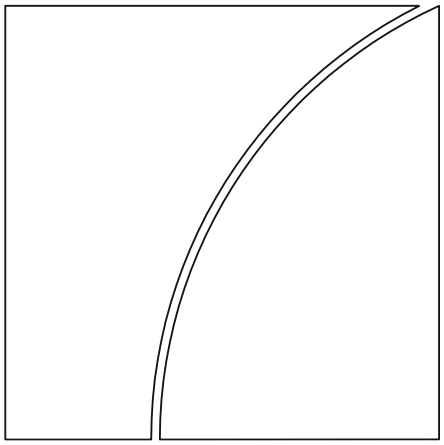
Basel Committee
on Banking Supervision



Cryptoasset standard amendments

July 2024

BIS

This publication is available on the BIS website (www.bis.org).

ISBN 978-92-9259-776-4 (online)

Introduction

In December 2023, the Basel Committee on Banking Supervision published a consultative document proposing certain amendments to the prudential treatment of banks' exposures to cryptoassets.[1] After considering the feedback from stakeholders on the consultation, the Committee has now finalised SCO60 Cryptoasset exposures. This document sets out the final revised standard which the Committee has agreed to implement by 1 January 2026. The Committee wishes to thank respondents for their feedback on the consultative document.

Based on the feedback received, the Committee has amended certain requirements relative to the proposals set out in the consultative document. At a high-level, these changes include:

- **Bankruptcy remoteness of cash.** The consultative text required reserve assets to be placed in structures that are bankruptcy remote from any party that issues, manages or is involved in the stablecoin operation, or that custodies the reserve assets. The final standard includes a limited exception to this requirement where a bank is *only* providing custody services to a stablecoin. In this instance, and consistent with current bank custody practices, the cash does not need to be held bankruptcy remote from the bank's other deposits.
- **Inclusion of securities financing transactions (SFTs) in Group 1b stablecoin reserve assets.** The consultative document noted that the Committee was actively considering whether, and under which conditions, stablecoin reserves that include SFTs could be included in the Group 1b category. The final standard permits cash receivable under reverse repurchase agreements to be included in Group 1b stablecoin reserves, subject to certain minimum conditions.
- **Various other amendments.** Other amendments have also been incorporated into the final standard, including to clarify external audit requirements for stablecoins reserve assets; the clearing requirements for exchange-traded funds (ETFs)/exchange-traded notes (ETNs); the frequency of due diligence requirements (which will be determined by national supervisors); and the haircuts that should be applied to ineligible collateral that are lent or posted under SFTs.

As outlined in the accompanying standard, *Disclosure of cryptoasset exposures*,[2] paragraphs 60.128 to 60.130 will also be removed from SCO60 and replaced by the requirements now set out in DIS55 Cryptoasset exposures.

The final revised sections of the standard are included in the annex below. The revised text will also be incorporated into the consolidated Basel Framework (SCO60 Cryptoasset exposures).

[1] Available at www.bis.org/bcbs/publ/d567.htm.

[2] Available at www.bis.org/bcbs/publ/d580.htm.

Annex: Revisions to the Basel Framework

Set out below are the final revisions to the cryptoasset chapter (SC060) of the Basel Framework.

SCO60.11

Cryptoassets that have a stabilisation mechanism will ~~only~~ meet classification condition 1 only if they satisfy all of the following requirements:

(1) […]

(2) […]

(3) The stabilisation mechanism enables risk management similar to the risk management of traditional assets, based on sufficient data or experience. For newly established cryptoassets, there may be insufficient data and/or practical experience to perform a detailed assessment of the stabilisation mechanism. Banks must document and make available to supervisors on request the assessment they conducted and the evidence used to determine~~Evidence must be provided to satisfy supervisors of~~ the effectiveness of the stabilisation mechanism, including the composition, valuation and frequency of valuation of the reserve asset(s) and the quality of available data.

