Circle Internet Financial, LLC
99 High Street
Suite 1701
Boston, MA 02110

Basel Committee on Banking and Supervision
Bank of International Settlements
Centralbahnplatz 2
4051 Basel
Switzerland

27 March, 2024

Re: Consultative Document: Cryptoasset standard amendments

Dear Members of the Basel Committee on Banking and Supervision,

Circle Internet Financial LLC (“Circle”) appreciates the opportunity to respond to the consultative document by the Basel Committee on Banking Supervision (“Committee”) on amendments to the cryptoasset standard (“proposed guidance”). We continue to prioritize engagement with regulators and international standard-setting bodies in the development of sound financial guidelines for the cryptoasset sector.

As a global financial technology company, Circle provides a payment system for the near-frictionless exchange of digital fiat currency through open, public blockchains and networks that has gained significant and widespread market utilization. Circle has a keen interest in the development of a transparent and well-regulated digital assets ecosystem that facilitates capital formation, maintains fair, orderly, and efficient transactions, and protects consumers and the financial system at large. Partnership between the public and private sector is critical in developing technology-neutral, principled, activity-based regulation. Circle commends the Committee for continuing to engage with the industry in this respect.

Though Circle is not a bank, we issue USDC, the largest regulated tokenized cash payment stablecoin, and a euro-backed and denominated analog, EURC, which are central components of the cryptoasset ecosystem and provide critical touch points between banking and cryptoassets. USDC has been integrated as a settlement option in leading merchant and credit card networks; supports cross-border remittances and humanitarian assistance; and is deployed as a payment option by e-commerce platforms. Circle has engaged widely with regulators on the development of cryptoassets and stablecoin regulatory regimes and holds money transmission licenses in the 48 U.S. states and territories that require them; a conditional registration as a Digital Asset Service Provider (‘Prestataire de Service sur Actifs Numériques’) with the French Financial Markets Authority, and an e-money application actively under review by French authorities; and a Major Payments Institution license in Singapore. A full description of Circle’s activities, including discussion of its operational risk management practices, terms of use and legal rights, attestations to the reserves backing its tokenized cash products, and audited financial statements can be found on Circle’s website.

Please find below responses to select issues from the Committee's consultation document:

Conclusions from the Committee's Review of Permissionless Blockchains

The Committee's consultative response notes that the Committee has completed a review of the risks associated with the use of permissionless blockchain technology and concluded that cryptoassets utilizing permissionless blockchains are ineligible for inclusion as Group 1 assets. We note that neither the considerations supporting this conclusion nor the substantive analysis underpinning it have been made public and so, as a result, our ability to comment is limited only to the overall conclusion that certain unique risks of permissionless blockchains are unmitigable. Procedurally, we encourage the Committee to release its review and to ensure that going forward there is robust public-private dialogue particularly when it impacts existing BCBS principles and guidance, for example, in the case of third-party and operational risk management.

Based solely on the overall conclusion, Circle offers two overarching considerations to help guide future discussions on the risks around permissionless blockchains. First, it is important to note that permission involving blockchain-based networks, similar to that of the internet, exists on a spectrum and is not constituted by a binary determination of permissioned or permissionless. Indeed, very tightly permissioned or even closed systems can exist on top of blockchain in the same fashion that permissioned and very sensitive financial systems operate ubiquitously on the permissionless internet. Second, communications protocols like the internet and blockchain do not need to be regulated in order to allow heavily regulated applications involving sophisticated and secure multi-factor permissioning to be built on top of them.

For these and other reasons detailed below, we believe that cryptoassets utilizing permissionless blockchain technology should not be unconditionally excluded from Group 1b cryptoassets and that regulators and banks should be able to develop approaches that mitigate the risks and identify controls for permissioned applications utilizing permissionless chains. Over time, blanket restrictions will introduce unnecessary complexity to banks engaging with blockchain technology and further encourage development of financial services utilizing permissionless technology outside of the regulated financial sector.

Indeed, there is a strong argument to be made that banks should be encouraged to leverage blockchains, cryptography, mobile-enabled wallets and other open-source technologies in order to advance their digital transformation and cybersecurity efforts. As the Committee knows all too well, the failure of any one bank, erodes confidence in banking. And yet, most banks, particularly small to mid-sized institutions, cannot keep up with the digital transformation space race taking place among larger global banks. Meanwhile, consumer and market preferences for technology-enabled financial services will continue stretching resources across the sector to remain relevant and competitive. Rather than stigmatizing blockchain-based financial services, Circle's successful operating experience and deep partnership with global banking institutions, suggests there is a collaborative model and opportunity at hand, which banks can benefit from and the Committee should encourage.

