allowing issues to be tackled and prepared for before later opening up the regulatory framework to more complex issues associated with native RWA tokens.

However, we would caution against such an approach without a clear roadmap for the introduction of later phases for native RWA tokens. We are aware of other jurisdictions that are already looking to solve the regulatory and legal challenges presented by tokenised capital market products on-chain, such as Project Acacia[3] by the Reserve Bank of Australia ("RBA") and the Digital Finance Cooperative Research Centre ("DFCRC"), and Project Guardian[4] by the Monetary Authority of Singapore ("MAS"). A phased approach could mean that Malaysia could risk falling behind on innovation and the domestic growth of the industry.

More importantly, such delays also risk isolating Malaysia from a global tokenised finance ecosystem that will develop on-chain, leading developers to look to other jurisdictions moving more proactively.

We would therefore recommend that the SC set out a clear roadmap for the regulation of native RWA tokens, including timelines for each stage and

[3] See https://www.rba.gov.au/media-releases/2024/mr-24-25.html, *RBA and DFCRC Joint Consultation Paper Project Acacia – Exploring the role of digital money in wholesale tokenised asset markets.*
[4] See https://www.mas.gov.sg/schemes-and-initiatives/project-guardian, *Project Guardian.*

industry consultations or discussion papers and legislative drafting.

Additionally, without a date in place for the introduction of a regulatory framework for native RWA tokens, the proposed regulatory framework, by limiting participation to existing traditional market participants and allowing only tokens that mirror the original asset without the utility, risks low levels of participation or becoming redundant.

Lastly, to fully realise the benefits of tokenisation, a robust settlement infrastructure is also essential. Tokenised assets require reliable digital assets for on-chain settlement to ensure secure and efficient transactions. Stablecoins have emerged as a crucial component of the tokenisation ecosystem, providing a middle ground between settlement in unbacked digital assets and fiat settlement, the latter of which undermines the benefits of tokenisation.

We believe that in order to achieve the maximum benefits available, it is important for the SC to remain agnostic in relation to the types of settlement assets available and permitted for use. This would allow for better cross-border interoperability, promote greater efficiencies and scale, and flexibility across the industry.

It is also important to recognise that asset tokenisation does not operate in isolation. For the long-term development of the tokenisation ecosystem, a successful framework that is holistic should be considered to foster innovation and create sustainable growth.

Q2: If you have issued or have been involved in the issuance of any tokenised capital market product, please provide your experience of such issuances, including, the type of capital market product that was tokenised, the tokenisation process and offering process as well as the challenges faced.

In particular, please also provide your comments on the following:

(a) What was the value proposition of the tokenised capital market product issued?

(b) What were the regulatory, legal, or technological impediments encountered? Please specify the key issues.

(c) What were the main risk areas identified, and what mitigation measures were implemented to address those risks?

Ripple has no comments on this question.

Q3: (a) Please provide comments and views on the above-mentioned proposed obligations on the issuer and RMO. Do you foresee any implementation issues and challenges in fulfilling these obligations? If yes, please describe your specific issues and challenges.

We would like to highlight several challenges in fulfilling these obligations in the short term and long term.

1. Clarification of Scope

Ripple recognises that the Consultation seeks to explore the tokenisation of various capital market products as defined under the Capital Markets and Services Act 2007 ("CMSA"),[5] specifically securities, derivatives, and unit trust schemes. The focus on digital twin representation tokens ensures that tokenisation is applied to products already within the SC's regulatory perimeter.

The framework's approach towards a technology agnostic, function-based and risk-based principle provides a sound foundation for the development of Malaysia's digital asset ecosystem.

While we agree with the importance of ensuring that issuers and RMOs seeking to adopt DLT have the necessary understanding and safeguards in place, we would like to highlight two key limitations in the proposed framework:

- Limited market participation: Restricting participation to entities already authorised as capital market participants could hinder broader market innovation and reduce the benefits of tokenisation.
- Narrow scope for participation: The framework's current scope, whilst appropriate for capital market products, may not address the increasing use of tokenisation for non-capital market assets, which will likely require broader legislative reform and cross-sectoral collaboration over time.

First, limiting participation to entities already authorised as capital market participants could restrict broader market innovation and reduce the benefits of tokenisation. Second, the framework's current scope, while appropriate for capital market products, may not address the increasing use of tokenisation for non-capital market assets, which will likely require broader legislative reform and cross-sectoral collaboration over time.

In considering the first limitation, we note that restricting participation to

[5] See https://www.sc.com.my/regulation/acts/capital-markets-and-services-act-2007, *Capital Markets and Services Act 2007.*

traditional capital market entities may constrain the potential benefits of tokenisation. Broader participation will be important to ensure that gains in efficiency, market access, and innovation are fully realised. Challenges in similar initiatives have been observed internationally. Under the European Union's DLT Pilot Regime[6], market infrastructure operators are required to meet the same capital, security, and operational standards as traditional financial market infrastructures. These requirements have resulted in limited adoption because the regime has not reduced frictions or costs, but instead introduced additional compliance complexities.

To avoid a similar outcome, the SC should consider designing a framework that facilitates broader participation while maintaining appropriate safeguards. Enabling a wider range of ecosystem participants could enhance the growth of tokenised capital markets in Malaysia.

On the second limitation, although the Consultation appropriately focuses on capital market products, tokenisation technology is increasingly being explored for other asset classes, including real estate deeds, commodities, and intellectual property rights.

For example, Ripple has supported groundbreaking pilots such as the Dubai Land Department's ("DLD") Real Estate Tokenisation Project,[7] a collaboration with the Dubai Virtual Assets Regulatory Authority ("VARA") and the Dubai Future Foundation ("DFF"). This initiative aims to set a global standard for on-chain real estate by directly linking title deeds to blockchain-based representations of ownership.

These developments fall outside the scope of the CMSA and would require further legislative reforms and coordination with other regulatory bodies. Over time, aligning the regulatory approach to these developments will be important to ensure comprehensive oversight of the digital asset economy.