(4) […]

(5) The cryptoasset passes the redemption risk test set out in [SCO60.12] and the issuer is supervised and regulated by a supervisor that applies prudential capital and liquidity requirements to the issuer. ~~The Committee considered also requiring cryptoassets with stabilisation mechanisms to meet a "basis risk test", but as yet has chosen not to implement this test.[3] The Committee will further study whether there are statistical tests that can reliably identify low-risk stablecoins, and if such a test is identified, will consider it as an additional requirement.~~

Footnotes

~~*[3] For a description of the basis risk test, see the second consultative document on bank exposures to cryptoasset: https://www.bis.org/bcbs/publ/d533.htm*~~

SCO60.12

Redemption risk test. The objective of this test is to ensure that the reserve assets are sufficient to enable the cryptoassets to be redeemable at all times for the peg value, including during periods of extreme stress. To pass the redemption risk test, the bank must ensure that the cryptoasset arrangement meets the following conditions:

(1) […]

(2) *Asset quality criteria for reserve assets* for cryptoassets pegged to currencies. For cryptoassets that are pegged to one or more currencies, the following requirements must be met:

(a) The reserve assets must ~~be~~ comprise~~d of~~ assets with minimal market and credit risk where:

(i) the reserve assets should consist mainly of assets with short-term maturities [5] and high credit quality[6]; and

(ii) the reserve assets have a proven record of relative stability of market terms (eg low volatility of traded prices and spreads) even during stressed market conditions.

(b) The reserve assets ~~shall~~ must be capable of being liquidated rapidly with minimal adverse price effect where:

(i) each reserve asset has a proven record as a reliable source of liquidity in the markets even during stressed market conditions, and those that are marketable securities are traded in large, deep and active markets;

(ii) if the price of a reserve asset is determined by a pricing formula, the formula must be easy to calculate and not depend on strong assumptions, and the inputs into the pricing formula must be publicly available;

(iii) the reserve assets provide sufficient daily liquidity to meet "instant" redemption requests from the cryptoasset holders; and

(iv) the reserve assets are placed in structures that are bankruptcy remote from any party that issues, manages or is involved in the stablecoin operation or custodies the reserve assets.[7]

(c) Eligible types of reserve assets include, but are not limited to:

(i) central bank reserves, to the extent that the stablecoin issuer is eligible to hold these reserves and the central bank's policies allow these reserves to be drawn down in times of stress;

(ii) marketable securities representing claims on or guaranteed by sovereigns and central banks with high credit quality[8] and cash receivable from very short-term reverse repurchase agreements on the basis that they are overcollateralised by these marketable securities[9]; and

(iii) deposits at banks with high credit quality and safeguards, such as a concentration limit applied at group level that includes entities with close links; bankruptcy remoteness of the deposits from any party that issues, manages or is involved in the stablecoin operation; and application of the Basel Framework (including the liquidity coverage ratio).

National supervisors may include other types of assets which fulfil the asset quality criteria for reserve assets as outlined above.

(d) The reserve assets must be denominated in the same currency or currencies in the same ratios as the currencies used for the peg value. A de minimis portion of the reserve assets may be held in a currency other than the currencies used for the peg value, provided that the holding of such currency is necessary for the operation of the cryptoasset arrangement and all currency mismatch risk between the reserve assets and peg value has been appropriately hedged.[10]

(3) *Asset quality criteria for reserve assets for cryptoassets not pegged to currencies.* For cryptoassets that are not pegged to currencies, the reserve assets must largely include asset(s) presenting the same risk profile of the reference assets. That means, the reserve assets should include only the reference assets, except for a de minimis portion of the reserve assets that may be held in cash or bank deposit, provided that the holding is necessary for the operation of the cryptoasset arrangement.

(4) *Management of reserve assets*. The governance arrangements relating to the management of reserve assets must be comprehensive and transparent. They must ensure that:

(a) The reserve assets are managed and invested with an explicit legally enforceable objective of ensuring that all cryptoassets can be redeemed promptly at the peg value, including under periods of extreme stress.

(b) A robust operational risk and resilience framework exists to ensure the availability and safe custody of the reserve assets.

(c) A mandate that describes the types of assets that may be included in the reserve must be publicly disclosed and kept up to date.

(d) An appropriate risk management framework exists to assess and monitor the risks of reserve assets, including but not limited to market risk, credit risk, concentration risk and liquidity risk. Examples include ongoing monitoring of deposit counterparties and custodians, daily valuation of reserve assets and stress testing.