To contextualize the above points, we believe it is important to differentiate between the layers of blockchain-based services and the implications on permissioning. Circle, as the issuer of USDC and EURC, retains deep experience in developing and implementing permissioned systems and controls via programmable and permissible smart contracts on top of the underlying permissionless blockchain infrastructure. Based on this operational familiarity and as a regulated financial institution, we highlight the following to help inform the discussion of blockchain infrastructure:

1) **Data validation layer:** The data validation layer is the base layer of a blockchain protocol which determines the format, sequencing, and validation into blocks of information similar to how the Internet Protocol (IP) system routes packets of information and governs the information flow between a network of servers that constitute the world wide web. Like IP, data validation on blockchains is use-case agnostic and centers on computations based on inputs to create an archival record. Permissioning at this layer applies to the type of information that can be processed and recorded on the blockchain by validators and sequencers (i.e. it is not a function of simply "gating" participants). Importantly, at the data validation layer, the network will continue to function regardless of whether there are few or many participants; however, network utility, security, and resilience to disruption may be reduced as permission is narrowed to a smaller number of participants (i.e. validators for blockchain and servers for the internet).

   Likening this to the SWIFT Society's banking network, the data validation layer would be akin to the SWIFT Society's utilization of Internet Protocol and Extensible Markup Language (XML)[1] underpinning the SwiftNet application as well as for connecting SWIFT's four data operating centers (OPC) that process transaction messages. Each OPC and application utilizing the internet has different levels of permissions to limit access and provide security (further described below); however, network data would be processed on the permissionless internet by servers maintained, and paid for, by third and fourth-party service providers.

2) **Application-level permission:** The next level up is the smart-contract or application layer in which network participants offer Application Programming Interfaces (APIs) and services determined and governed by the application developer or smart contract programs. Like applications built on the internet, this level is generally viewed as being available for "permissioning" as it is governed by the policies and terms unique to the application provider. Common permissioning criteria for blockchain-based financial

[1] Swift website, "SwiftNet Link," accessed 14 March, 2024.

services include limitations to: customers or contractual relationships; lack of identification on a sanctions list; or transaction history risk profile. Similar to the internet, the ability to control an application or designate permission does not depend on the data validation layer or network accesses governing the data layer, preserving the discretion of the application provider to determine solutions (scaling, identify management, etc.) to comply with its regulatory requirements.

Drawing from the SWIFT analogy, the SWIFT Society as a corporate entity would issue the policies governing the use and eligibility to access its APIs that are then permissioned to its global network of SWIFT-participating banks, subject to SWIFT's compliance monitoring.

3) **User-interface level:** The most widely accessible level is the user-interface layer in which individuals engage with the blockchain or internet protocol either indirectly through APIs or smart-contracts such as wallets, custody tools, etc. As with the application layer, the user-interface layer can be permissioned, the degree to which depends on the function intended by the application providers. For example, access to a financial smart contract-based application may be subject to a financial institution's direct permissions, while access to blockchain wallets or mobile banking services utilizing an API may be further permissioned based on security or other factors consistent with the Committee's existing guidance on third-parties and operational resiliency.

In keeping with the SWIFT analogy, a user interface service could be considered the SWIFT member bank's mobile banking wallet in which a user can input the information to support a fund transfer message processed through the SWIFT system. In such a case, the mobile banking tool would be issued and permissioned by a third-party bank of the SWIFT Society with separate permissions based on the bank's own KYC and other regulatory requirements.

Based on these structural elements and the similarities between web- and blockchain-based permissioning, we believe that it is critical to approach both protocols from a similar regulatory framework before introducing standards that could lead to differing interpretations of existing Committee guidance depending on the technology used. Fundamentally, regulating blockchain at the application layer preserves the discretion of national regulators to apply existing financial services rules on an activities basis whereas regulating at the protocol layer – as the Committee's conclusion appears to advocate – creates a "one-size-fits-all" regulatory standard, while breaching the spirit of technology-neutral, activity based regulations. Additionally, we see an apparent difference in the Committee's approach to blockchain versus internet-based protocols in which the Committee has focused on a "risk elimination" standard with blockchain technology versus a "risk-based mitigation" approach with permissionless internet protocols. It is important to note that neither banks, the SWIFT Society, nor governments can fully mitigate the risks present at the internet protocol layer whether for permissioned or permissionless financial services built on top of it, including, for example, risks from data processing involving services paid for by unverified and unknown service providers.