2. <u>Importance of Secondary Market Participants</u>

Such restrictions may also impact the availability of secondary market participants, which are a key element in the success of a regulatory framework in this sector. Secondary markets play a vital role in ensuring liquidity and price discovery, making them essential for the operation of tokenised capital markets.

---

[6] See https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/dlt-pilot-regime, *DLT Pilot Regime.*

[7] See https://dubailand.gov.ae/en/news-media/dubai-land-department-launches-pilot-phase-of-the-real-estate-tokenisation-project#/, *Dubai Land Department Launches Pilot Phase of the 'Real Estate Tokenisation Project'.*

It is important to emphasise that liquidity is fundamental to the effective utilisation of capital market products, and this is where tokenisation can offer meaningful benefits. The value of tokenising assets does not lie merely in representing them on a blockchain, but in removing the frictions that impede their practical use. These frictions span the full lifecycle of an asset – from subscription and redemption processes, to secure custody, and on to more advanced use cases such as the deployment of assets as collateral. For instance, tokenised assets are unlikely to be accepted as collateral if there is no underlying market liquidity. Therefore, enabling liquidity must be a central consideration in any regulatory framework aimed at supporting the development of tokenised capital markets.

Therefore, we believe that to maximise the benefits of tokenisation, it is necessary to establish these key components within the secondary market:

- Demand-side factors: Investor participation and institutional adoption drive liquidity in secondary markets. Factors such as ease of access, interoperability with traditional financial systems, and efficient trading mechanisms will influence the level of demand for tokenised capital market products.
- Supply-side factors: The availability of tokenised capital market products on secondary markets is critical. This would require issuers, market makers, and liquidity providers to facilitate smooth trading.

An example of where such an initiative has fallen short can be seen in the Qatar Financial Centre ("QFC") tokenisation regime as part of its Digital Assets Framework 2024.[8] The framework was established with no previous infrastructure for secondary markets. What has become clear, as the QFC has struggled to operationalise this regulatory regime, is that for a tokenisation framework to be successful, there first has to be an operational secondary market and digital asset ecosystem (i.e. exchanges, insurance, and software providers that can provide the services necessary for the industry to operate). By restricting such a framework to existing traditional financial issuers and recognised market operators, therefore, the SC risks cutting off what has the potential to be a large sector of this market, which could be key in facilitating the necessary secondary market trading.

While secondary market development is essential to unlocking the full benefits

[8] See https://www.qfc.qa/en/media-centre/news/list/qatar-financial-centre-issues-qfc-digital-assets-framework-2024, *Qatar Financial Centre Issues QFC Digital Assets Framework 2024.*

of tokenisation, the SC should also be mindful of the potential risks associated with introducing liquidity into traditionally illiquid capital market products. Sudden liquidity can lead to increased price volatility, shallow market depth, and valuation instability as real-time market prices replace model-based valuations. It can also encourage excessive leverage or collateral reuse, amplifying systemic risks. Therefore, we recommend that the SC adopt a phased and measured approach to secondary market development, ensuring that market structures are resilient and that appropriate risk disclosures are in place to protect investors and promote sustainable liquidity growth.

3. Guidance on Ownership Mechanisms

The proposed regulatory framework would benefit from further guidance on the mechanisms to ensure consistency in the legal and beneficial title of tokens with the underlying capital market product. Under the current legal framework in Malaysia, ownership rights in securities and other capital market products are generally evidenced through centralised registers or depositories governed by the CMSA and the Securities Industry (Central Depositories) Act 1991 ("SICDA").[9] These statutes do not explicitly recognise digital or tokenised representations as legally conclusive proof of ownership. As such, the SC should set clear parameters and guidance on the legal status of tokenised records, particularly where discrepancies may arise between on-chain records and statutory registers, to avoid legal ambiguity.

4. Real-world Economic Value and the Future Steps Beyond Digital Twins

Having outlined the importance of secondary market infrastructure earlier, we now turn to the broader economic benefits that tokenisation can deliver.

The current focus on digital twin representation tokens addresses an important initial stage. However, tokenisation efforts should be directed at delivering measurable economic benefits, such as:

- Improved market efficiency: Tokenisation can streamline issuance, trading, and record-keeping processes by automating workflows through smart contracts. This reduces administrative overhead and operational delays, improving overall market efficiency.
- Enhanced liquidity: By enabling 24/7 trading and broader investor access, tokenisation can unlock liquidity for traditionally illiquid assets. Increased market participation and faster transaction settlement can contribute to deeper liquidity pools.
- Fractionalisation of assets: Tokenisation allows high-value assets to be

[9] See https://www.sc.com.my/regulation/acts/securities-industry-central-depositories-act-1991, *Securities Industry (Central Depositories) Act 1991* .

divided into smaller, tradable units. This lowers investment barriers, expands the investor base, and facilitates portfolio diversification.

- Improvements in settlement processes: Settlement times can be shortened through near-instantaneous clearing enabled by DLT. This reduces counterparty risk and minimises the need for complex reconciliation between intermediaries.
- Programmability and composability: Tokenisation could significantly reduce risk in complex business transactions by automating processes, minimising operational inefficiencies, and lowering costs. Furthermore, they enable the development and delivery of more sophisticated capital market products and services, making them accessible to a broader range of users and beneficiaries. By embedding logic directly into financial instruments and enabling seamless interaction between different digital components, programmability and composability have the potential to transform capital market infrastructure and expand market participation.

Looking ahead, it would be useful for the SC to consider a regulatory pathway for the direct issuance of native tokenised capital market products. These are products created, recorded, and transferred entirely on DLT-based infrastructure, without reliance on off-chain traditional records.

Issuing native tokenised capital market products could allow market participants to benefit from features such as programmable assets and more efficient market operations. Providing clarity on future regulatory plans in this area would support long-term industry development.

Q3: (b) In your view, are there any other additional general obligations that should be imposed on issuers and RMOs relating to the offering of tokenised capital market products?