(e) The composition and value of the reserve assets are publicly disclosed on a regular basis. The value and outstanding amount of cryptoassets in circulation must be disclosed at least ~~daily~~once every trade day and the composition must be disclosed at least weekly. This disclosed information must be verified by an independent third party at least semi-annually to confirm its completeness, fairness of valuation and accuracy.

(f) The composition and value of the reserve assets and the outstanding amount of cryptoassets in circulation are subject to an independent external audit at least annually to confirm they match the disclosed reserves and are consistent with the mandate.

Footnotes

[4] For example, consider a cryptoasset that is redeemable for a given currency amount (ie the currency amount is the reference asset) but is backed by bonds denominated in the same currency (ie the bonds are the reserve asset). The reserve assets will give rise to credit, market and liquidity risks that may result in losses relative to the value of the reference asset.

[5] Supervisors may specify: (i) a maximum maturity limit for individual reserve assets and/or (ii) a portfolio weighted average maturity limit for a pool of reserve assets. In case supervisors allow longer-term assets as reserve assets, the level of overcollateralisation should be sufficient to cover potential declines in those asset values so that the cryptoassets remain redeemable at all times for the peg value, including during stressed periods and periods of volatile markets.

[6] These include: (i) marketable securities representing claims on or guaranteed by sovereigns or central banks with a low risk of default (eg subject to a 0% risk weight under the standardised approach to credit risk or equivalent, or subject to a non-0% risk weight to the extent that the cryptoasset is pegged to the domestic currency of the sovereign or central bank); and (ii) deposits at highly rated banks with a low risk of default.

[7] In the case of cash deposits in a bank that only provides custody services to the stablecoin, such cash deposits are not required to be bankruptcy remote from that bank, subject to it being a prudentially regulated bank that meets the conditions set out in [SCO60.12(2)(c)(iii)].

[8] For example, securities referred to under [LCR30.41(3)] can be considered, as well as securities representing claims on or guaranteed by a sovereign or central bank with a non-0% risk weight under the standardised approach to credit risk, to the extent that the cryptoasset is pegged to the domestic currency of that sovereign or central bank.

[9] The following are excluded from the calculation of eligible reserve assets: (i) cash received from repurchase agreements and similar securities financing transactions (SFTs), which expand the balance sheet and, thus, increase leverage at the stablecoin issuer; and (ii) securities received from collateral swaps, which can allow lower quality or less liquid securities to be temporarily swapped for higher quality or more liquid securities. At national discretion, the cash or securities received from repurchase agreements and similar SFTs as well as collateral swaps may still be permitted provided that sufficient regulatory safeguards, such as unwind mechanisms in the short-term horizon, are in place to avoid these outcomes, and the securities lent or posted in these transactions are not included in the eligible reserve assets calculation to avoid double counting.

[10] In case of hedging, the collateral used in credit support annex agreements should be encumbered and subtracted from what is considered the reserve asset funds.

SCO60.14

Classification condition 2: All rights, obligations and interests arising from the cryptoasset arrangement are clearly defined and legally enforceable in all the jurisdictions where the asset is issued and redeemed. In addition, the applicable legal framework(s) ensure(s) settlement finality in both primary and secondary markets. Banks are required to conduct a legal review of the cryptoasset arrangement to ensure this condition is met and make the review available to their supervisors upon request.

SCO60.15(2)

At all times the cryptoasset arrangements are properly documented. For cryptoassets with stabilisation mechanisms, cryptoasset arrangements must clearly define which parties have the right to redeem; the obligation of the redeemer to fulfil the arrangement; the time frame for this redemption to take place; the traditional assets in the exchange; and how the redemption value is determined. These arrangements must also be valid in instances where parties involved in these arrangements may not be located in the same jurisdiction where the cryptoasset is issued and redeemed. At all times, settlement finality in cryptoasset arrangements must be properly documented such that it is clear when the cryptoasset has become irrevocably and unconditionally transferred, so that key financial risks are moved~~transferred~~ from one party to another~~, including the point at which transactions are irrevocable~~. The documentation described in this paragraph must be publicly disclosed by the cryptoasset issuer. If the offering of the cryptoasset to the public has been approved by the relevant regulator on the basis of this public disclosure, the condition in [SCO60.15(2)] will be considered fulfilled. Otherwise, an independent legal opinion would be needed to confirm [SCO60.15(2)] has been met.