Looking more narrowly at the proposed guidance, the determination of unique and unmitigable risks for blockchain likewise seems to contradict previous guidance regarding network reliance on third-parties, due diligence, and resilience for critical services. The Committee's 2021 guidance on the "Principles for Operational Resilience" emphasizes that banks take a due diligence-driven approach to third-parties and resiliency-based approach to critical cyber and network operations. It will be important to understand the Committee's assessment of how these principles are applied with third party blockchain protocols and, importantly, when the 2021 guidance may be superseded with respect to Group 1b or 2 cryptoassets, including any technical factors that make certain technological risks at the protocol level unmitigable.

Lastly, we encourage the Committee to conduct further assessment into the potential tradeoffs involved between the different degrees of permissioning at the various protocol layers. For example, a central facet of the blockchain data protocol layer is the relationship between distributed ledger network security and the size of the network. Permissionless distributed ledgers consisting of a geographically diverse network of validators offer significant security and network resiliency benefits when compared to permissioned protocols that may consist of one or few validators. Financial and anti-money laundering experts have noted that permissionless blockchains offer significant cyber-security enhancements over traditional systems both by increasing the challenge to would-be abusers and by creating widely visible and traceable records.[2]

Falsification of blockchain transactions becomes exponentially more challenging as the network of validators grows, leaving permissioned systems at potential greater vulnerability to insider or external threats. Permissionless protocols likewise offer added resiliency benefits by acting as continuously verifiable point-in-time snapshots of the distributed ledger for both issuers and banks. These together can play a critical role in business continuity and contingency planning in the event of disruption at the application layer or user-interface layer. We would urge the Committee to make clear its position on the relationship between network security, business continuity, and the degree of permission as well as the interplay between these factors as part of multi-organization networks.

There is something to be said for leveraging constantly upgradable open-source technologies in banks and banking. Too many of the world's financial technologies, particularly closed or legacy systems, labor under single points of failure or end up catering to the competitive advantage of single, well-endowed large banking institutions, rather than advancing the state of the industry

[2] Michael Mosier, Written testimony before the U.S. House Financial Services Committee, 15 February, 2024.

overall. This in turn can lead to a veritable technological moral hazard – where technological advantages accrue to large, first mover banks, while midsized and small institutions grapple with seeking permission rather than forgiveness from prudential regulators. Overly prescriptive rulemaking, especially in the convergence of digital assets and blockchain-based financial services with banking, may inadvertently skew a technology and sector that greatly favors banks and can level the playing field between banks and fintechs, rather than being an unchecked source of risk.

SCO60.12 - Eligible Reserve Assets and Reverse Repurchase Agreements

We appreciate the Committee's consultative reengagement on the issue of eligible reserve assets and, in particular, the discussion of additional classes of eligible reserve assets for Group 1b cryptoassets. We agree with the general principles that eligible reserve assets have: 1) short maturities; 2) high credit quality; and 3) deep liquidity even during stress periods. We likewise largely agree with the Committee's conclusions regarding some of the considered reserve assets such as cash borrowed via repurchase agreements. However, we encourage the Committee to make several modification to the reserve management criteria that together would support more effective market risk and general reserve management:

1. *Reverse repurchase agreements* should be explicitly included as eligible reserve assets in SCO60.12(2)(c): short-duration (one week or less) reverse repurchase agreements backed by Level 1 high quality liquid assets (HQLA) consisting of marketable securities.

2. We encourage the Committee to explicitly allow *regulated custodial reserve management structures* that consist solely of eligible reserve assets, including regulated money market funds, to SCO60.12(b).

3. The requirement for banks that hold cash deposits to apply the Basel Framework (including the Liquidity Coverage Ratio) should be subject to a materiality threshold in order to facilitate settlement and transaction services.