We believe the following additional obligations could be considered to enhance the robustness of the framework:

1. Stress testing: Issuers and RMOs should be required to conduct operational stress tests on the DLT infrastructure. These tests should include assessments of smart contract robustness and resilience against cybersecurity risks to ensure the integrity and reliability of tokenised systems under adverse conditions.
2. Smart contract audits: Issuers should provide greater transparency regarding the audit status of smart contracts that underpin the tokenisation process. Disclosures should confirm whether the smart

contracts have undergone independent audits, and summaries of the audit findings should be made available to the public to promote trust and ensure investors are adequately informed about potential vulnerabilities.

3. Legal finality of ownership: Issuers and RMOs should clearly state whether the on-chain or off-chain record is considered the legally final record of ownership. Establishing legal finality is important to avoid uncertainty among investors and to reduce the risk of disputes in the event of discrepancies between different record-keeping systems.
4. Adoption of interoperability: Where applicable, issuers and RMOs should maintain interoperability standards to support cross-chain functionality. This would enable tokenised assets to move efficiently across different blockchain networks, reducing the risk of liquidity fragmentation and promoting broader market integration.
5. Secondary market disclosures: Finally, issuers should be encouraged to demonstrate how they intend to support liquidity in secondary markets. This could include providing information about arrangements with market makers or plans for listing tokenised products on trading platforms. Clear liquidity support plans would be important to ensure that tokenised capital market products are not only issued but also actively traded, thereby enhancing their market viability.

Q4: (a) Which type of DLT network would your entity prefer to adopt (e.g. private network, public network or any specified network)? Please elaborate the reasons for your preference.

In line with the SC's objective of regulations being designed and applied in a way that does not unfairly favour or disadvantage any particular technology, we strongly believe that the preference of DLT networks should be open to firms without limitation on certain models.

There is a growing consensus about the benefits of permissionless blockchains, including for financial use cases. In addition, permissionless blockchains are not all alike and do not pose the same risks. For example, the XRP Ledger ("XRPL")[10] is purpose built for institutional use, and incorporates features that make it suitable for regulated financial activities (such as permissioned domains and programmable compliance).

---

[10] *The XRP Ledger (XRPL) is a decentralised layer 1 blockchain renowned for its decade-long reliability and stability in tokenising and exchanging crypto-native and real-world assets. Designed to support businesses and builders, it is powered by XRP, a cryptocurrency purpose-built for payments. Trusted by over 1,000 visionary builders and businesses worldwide, the XRP Ledger offers institutional-grade functionality and built-in features to enable secure, efficient, and scalable financial services and use cases. It is more than just a blockchain – it is a global developer community dedicated to transforming future business solutions. Learn more at XRPL.org.*

Public and private DLT networks each offer distinct advantages and trade-offs, and the ability to select the appropriate network is key to maximising the benefits of DLT for financial markets.

Research and industry projects has consistently demonstrated that the choice between public and private DLT networks should be driven by application-specific risk, operational, and compliance considerations:

- DLT in Payment, Clearing and Settlement: An Analytical Framework Report[11]: Led by the Bank for International Settlements ("BIS") Committee on Payments and Market Infrastructures ("CPMI"), the report highlighted the trade-offs between public and permissioned DLT networks, noting that while public DLTs promote transparency and resilience, they introduce governance challenges, scalability constraints, and compliance difficulties, particularly for regulated financial markets.
- Project Ubin[12]: Project Ubin by the MAS explored the use of permissioned DLTs for interbank payments and securities settlement, and found that private DLT networks facilitated better control over participants, supported regulatory compliance, and enabled integration with existing financial market infrastructure.
- Project mBridge[13]: In collaboration with the BIS Innovation Hub Hong Kong Centre, the Hong Kong Monetary Authority ("HKMA"), the Bank of Thailand ("BOT"), the Digital Currency Institute of the People's Bank of China ("PBC DCI") and the Central Bank of the United Arab Emirates ("CBUAE"), the mBridge Ledger explored a hybrid permissioned DLT network for cross-border CBDC settlements. The project demonstrated that permissioned DLTs could achieve efficiency gains and regulatory compliance, balancing the openness of DLT with the need for participant verification and transaction privacy.

These studies collectively conclude that no single DLT network model is universally superior. Instead, network design should be tailored to the specific requirements of the financial product or transaction, balancing openness, security, scalability, and regulatory compliance.

Further, DLT introduces fundamental changes to market infrastructure, including decentralisation, immutability, and smart contract automation. These features enhance efficiency, security, and auditability but also introduce new

---

[11] See https://www.bis.org/cpmi/publ/d157.pdf, *Distributed ledger technology in payment, clearing and settlement: An analytical framework.*
[12] See https://www.mas.gov.sg/schemes-and-initiatives/project-ubin, *Project Ubin: Central Bank Digital Money using Distributed Ledger Technology.*
[13] See https://www.bis.org/publ/othp59.htm, *Project mBridge: connecting economies through CBDC.*

regulatory, operational, and legal risks. For example:

- Decentralisation: This increases resilience but complicates regulatory oversight due to the absence of a central controlling entity.
- Immutability: This ensures strong data integrity but presents challenges in correcting operational errors or addressing disputes.
- Transparency: This varies between permissioned and permissionless networks, impacting AML/CFT compliance and data protection.
- Consensus mechanisms: This affects the network security and efficiency, with different models such as proof of stake or Byzantine fault tolerance carrying distinct implications for scalability and governance.

Given the differentiated risk profiles and operational characteristics of public and private DLT networks, Ripple supports an open approach that permits the use of both models, subject to appropriate risk management, interoperability standards, and regulatory compliance measures.

Q4: (b) What factors should be considered in determining a suitable network?

Ripple would like to emphasise that no individual blockchain network serves as a complete end-to-end solution for financial use cases. The suitability of any given network should be evaluated within the broader context of the full technological and operational stack supporting the use case. Accordingly, we recommend that the SC develop a framework, and potentially a set of best practices, for assessing network suitability. However, the SC should avoid prescribing or endorsing a fixed list of acceptable networks, as this could inadvertently stifle innovation and limit flexibility in technology choices.