SCO60.18

All entities~~Entities~~ that execute redemptions, transfers, storage or settlement ~~finality~~of the cryptoasset, or manage or invest reserve assets, must: (i) be regulated and supervised, or subject to appropriate risk management standards; and (ii) have in place and disclose a comprehensive governance framework.

SCO60.20

Banks, on an ongoing basis, are responsible for assessing whether the cryptoassets to which they are exposed are compliant with the classification conditions set out in [SCO60.6] to [SCO60.19] and the hedging recognition criteria set out in [SCO60.55]. These assessments will determine whether the cryptoassets are classified as Group 1a, Group 1b, Group 2a or Group 2b. To this end, banks must have in place the appropriate risk management policies, procedures, governance, human and IT capacities to evaluate the risks of engaging in cryptoassets and implement these accordingly on an ongoing basis and in accordance with internationally accepted standards. Banks must fully document the information used in determining compliance with the classification conditions and make this available to supervisory authorities on request. In addition:

(1) [...]

(2) [...]

(3) For cryptoassets that are classified as Group 1b, a bank must perform due diligence to ensure that they have an adequate understanding, at acquisition and thereafter on a regular basis, of the stabilisation mechanism of the cryptoasset and of its effectiveness. As part of that due diligence, a bank must conduct statistical or other tests demonstrating that the cryptoasset maintains a stable relationship in comparison to its reference asset (basis risk test). Banks must make available to their supervisors, upon request, the methodology used and the results of such tests, and the supervisors may override the classification based on the test results or the inadequacy of the bank's methodology.

SCO60.55(1)

The bank's cryptoasset exposure is one of the following:

(a) A direct holding of a spot Group 2 cryptoasset where there exists a derivative or exchange-traded fund (ETF)/exchange-traded note (ETN) that ~~is traded on a regulated exchange that~~ solely references the cryptoasset and that is traded on a regulated exchange and, in the case of a derivative, is cleared through a qualifying central counterparty (QCCP).

(b) A derivative or ETF/ETN that references a Group 2 cryptoasset, where the derivative or ETF/ETN has been explicitly approved by a jurisdiction's markets regulators for trading or the derivative is cleared by a ~~qualifying central counterparty (~~QCCP~~)~~.

(c) A derivative or ETF/ETN that references a derivative or ETF/ETN that meets criterion (b) above.

(d) A derivative or ETF/ETN that references a cryptoasset-related reference rate published by a regulated exchange that clears trades using this reference rate through a QCCP.

SCO60.94

For SFTs, banks must apply the comprehensive approach formula set out in the credit risk mitigation section of the standardised approach to credit risk (ie CRE22.45 to CRE22.65). As noted in SCO60.30, only Group 1a cryptoassets that are tokenised versions of the instruments included on the list of eligible financial collateral set out in CRE22 may qualify for recognition as eligible collateral. Group 1b, Group 2a and Group 2b cryptoassets are not eligible forms of collateral in the comprehensive approach and therefore when banks receive them as collateral they will receive no recognition for the purposes of the net exposure calculation to the counterparty. As with all non-eligible collateral, banks that lend Group 1b, Group 2a or Group 2b cryptoassets as part of an SFT must apply~~the same~~ a haircut of 30%, consistent with CRE22.54~~that is used for equities that are not traded on a recognised exchange (ie a haircut of 25%)~~.

SCO60.99

For the purpose of calculating counterparty credit risk for derivative exposures that have Group 2b cryptoassets as the underlying or that are priced in units of a Group 2b cryptoasset, the exposure will be the Replacement Cost (RC)[17~~4~~] plus the Potential Future Exposure (PFE), both multiplied by the alpha factor specified in CRE52.1, where the PFE is to be calculated as 50% of the gross notional amount. The RC must be calculated using the requirements specified in the SA-CCR framework (ie the rules set out in the credit risk standard [CRE52]), with the exception that~~When calculating the RC,~~ netting is permitted within eligible and enforceable netting sets only between exposures to the same Group 2b cryptoassets. Netting sets containing both derivatives related to Group 2b cryptoassets and other asset transactions, must be split into two: one containing the derivatives related to cryptoassets; and one containing derivatives related to the other asset transactions. When calculating the PFE for Group 2b cryptoassets, the 50% of the gross notional amount must be applied per transaction – Group 2b cryptoassets must not form part of any hedging set.