Reverse Repurchase Agreements backed by Level 1 HQLA

At a principles level, we believe it is important for Group 1 cryptoasset issuers to retain access to the standard cash management tools that are widely and effectively used in managing liquidity, credit, and duration risk. Reverse repurchase agreements play an important role in global markets in this respect, helping manage credit risk as well as market risk in sovereign debt markets. Circle currently uses reverse repurchase facilities backed by short-duration U.S. Treasurys held at GSIB counterparts as an important reserve management tool within Circle's custodial reserve fund. From a macro-prudential management standpoint and at a principles level, reserve management of Group 1b cryptoassets should be explicitly built on top of the full suite of Level 1 HQLA credit and duration risk management tools currently available to financial risk managers. This is critical to avoid putting issuers at risk during periods of market fluctuation and to avoid the concentration of risk as the Group 1b cryptoasset sector grows. Importantly, this is consistent with the Committee's 2017 guidance on the Liquidity Coverage Ratio which treats HQLA-eligible assets that constitute all or a part of a pool of collateral for reverse repurchase agreements in the stock as HQLA, provided they are overcollateralized.[3]

Limiting available reserve assets only to a subset of high quality, highly liquid reserve assets may have the unintended effect of concentrating risks in issuers that could, over time, cause an accumulation in the Group 1b sector. For example, large concentrations of deposits could serve as a transmission risk to holders of a stablecoin as well as to the depository institution even subject to concentration limits and spread across depository institutions. During periods of sovereign debt concerns – for example relating to U.S. debt limits – issuers may seek to reduce market risk by shifting assets to short-duration reverse repurchase agreements. Indeed, many well-managed cash funds shifted assets away from Treasury markets to reverse repurchase agreements during the summer 2023 U.S. debt ceiling negotiations. The current construct would limit issuers' ability to shift to safer assets outside of cash, likely leading to larger concentrations of bank deposits which could transmit risk to holders of the issuer as well as the depository institutions. As the sector grows, this limitation could create the potential for more systemic vulnerabilities. Layering reserve management on top of the full suite of Level 1 HQLA liquidity tools available to the financial system would de-risk Group 1b cryptoassets and reduce susceptibility in the sector to swings in a narrower pool of eligible reserve assets.

The Committee notes in its discussion that stablecoin issuers may not have the legal right or operational capacity to monetise collateral with sufficient speed. From an operational perspective, Group 1b issuers – based on the current composition of eligible assets – will already have the capacity to liquidate collateral held for marketable securities representing claims on or guaranteed by the sovereign. Additionally, the Circle reserve fund maintains the legal right to liquidate the underlying assets which, when combined with the fund's overcollateralization, results in both the capacity, legal rights, and liquidity risk management to allow for timely redemption of reverse repurchase agreement holdings.

As a result of these factors, we encourage the Committee to allow issuers to balance their reserve portfolios to address periods of market fluctuation and allow better management of credit risk. Short-dated (one week or less) reverse repurchase agreements overcollateralized solely by Level 1 HQLA – like government debt instruments – present an important alternative that can help provide short-term liquidity and manage credit and duration risk to both issuers and custodians.

[3] BCBS, "Basel III: The Liquidity Coverage Ratio framework, frequently asked questions," June 2017.

Regulated Money Market Funds Comprised Solely of Eligible Reserve Assets

We likewise encourage the Committee to make explicit the ability for issuers of Group 1b assets to utilize institutional reserve management services offered by approved custodians, including use of money market funds consisting of eligible reserve assets. Circle currently holds a portion of its reserve assets in an SEC-registered government money market fund managed by a leading global custodian. The portfolio consists of a mix of short-dated U.S. Treasurys (with maturities of 3 months or less), overnight U.S. Treasury reverse repurchase agreements with leading global banks, and a limited amount of cash. In addition to the institutional reserve and liquidity management expertise brought to bear by the custodian, such funds offer additional transparency to consumers and segregation of customer funds consistent with the requirements and objectives of SCO60.12(4). Assets Under Management of the Circle Reserve Fund are publicly available via the fund ticker with real-time, verified metrics, which is a stark contrast to the lack of transparency inherent in even well-established payment systems and e-money companies.

The Circle Reserve Fund is also subject to the requirements of the U.S. Investment Company Act of 1940, including oversight from an independent board and daily reports on fund portfolio holdings. Additionally, the Circle Reserve Fund does not contain any Circle corporate assets and are held for the benefit of USDC customers only. We see this segregated structure as beneficial for USDC holders and institutional partners alike and an important part of our conservative reserve management model.