In determining a suitable network, several factors should be considered to reflect operational needs and regulatory requirements.

1. Privacy and Data Protection

One important factor to consider when determining a suitable network is the level of privacy that it offers users. Depending on the types of data that will be transacted through the network, entities may wish to seek additional layers of privacy. Networks may be required to facilitate sensitive financial and personal data, in which case, private networks are often better suited for adoption.

2. Governance and Regulatory Compliance

Another important factor is governance. Public networks offer some distinct advantages, such as transparency and open access. As highlighted in our

response in Q3(a), integration with secondary market participants, access to liquidity, and the generally stronger ecosystems and adoption rates associated with the public networks are important factors when determining suitability.

It is also important to consider how different blockchain architectures support the enforcement of regulated market practices and legal standards in capital markets. For example, consensus mechanisms such as Proof-of-Work ("PoW") and Proof-of-Stake ("PoS") may introduce vulnerabilities in transaction ordering and acceptance. These mechanisms can be susceptible to manipulation (such as front-running) due to the way in which anonymous or pseudonymous validators are selected to define the contents of a block or epoch.

This could raise questions about the reliability, transparency, and enforceability of key market practices in such environments. As such, we encourage the SC to take these technical characteristics into account when assessing the suitability of blockchain networks for regulated financial applications.

Ultimately, the decision should be based on a risk-based assessment of the network's ability to meet requirements for privacy, governance, transparency, liquidity, scalability, and regulatory compliance. Different applications may warrant different network models, and firms should retain the flexibility to select the network architecture best aligned with their operational and regulatory needs.

Q5: What type of controls and safeguards will your entity implement to address the risks that may arise from the use of DLT network? Please describe the specific controls and safeguards.

We believe it is essential that certain controls are in place to avoid assets being stolen, co-mingled with other assets, or otherwise misused.

1. Custody Arrangements

Effective custody measures are a key pillar of trust in all financial service industries and it is important to ensure industry best practices are being maintained. Custody methods can come in different formats, and should be best decided by firms based on their risk management framework. There are different ways to implement a custody regime to safeguard assets, such as self-custody and/or using a third-party service provider. Each format carries its own specific benefits and risks and will be more suitable depending on the business model or intentions of the investor or beneficial owner.

In line with the principle of “same activity, same risk, same regulation”, we believe that the SC should remain neutral in this regard and that there should be a focus on adopting international best practices and standards.

Self-custody, which carries its own specific benefits and risks, will be more suitable depending on the business model or intentions of the investor or beneficial owner. We believe it is essential to access and address the risk associated with different custody technologies and formats, maintaining a technological-agnostic framework while balancing security with operational efficiency. In relation to the associated risks, self-custody relies on the user maintaining access to their private keys and therefore if these keys are lost, the assets will likely be permanently lost. This contrasts with third party custody providers whereby key recovery mechanisms are usually in place.

However, self-custody also gives investors direct control over their assets, and eliminates the risk of a custodian’s insolvency or losses due to a cyber attack on a custodian provider. As such, we believe custody technology solutions should provide robust methods for key recovery in disaster scenarios where the key becomes unavailable or inaccessible.

2. Smart Contract and Security Audits

Given the nature of DLT networks, it is vital to ensure In addition to the general controls expected of a licensed entity in relation to cybersecurity and risk management, the nature of DLT networks means that controls in place to ensure the robustness and effectiveness of any smart contracts used are vital to safeguarding operations. Such controls are tested through audits of the underlying code and continuous monitoring of execution as well as initiatives such as bug bounties and penetration testing of the infrastructure.

3. Reconciliation Controls

Ensuring there are no discrepancies between tokenised records and the records of the underlying asset is critical. Controls should include real-time or daily reconciliation of parallel on-chain and off-chain records as well as clear procedures in place to investigate discrepancies, identify root causes, and for reporting to regulatory authorities where necessary.

4. Legal and Technical Finality Controls

To safeguard the rights of token holders, it is essential to establish clear and enforceable legal and technical controls. Finality controls include the implementation of robust token issuance agreements that clearly set out the

legal status of the token and how ownership is connected to the beneficial or legal ownership of the underlying asset.

Q6: (a) Please provide comments and views on the above-mentioned proposed requirements, including the requirement to maintain dual records, both on-chain and off-chain. Do you foresee any implementation issues and challenges in complying with these requirements? If yes, please describe your specific issues and challenges.

While we agree with the proposed requirement for the maintenance of dual records, an issue to consider is the potential legal issues that could occur should these records diverge, whether this is due to a technical or operational error. Divergences between the on-chain and off-chain records could create uncertainty regarding ownership rights and settlement finality, leading to disputes among investors, issuers, and market operators.

Given that current Malaysian laws generally recognise off-chain records as the legal source of truth for ownership, there is a need for clear guidance on how tokenised on-chain records would be treated in the event of any conflict. For instance, under the Companies Act 2016,[14] the register of members maintained by the company is deemed conclusive proof of legal ownership of shares under section 50. Similarly, under the SICDA Act,[15] ownership of securities is evidenced by entries in the central securities depository system operated by Bursa Malaysia Depository under section 35. These statutes do not currently recognise blockchain-based or tokenised records as authoritative for determining ownership.

Without clear regulatory guidance, there is legal uncertainty over whether on-chain tokenised records would have evidential value or legal standing in Malaysia's High Court in the event of discrepancies with statutory or depository records. This uncertainty could undermine investor protection and market confidence.

We recommend that the SC should issue clear rules and guidance requiring that any token issuance documentation specify from the outset which record, on-chain or off-chain, shall take legal precedence in the event of any divergence. This clarity would be essential for investor protection, legal

---

[14] See https://www.ssm.com.my/Pages/Legal_Framework/Document/Companies%20Act%202016_Akta%20777_BI%20(1.8.2022).pdf, *LAWS OF MALAYSIA ONLINE VERSION OF UPDATED TEXT OF REPRINT Act 777 COMPANIES ACT 2016 As at 1 August 2022.*

[15] See https://www.sc.com.my/regulation/acts/securities-industry-central-depositories-act-1991, *Securities Industry (Central Depositories) Act 1991 .*

certainty, and market integrity.