Footnotes

[17~~4~~] The replacement cost is subject to a floor of zero.

SCO60.118

Breaches of the Group 2 exposure limit threshold of 1% should not generally occur and banks must have arrangements in place to ensure compliance with the limit. Any breach that does occur must be communicated immediately to the supervisor and must be rapidly rectified. Until compliance with the 1% limit is restored, the bank's exposures that are in excess of the threshold will be subject to the capital requirements that apply to Group 2b cryptoasset exposures (as set out in [SCO60.83] to [SCO60.85]). If a bank's exposures exceed 2% of its Tier 1 capital, all Group 2 cryptoasset exposures will be subject to the

capital requirements that apply to Group 2b cryptoasset exposures. Regarding a breach of the 1% limit, banks must calculate the RWA arising from its Group 2 cryptoassets using the following formula[20], where:

(1) *A* refers to the RWA for the bank's exposure to Group 2 cryptoassets ignoring the impact of the breach of the 1% Group 2 exposure limit.

(2) *B* refers to the RWA for the bank's exposures to Group 2 cryptoassets assuming all exposures (ie both Group 2a and Group 2b) are subject to the requirements that apply for Group 2b exposures, as set out in [SCO60.83] to [SCO60.86].

(3) *Group 2 exposure* refers to the exposure amount that is calculated in accordance with [SCO60.119].

$$RWA = A + (B - A) \times \frac{Group\,2\,exposure - 1\%\,of\,Tier\,1\,capital}{2\%\,of\,Tier\,1\,capital - 1\%\,of\,Tier\,1\,capital}$$

Footnotes

[20] As an illustrative example of the formula set out in [SCO60.118], consider a bank that has:

- *Group 2 exposures of $100, consisting of:*
  - *Group 2a exposures of $20 with RWA of $200 (ie average RW of 1000%)*
  - *Group 2b exposures of $80 with RWA of $1,000 (ie average RW of 1250%)*
- *Total Group 2 RWA ignoring application of the 1% limit is $1,200*
- *All exposures above measured using the [SCO60.119] (ie the Group 2b approach, except derivatives that use the delta equivalent methodology)*
- *Tier 1 capital of $8,500 (ie the 1% Group 2 limit = $85)*

Applying the formula set out in [SCO60.118] to this bank:

- *A = $1,200 (ie total RWA ignoring the application of the cap)*
- *B = $1,250 = ($20 * 1250%) + $1,000 (ie total RWA if all of Group 2a were treated as Group 2b)*
- *Total Group 2 RWA after the cap is $1,209, calculated as: 1200 + (1250 – 1200)*[(100–85)/(170 – 85)]*

~~SCO60.128~~

~~The disclosure requirements for banks' exposures to cryptoassets or related activities must follow the five general guiding principles for banks' disclosures set out in [DIS10]. As such, in addition to the quantitative information described above, banks must provide qualitative information that sets out an overview of the bank's activities related to cryptoassets and main risks related to their cryptoasset exposures, including descriptions of:~~

~~(1) business activities related to cryptoassets, and how these business activities translate into components of the risk profile of the bank;~~

~~(2) risk management policies of the bank related to cryptoasset exposures;~~

~~(3) scope and main content of the bank's reporting related to cryptoassets; and~~

~~(4) most significant current and emerging risks relating to cryptoassets and how those risks are managed.~~

~~SCO60.129~~

In accordance with the general guiding principles, banks must disclose information regarding any material Group 1a, Group 1b, Group 2a and Group 2b cryptoasset exposures on a regular basis, including for each specific type of cryptoasset exposure information on:

(1) the direct and indirect exposure amounts (including the gross long and short components of net exposures);

(2) the capital requirements; and

(3) the accounting classification.

SCO60.130

In addition to the separate disclosure requirements set out above that apply to all Group 1a, Group 1b, Group 2a and Group 2b cryptoassets, banks must include exposures to Group 1 cryptoassets in the relevant existing disclosure templates that apply to traditional assets (eg for credit risk and market risk).