This treatment has already been adopted in key regulatory frameworks such as the EU's Markets in Crypto Asset Regulation (MiCA), which explicitly includes reserve assets in undertaking for collective investment in transferable securities (UCITS) consisting of other eligible reserve assets and subject to concentration limits.[4] As a result, we recommend the Committee include an additional sub-section to SCO60.12(b) that stipulates that reserve assets can be placed in custodial reserve management structures, including money market funds, consisting solely of eligible reserve assets.

Materiality Threshold for Cash Held at Banks

Lastly, we recommend the Committee amend the requirement for banks that hold cash deposits to apply the Basel Framework (including the Liquidity Coverage Ratio) to establish a materiality threshold. Not all banks are required to implement the Liquidity Coverage Ratio, and this requirement would limit the banking partners available to Group 1b issuers to facilitate settlement and transaction services. The implementation of a materiality threshold for deposits at these

[4] EU Markets in Crypto Asset legislative text, Article 38 "Investment of the reserve of assets," subsection 2.

institutions could effectively limit exposure to manageable levels; particularly for firms with sound risk mitigation strategies. The ability for a stablecoin issuer to establish these banking relationships would also enable the creation of further redundancies to facilitate transaction services.

SCO60.12(4) and SCO60.20(3): Stabilization Mechanisms

Circle recognizes and agrees with the importance the Committee places on ensuring effective stabilization in comparison to the cryptoasset's referenced assets and appreciates the careful analysis during the first two consultations regarding the basis risk test and stabilization. In particular, we agree that the management of reserve assets must be comprehensive in order to ensure cryptoassets can be redeemed promptly at peg value, including under periods of stress. However, there remain key differences between the stabilization mechanisms for Group 1b and Group 2 cryptoassets that we believe should be taken into account before imposing the additional, and potentially duplicative, stress testing requirement in SCO60.20(3) on top of those in SCO60.12(4).

In distinguishing between Group 1b and Group 2 cryptoassets, we note that effective stabilization mechanisms for Group 1b asset-referenced cryptoassets depends on the ability for Group 1b issuers to convert reserves to fulfill timely redemption at par with the underlying reference assets. Similar to other exchange markets, this ability rests on meeting the primary market demand and not the stability of secondary market prices. Studies have often overemphasized the peg price of stablecoins in secondary markets;[5] however, this misses the crucial point that the ability of stablecoin issuers to fulfill redemption lies in the strength of their balance sheets and effective liquidity and reserve management. Even in times of stress or heavy redemption, secondary market price does not have any bearing or influence over the issuer's ability to redeem holder funds – which for regulated stablecoin issuers like Circle is a paramount fiduciary obligation enshrined even in today's state money transmission and electronic stored value laws.

Conversely, Group 2 cryptoassets rely heavily, if not solely, on secondary markets for stability, a distinction that should be noted. The primary market involves the direct issuance and redemption of stablecoins against fiat currencies from the issuer, ensuring that the price of conversion remains at parity. Table 1 shows the parity in primary market redemption for USDC – even in times of market stress – which reflects the nature and liquidity of Circle's reserve holdings. Furthermore, primary redemption markets account for 95 percent of volume of exchange between USDC and USD.

[5] Gorton, G B, E C Klee, C P Ross, S Y Ross, and A Vardoulakis (2023), "Leverage and stablecoin pegs", VoxEU.org, 23 February.

Table 1 - Price distribution of tokenized cash in primary and secondary markets[6]

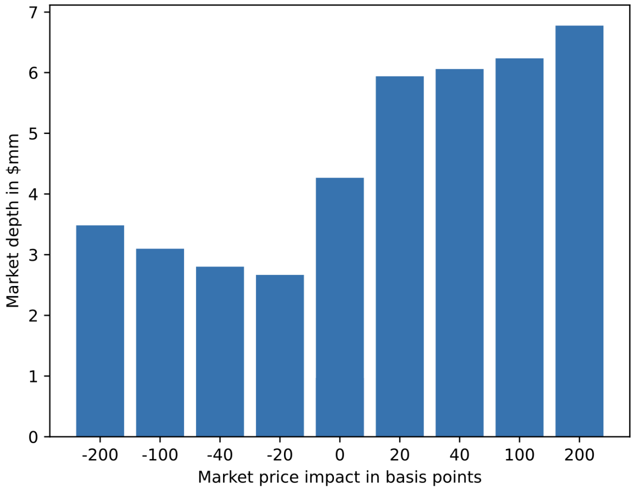
		Daily volume weighted average price of USDC in USD					
Market	**Average daily volume ($millions)**	**Min**	**1%**	**Mean**	**50%**	**99%**	**Max**
Primary	$648.6	$1	$1	$1	$1	$1	$1
Secondary	$33.3	$0.9452	$0.9991	$0.9999	$1.0000	$1.0007	$1.0109