Additionally, maintaining dual records may pose operational challenges for entities, particularly with regard to:

- Real-time reconciliation of the two records;
- Increased costs and system complexity in maintaining parallel infrastructure;
- Enhanced cybersecurity and operational controls to prevent tampering or inconsistencies across systems; and
- Regulatory reporting and audit trail requirements for both sets of records.

Firms would need to ensure that robust reconciliation processes are implemented, supported by technologies that can automatically flag discrepancies and initiate investigation protocols in real time.

Q6: (b) Other than the obligations set out in paragraph 6.7 above, what would be the other appropriate steps that can be adopted by your entity?

Beyond the obligations set out in paragraph 6.7, we believe the following additional steps could strengthen the integrity and resilience of the dual record-keeping framework:

1. Real-Time Reconciliation and Audit Trails

Systems should be implemented that perform automated, real-time reconciliation between on-chain and off-chain records. These systems include

- Blockchain-based DLT platforms for on-chain records;
- Registry management systems or central securities depository ("CSD") systems for off-chain records;
- Reconciliation engines to monitor data consistency; and
- Cybersecurity frameworks to safeguard data integrity, and immutability audit logging tools to maintain verifiable records.

These systems help to generate immutable audit trails of all reconciliations and flag any discrepancies immediately for investigation and resolution.

2. Legal Finality Provisions in Issuance Documentation

In addition to the SC guidance, entities should embed legal finality provisions directly into token issuance agreements. These provisions should clearly establish the legal standing of records and outline dispute resolution mechanisms in the event of discrepancies.

3. Third-Party Audits and Certification

From a compliance perspective, firms should engage with independent third-party auditors to periodically review the reconciliation processes and verify the integrity of both the on-chain and off-chain records. Independent verification would provide additional assurance to investors and regulators.

4. Disaster Recovery and Business Continuity Planning

Firms should look to implement comprehensive business continuity plans that specifically address scenarios involving loss of synchronisation between the records. This should include backup strategies, failover systems, and contingency reconciliation protocols.

5. Smart Contract Safeguards

Where smart contracts are used in maintaining or updating tokenised records, firms should ensure that they include safeguards such as time-stamped logs, multi-signature approval for record updates, and built-in reconciliation triggers to mitigate risks of inconsistency.

Q7: Please provide your comments and views on the above-mentioned proposed requirement for issuers to disclose additional information, specifically:

(a) Are there any additional disclosures that are necessary to enable investors to make an informed investment decision?

In addition to the points listed in Section 6.8 of the Consultation, the SC may wish to consider the following key areas for additional disclosures to enhance investor protection and ensure informed decision making:

1. Custody and Safekeeping Arrangements

   The disclosure document should detail how and where the underlying capital market product is held, and whether the custody is managed directly by the issuer through self-custody means or by a third-party service provider. If a third-party custodian is used, the disclosure should specify the custodian's regulatory status, licensing details, and the jurisdiction in which custody services are provided.

2. Rights of the Token Holder

   The document should clearly specify the associated rights conferred by holding the token, including legal ownership, entitlement to dividends or profits, voting rights, and participation in corporation actions. It will also

be important to set out clearly any rights in the event of an insolvency of the issuer. This helps to clarify whether the token holders are treated as secured or unsecured creditors and any ranking in the issuer's capital structure.

3. Regulatory Status and Jurisdiction
   Issuers should disclose their regulatory status, including the relevant licensing or registration information, and specify the jurisdiction governing the issuance and operation of the tokenised capital market product. Additionally, various key individuals involved in the issuer's operations, such as the Board of Directors and Senior Management, should be identified, along with their qualifications and relevant experience.

4. Dispute Resolution Mechanisms
   Lastly, the document should include information on the mechanisms available for dispute resolution in the event of legal or contractual disputes. This should specify the applicable law, jurisdiction for dispute resolution, and whether arbitration, mediation, or court proceedings will be the primary mechanism.

Q7: (b) Do you foresee any implementation issues or challenges in complying with the proposed additional disclosure requirements, including those you have suggested above? If yes, please describe your specific issues and challenges.

We believe that the disclosure requirements set out in Section 6.8 of the Consultation are reasonable and aligned with investor protection objectives. However, we recommend proceeding with caution in requiring disclosures related to cybersecurity risks and mitigation measures.

Excessive public disclosure of cybersecurity frameworks, controls, or vulnerabilities could inadvertently expose issuers or RMOs to heightened security risks by providing malicious actors with information that could be exploited. Disclosing too much detail may undermine the very systems designed to protect market participants.

To mitigate this risk, we suggest that public disclosure in this area be limited to high-level information. For instance, issuers and RMOs could be required to disclose that they comply with internationally recognised cybersecurity

standards or certifications, such as ISO/IEC 27001,[16] without revealing specific system architectures, threat mitigation strategies, or internal vulnerabilities.

Q8: (a) Please provide your comments and views with regard to the above-mentioned proposed obligations of an RMO. Do you foresee any implementation issues or challenges in fulfilling these obligations? If yes, please describe your specific issues and challenges.

Ripple believes the obligations for RMOs set out in Section 7.2 of the Consultation are reasonable and in line with international best practices. While we appreciate the flexibility of the SC's proposals in Section 7.2 (c), particularly in relation to the requirement for RMOs to consider the features and risks of the tokenised capital market product when implementing custodial arrangements, we believe that RMOs would benefit from further regulatory guidance on key considerations.

The features and risks of tokenised capital market products in relation to custody can vary significantly. These may include:

- The level of control and access to private keys;
- Transferability restrictions imposed by smart contracts or token design; and
- The ability of tokens to exist across multiple blockchains, which can increase the complexity of custody due to interoperability issues and the need to manage protocol upgrades or forks.

Without clear standards, RMOs may face challenges in ensuring that their custody arrangements adequately address the specific operational, technological, and cybersecurity risks posed by different token structures.

Further guidance on risk assessment frameworks and recommended practices for digital asset custody would help RMOs implement more consistent and robust safeguarding measures.

Q8: (b) Other than the obligations imposed on a RMO as set out in paragraph 7.2 above, what would be the other appropriate steps that that can be adopted by your entity?

Ripple believes that the obligations set out for RMOs in Section 7.2 of the Consultation is reasonable and aligned with international best practices for market infrastructure operators.

---

[16] See https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en, *ISO/IEC 27001:2022(en): Information security, cybersecurity and privacy protection — Information security management systems — Requirements.*

While Ripple itself might not be considered a RMO within the Malaysian regulatory framework, we support RMOs and other market participants by providing blockchain infrastructure and solutions that facilitate secure issuance, transfer, and settlement of tokenised assets. Hence, our comments are made from the perspective of a technology provider supporting the broader tokenisation ecosystem.

We believe the following steps could further strengthen the operational resilience and investor protection framework for RMOs:

1. Independent Risk Assessments for Custodial Providers
   RMOs should conduct independent, periodic risk assessments of their third-party custodial service providers. This should include evaluating cybersecurity practices, private key management protocols, disaster recovery capabilities, and the financial health of the custodian.

2. Smart Contract Security Audits
   Where smart contracts are integral to the token's custody or transferability, RMOs should ensure that these contracts undergo independent third-party audits before deployment and periodic re-audits post-deployment, especially after protocol upgrades.

3. Token Standards and Interoperability Assessment
   RMOs should implement internal frameworks to assess the technical standards of tokens (e.g., ERC-20, ERC-1400) and their interoperability with custody systems and trading platforms. Tokens with multi-chain implementations should be subjected to enhanced scrutiny to ensure consistent custody practices across networks.

4. Custodial Insurance Coverage
   RMOs should consider obtaining insurance coverage to mitigate the risk of loss of tokenised assets due to cyberattacks, internal fraud, or operational failures at the custodian.

5. Business Continuity and Incident Response Planning
   RMOs should have a comprehensive incident response plan specifically addressing breaches or failures involving token custody. The plan should include clearly defined recovery time objectives ("RTO"s) and recovery point objectives ("RPO"s) aligned with international standards such as ISO 22301.

6. Investor Disclosure on Custody Risks
   RMOs should be required to disclose to investors key information about the custody arrangements, including whether custody is performed in-house or outsourced, and the nature of the safeguards in place. High-level disclosures on the custody risk management framework would enhance transparency and build investor trust.

Q8: (c) What other additional obligations that you think should be imposed, if any?

Ripple believes that a long term objective of the SC should be to foster and ensure interoperability among RMOs and traditional financial market operators. Interoperability is critical to enabling the scalability, efficiency, and institutional adoption of tokenised capital market products.

Traditional financial markets are designed to handle high transaction volumes efficiently, whereas many DLT networks face throughput limitations, congestion issues, and high latency. This can hinder the ability of DLT-based systems to process transactions at the speed and scale required for mainstream financial applications. Additionally, interoperability between DLT-based and traditional financial systems remains a concern, as existing financial infrastructure relies on centralised systems that may not seamlessly integrate with decentralised networks.

We recommend that the SC consider imposing additional obligations on RMOs to:

- Develop and implement technical standards that facilitate interoperability with traditional financial infrastructure such as clearinghouses, payment systems, and central securities depositories.
- Support interoperability between different DLT networks, particularly in the case where multiple RMOs may operate distinct blockchain platforms.
- Incorporate best practices in the use of cross-chain solutions, application programming interfaces (APIs), and messaging protocols that ensure consistency, data integrity, and efficient transfer of tokenised assets across systems.

Establishing a framework for interoperability at an early stage will be crucial to enabling broader market participation, facilitating cross-platform transactions, and ensuring that Malaysia's capital markets remain competitive and integrated

with global financial ecosystems.

Q9: (a) Please provide your comments and views on the above-mentioned proposed requirements related to technology risk management. Do you foresee any implementation issues and challenges with regard to issuers' complying with the requirements as set under the GTRM? If yes, please describe your specific issues and challenges.

Ripple does not see any concerns with issuers' complying with the requirements set out in the GTRM.

In relation to the robustness and integrity of smart contracts, we also believe further consideration should be given to whether certain business logic should be implemented on-chain, particularly in the context of tokenisation of capital market products, and whether doing so would be redundant or potentially introduce further technology risks.

While we acknowledge that smart contracts will be a vital part of the tokenisation process from issuance, to transfer, to redemption, many data driven events for capital market products are already handled in off-chain systems for the underlying asset. For example, interest payments linked to the reference rates such as the Malaysia Overnight Rate ("MYOR"), where a bond pays interest every six months if MYOR exceeds a specified threshold, or the early redemption of a callable bond based on market conditions, are currently managed through reliable business rules and off-chain data feeds in traditional finance.

Replicating this business logic on-chain through smart contracts could:

- Introduce unnecessary complexity and immutability risks;
- Increase costs due to the need for audits and maintenance; and
- Create vulnerability to coding bugs and operational errors.

Issuers and RMOs should carefully assess whether there is a clear operational or economic benefit to automating such lifecycle events on-chain. In many cases, particularly for digital twin representation tokens, the blockchain may be more appropriately used for recording and evidencing states such as token balances, ownership rights, and settlement finality, rather than encoding complex business logic.

Q9: (b) Other than the obligations as set out in paragraph 8.2 above, what would be the other appropriate steps that can be adopted by your entity?

As well as the robustness and integrity of smart contracts deployed, consideration should be given to the underlying presumptions and the laws upon which these smart contracts are predicated. While a common benefit of smart contracts is often that they are 'immutable', such a benefit can also create a technology risk in the event that the underlying presumptions or laws upon which the contract is based change. This can happen due to technological advancements or political purposes and can render a smart contract redundant overnight.