On the other hand, secondary markets for the conversion between stablecoins and fiat currencies tend to be relatively illiquid and are particularly shallow over weekends. Circle has found that many major global exchanges and market makers maintain thin USDC liquidity, particularly over weekends, that significantly amplifies both the potential and magnitude for secondary price dislocation in those markets. Table 2 highlights the impacts of the comparative lack of liquidity in secondary markets in USDC which may temporarily deviate from parity. The table reflects that even on the largest secondary market for USDC to USD conversion, Kraken, there is an average market depth of roughly $3 million for 1 percent price impact (i.e. a “depeg” of 1 percent on the exchange is extremely likely if a single customer orders more than $3 million USDC). Price dislocation in this case reflects the relative illiquidity rather than underlying stability of the token. Importantly, the depth of liquidity within secondary markets is entirely outside of the issuer’s control and, as a result, we strongly believe it should not be taken into account when determining the efficacy of the cryptoasset’s stabilization mechanism for Group 1b cryptoassets.

Table 2 - Market depth on Kraken for USDC/USD[7]

[6] Note: This table shows the daily price distribution of USDC in USD and the associated volume in the primary and secondary market. The primary market volume is the sum of gross daily issuance and redemption. The secondary market volume and price are based on the conversion rate of USDC to and from USD on exchanges. The price and secondary market volume data are from Kaiko. The sample period is from 1 March 2021 to 13 March 2023, inclusive of the weekend of 11 March 2023, during which the secondary market prices of USDC temporarily deviated from parity in the aftermath of the collapse of Silicon Valley Bank.

[7] Average market depth on Kraken for USDC conversion to USD from February 2024. Source: Kraken; Circle staff calculation.



Affirming the treatment in SCO60.12(4), balance-sheet-based analyses of tokenized cash stablecoins show that a model of stablecoin issuance backed by full reserves held in highly liquid, short-term assets can have a liquidity ratio that is both independent of secondary markets and stronger than that of typical banks which fractionally lend.[8] As Table 3 shows, the liquidity ratio of tokenized cash ranges from around 200% to over 800%, based on historical observation of run rates and varying assumptions which is a direct result of the full-backing model employed by tokenized cash stablecoins, in stark contrast to the fractional-reserve banks that tend to hold a significant portion of illiquid assets.[9]

Table 3 - Liquidity ratio side-by-side comparison[10]

Assumption	Outflow rate	Liquidity ratio
Standard Basel LCR non-operational deposit outflow rate	40.0%	200%
Observed USDC 30-day worst outflow rate with inflows capped at 75% of outflows	9.2%	870%
Observed USDC 30-day worst outflow rate with 0% inflow	36.9%	217%
U.S. GSIBs' LCR average 2022Q4		120%

As a result, Circle believes that it is important to focus assessment of stabilization mechanisms for Group 1b cryptoassets purely on the reserve management criteria captured in SCO60.12(4) which are designed to effectively monitor and assess the risks to the reserve and for timely liquidation. SCO60.20(3) is duplicative and interchangeable with SCO60.12(4)(d) and could add additional

[8] Liao, Gordon (2022), "Macroprudential considerations for tokenized cash", SSRN Working Paper.
[9] Liao, Gordon (2023), "Payment versus trading stablecoins," CEPR, 25 March 2023.
[10] Ibid. Liao 2022.

complexity as banks take potentially differing interpretations of assessing stabilization mechanisms.

SCO60.12(4)(f): External Audit Requirement

We note that the requirement in SCO60.12(4)(f) that reserve assets be subject to an independent external audit at least annually is duplicative and redundant to the requirements set out in the rest of SCO60.12(4). Section (e) requires semi-annual verification of disclosed reserve information by a third-party auditor to confirm completeness, fairness of valuation, and accuracy particularly while section (d) requires a risk management framework for the bank's own independent assessment of the reserve assets. Together, these requirements create the structures for accountability of the cryptoasset issuer as well as for the bank's own look-through risk assessment and management. As a result, we recommend that SCO601.2(4)(f) not be included.