Ideally, smart contracts should be designed with adaptability and flexibility in mind. We believe rather than focusing only on deployment therefore, considerations should also be given to how smart contracts will be managed, upgraded, and extended where necessary.

Q10: Among others, the GTRM specifies that capital market participants *'must establish a technology audit plan that provides appropriate coverage of critical technology'*. Which critical components of the DLT would need to be included in the technology audit plan? Do you foresee any implementation issues or challenges in incorporating such components into a technology audit plan?

Ripple believes that a technology audit plan for tokenised capital market products should cover the following critical components:

1. Core Protocol and Network Governance
   Audit plans should begin with the foundational aspects of the DLT protocol itself. This includes the governance mechanisms, validator selection and incentives, consensus mechanisms, and the security of protocol-level operations. Any breaches at this layer could undermine the reliability and integrity of the entire tokenisation stack.

2. Smart contracts
   Audits should be conducted periodically on smart contracts to ensure that coding vulnerabilities, operational inefficiencies, or manipulation risks do not result in unintended outcomes such as unauthorised transfers. Audits should assess not only the underlying code but also the operational performance and security of smart contracts throughout

their lifecycle.

3. Custodial arrangements
   Audits should evaluate the effectiveness of custody controls, including the segregation of client assets and the robustness of procedures for managing events such as key loss, key compromise, or unauthorised access.

4. Disaster Recovery and Operational Resilience
   Audits should assess the adequacy of business continuity planning and operational resilience measures. This includes evaluating the scenarios and metrics used for stress testing and ensuring that contingency measures address both traditional risks such as physical disruptions and cyberattacks and risks unique to distributed ledger technology such as smart contract failures and consensus disruptions.

5. Off-chain Dependencies
   In addition to auditing on-chain components, an assessment should also be performed on off-chain dependencies such as external data feeds (oracles). This should include verifying the accuracy, integrity, and reliability of data inputs and assessing the risks associated with dependency failures or data manipulation.

In addition to a technology audit, an assessment should also be carried out to assess the reliance on off chain dependencies such as external data feeds. This should assess whether the data being received is accurate as well as the risk of manipulation or failure of these dependencies.

Q11: Please provide your comments and views on the above-mentioned proposed requirements to conduct due diligence on third-party service providers, and assess and manage any risk that may arise. In particular, please share your comments on the following:

(a) What are the key considerations that should be taken into account when conducting the due diligence?

When conducting due diligence on third-party service providers, Ripple believes that many of the considerations should align with the expectations for financial firms in the traditional sector. These include evaluating the provider's regulatory status, jurisdictional risk, track record, and operational experience.

Due diligence should also assess the provider's exposure to cybersecurity threats and the adequacy of its business continuity and disaster recovery plans. Controls must be in place to ensure operational resilience and the protection or compensation of clients in the event of a breach or security incident.

For third-party service providers offering custody and tokenisation solutions, additional technology-specific considerations are required.

1. Security Certifications and Standards
   Third-party providers should meet the highest industry standards for information security and custody operations. Relevant certifications include:

   - System and Organisation Control ("SOC") 1 for internal financial controls and SOC 2 for managing customer data;
   - ISO/IEC 27001 for information security management systems;
   - The Cryptocurrency Security Standard ("CCSS") by the Cryptocurrency Certification Consortium, which sets out requirements related to key and seed generation, wallet creation, key storage, key usage, key compromise policies, and access controls.

2. Custody Technology Models
   Due diligence should evaluate whether the custody provider employs Hardware Security Modules ("HSM"s) or Multi-Party Computation ("MPC") models:

   For HSM-based custody, service providers should offer bank-grade security. While devices certified at Federal Information Processing Standard ("FIPS") 140-2 Level 4 by the National Institute of Standards and Technology ("NIST") provide the highest level of assurance, devices certified at FIPS 140-2 Level 3 is generally considered the industry standard among financial institutions, and custodians, providing sufficient protection for secure key storage and recovery given their broader availability and operational practicality.

   For MPC models, it is important to assess whether the service provider holds or shares custody of private key material, and how security and recovery are managed.

Ultimately, the choice of custody architecture, whether HSM, MPC, or hybrid, should be determined by each market participant's specific risk appetite, regulatory obligations, and operational needs, while factoring in practical trade-offs such as implementation requirements, operational complexity, including any cold wallet operations, cost, and security requirements.

3. Deployment Models: Software-as-a-Service vs On-Premises
   Due diligence should assess whether custody solutions are deployed as Software-as-a-Service ("SaaS") or on-premises. SaaS solutions are hosted and maintained by the custody provider, while on-premises solutions are operated in-house or privately in the cloud by the issuer or RMO.
   - Service providers should offer both deployment models to accommodate the issuer or RMO's operational and regulatory needs.
   - Special attention should be given to the location of SaaS solutions. Solutions hosted outside of Malaysia may raise concerns regarding compliance with local data protection and privacy laws, whereas on-premises deployments are typically subject to local jurisdictional controls.

4. Key Management and Security Controls
   Due diligence should focus on how service providers generate, store, and manage private keys, ensuring there are no single points of failure that could result in the irreversible loss of assets. Risks could arise at the technical level, through vulnerabilities in software or smart contracts, during the transition between cold and hot storage, or from weaknesses in physical and human security protocols.

   Additionally, providers must implement internal controls to mitigate risks related to insider threats and collusion. This includes segregation of duties, strict access management, and continuous activity monitoring. The importance of such controls is underscored by recent industry incidents, such as the data breach at Coinbase, which was facilitated through compromised customer support channels.

Q11: (b) Do you foresee any implementation issues and challenges with regards to conducting due diligence based on the considerations that you have highlighted? If yes, please describe your specific issues and challenges.

While we believe the considerations highlighted reflect international best practices, we foresee several practical challenges in implementation that should be taken into account:

1. Vendor Transparency

Service providers, particularly in the custody and digital asset space, may be reluctant to disclose detailed internal security controls and custody architecture due to proprietary concerns and cybersecurity risks. This limits issuers' and RMOs' ability to conduct comprehensive due diligence.

Frameworks such as the Guidelines on Consumer Protection Measures by Digital Payment Token Service ("DPT") Providers[17] and the Swiss Financial Institutions Act ("FinIA")[18] governed by the Swiss Financial Market Supervisory Authority ("FINMA"), have introduced disclosure and auditability requirements to address similar challenges.

To balance transparency and security, we recommend requiring independent audits and certifications (e.g., SOC 1, SOC 2, ISO 27001, CCSS) and disclosure of high-level audit summaries to clients.

2. Auditability of Emerging Technologies

For newer custody models, such as those based on MPC or novel key management solutions, independent audits and certifications are not always widely available. This may pose challenges in verifying the robustness of the custody architecture.

3. Jurisdictional Risk and Compliance

Cross-border provision of SaaS custody services may lead to challenges in ensuring compliance with Malaysia's data protection, cybersecurity, and financial regulations. This risk is heightened where the service provider's data

---

[17] See https://www.mas.gov.sg/regulation/guidelines/ps-g03-guidelines-on-consumer-protection-measures-by-dpt-service-providers, *Guidelines on Consumer Protection Measures by DPT Service Providers [PS-G03] (revised on 19 September 2024)*. Under Section 3.4 that DPT service providers must implement robust risk management systems for safeguarding customer assets, including ensuring secure key management and cybersecurity frameworks.

[18] See https://www.fedlex.admin.ch/eli/cc/2015/853/en, *Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading, Swiss Financial Institutions Act (FinIA)*. Under Articles 9 and 11, and Financial Market Infrastructure Act (FMIA), Article 73e (as amended by the DLT Act, 2021), financial institutions and DLT trading facilities handling tokenised securities are required to implement internal controls, maintain operational resilience, and undergo independent audits.

centres are located outside Malaysia's jurisdictional oversight.

We recommend that the SC consider providing further guidance or industry templates for minimum due diligence standards for third-party digital asset service providers. This would help harmonise practices and reduce the burden on individual market participants.

Q11: (c) Other than the obligations as set out in paragraph 9.2 above, what would be the other appropriate steps that can be adopted by your entity?

In addition to the obligations set out in paragraph 9.2 of the consultation paper, Ripple recommends the following additional steps to strengthen risk management when engaging third-party service providers:

1. Continuous Monitoring: Entities should implement continuous monitoring frameworks to assess the service provider's operational resilience, cybersecurity posture, and compliance with service-level agreements. This includes ongoing threat intelligence monitoring and real-time security incident reporting.
2. Third-Party Security Audits: Service providers should be required to undergo periodic independent security audits conducted by qualified third-party auditors. Audit summaries or certifications should be shared with clients to promote transparency.
3. Incident Notification Requirements: Clear contractual obligations should be established requiring service providers to notify issuers and RMOs promptly in the event of security breaches, service disruptions, or any material incidents impacting client assets.
4. Exit and Recovery Plans: Issuers and RMOs should maintain contingency plans, including exit strategies and data recovery measures, to address potential service termination or failure of the third-party provider. This ensures the continuity of operations and the protection of client assets.
5. Vendor Risk Scoring and Periodic Reviews: Entities should assign risk ratings to third-party providers based on the criticality of services provided and perform periodic re-assessments to capture changes in operational risk or regulatory environment.

These additional measures would help ensure that third-party risks are continuously managed throughout the service lifecycle, not just at onboarding.

Q12: Please provide your comments and views on the proposed requirements for capital market participants to remain responsible for the tokenisation arrangement, including the record-keeping of ownership, regardless of the outsourcing arrangements that they may have regarding the tokenised capital market product.

(a) Do you foresee any implementation issues and challenges in complying with these requirements? If yes, please describe your specific issues and challenges.

Ripple believes this proposal is reasonable. Maintaining ultimate responsibility by issuers and RMOs, even when outsourcing, is critical to safeguarding the integrity of tokenised capital market products.

Q12: (b) Other than the obligation for an issuer and a RMO to be responsible for the management and operational soundness of the record-keeping of ownership, as set out in paragraph 9.4 above, what would be the other appropriate steps that would suit your entity towards meeting a similar objective?

As noted in our earlier response to Q6(a), robust reconciliation processes, backup record maintenance, and disaster recovery planning are essential safeguards. Additionally, to strengthen operational soundness, issuers and RMOs should implement a governance framework for outsourced record-keeping, mandate independent audits, and ensure compliance with international standards such as ISO/IEC 27001 or SOC 2. These measures would reinforce the integrity of ownership records and bolster investor protection.

Q13: (a) Please provide your comments and views on the above mentioned proposed requirements imposed on CMSL holders and registered persons.

While Ripple is not a CMSL holder or a registered person, we support the SC's proposed requirements for CMSL holders and registered persons dealing with tokenised capital market products.

Q13: (b) Do you foresee any implementation issues and challenges with regard to such requirements? If yes, please describe your specific issues and challenges.

Ripple has no comments on this question.

Q13: (c) Other than the requirements as set out in this Chapter 11, what would be the appropriate steps that can be adopted by your entity?

Ripple would like to suggest that the SC consider promoting the development of industry standards and providing practical guidance on best practices for conducting technology due diligence and smart contract audits, to support intermediaries in fulfilling these obligations.

Q14: (a) Please provide your comments and views on the above- mentioned proposed requirement for dealing in tokenised capital market products.

Ripple supports the SC's proposed requirements that dealings in tokenised capital market products should be restricted to trading venues and counterparties that are subject to strong regulatory oversight, particularly those with robust AML/CFT frameworks.

This approach aligns with international best practices and is essential to safeguard the financial system against cross-border risks and ensure investor protection.

Q14: (b) Do you foresee any implementation issues and challenges with regard to the proposed requirements for CMSL holders above? If yes, please describe your specific issues and challenges.

Ripple has no comments on this question.