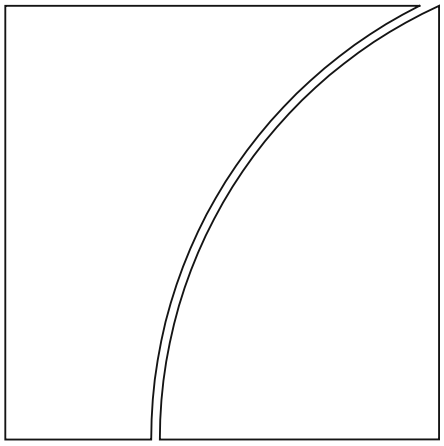
Basel Committee
on Banking Supervision



Prudential treatment of cryptoasset exposures

December 2022

BIS

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

ISBN 978-92-9259-614-9 (online)

Contents

Prudential treatment of cryptoasset exposures

1. Introduction

In June 2022 the Basel Committee on Banking Supervision issued its second consultation on the prudential treatment of banks' exposures to cryptoassets.[1] After considering the feedback from stakeholders to the consultation, the Committee has now finalised its prudential standard, which has been endorsed by the Committee's oversight body, the Group of Governors and Heads of Supervision. This document sets out the final standard which the Committee has agreed to implement by 1 January 2025. The text will be incorporated into the consolidated Basel Framework shortly. The Committee wishes to thank respondents for their feedback to the second consultation.

Set out below is a short summary of the structure of the finalised standard (Section 2), a description of the key elements that were changed relative to the proposal in the second consultation (Section 3), a description of key elements of the proposal that the Committee intends to closely monitor in the near term (Section 4), and the text of the standard itself, in the form of a new chapter of the consolidated Basel Framework (Section 5).

2. Structure of the standard

The structure of the standard is unchanged from the proposal set out in the second consultation. Under the standard banks are required to classify cryptoassets on an ongoing basis into two groups:

- **Group 1 cryptoassets.** Those that meet in full a set of classification conditions. Group 1 cryptoassets include tokenised traditional assets (Group 1a) and cryptoassets with effective stabilisation mechanisms (Group 1b). Group 1 cryptoassets are subject to capital requirements based on the risk weights of underlying exposures as set out in the existing Basel Framework.[2]
- **Group 2 cryptoassets.** Those that fail to meet any of the classification conditions. As a result, they pose additional and higher risks compared with Group 1 cryptoassets and consequently are subject to a newly prescribed conservative capital treatment. In addition to any tokenised traditional assets and stablecoins that fail the classification conditions, Group 2 includes all unbacked cryptoassets. A set of hedging recognition criteria is used to identify those Group 2 cryptoassets where a limited degree of hedging is permitted to be recognised (Group 2a) and those where hedging is not recognised (Group 2b).

Additional key elements of the standard include:

- **Infrastructure risk add-on**: An add-on to risk-weighted assets (RWA) to cover infrastructure risk for all Group 1 cryptoassets that authorities can activate based on any observed weaknesses in the infrastructure on which cryptoassets are based.
- **Redemption risk test and a supervision/regulation requirement**: This test and requirement must be met for stablecoins to be eligible for inclusion in Group 1. They seek to ensure that only stablecoins issued by supervised and regulated entities that have robust redemption rights and governance are eligible for inclusion.
- **Group 2 exposure limit**: A bank's total exposure to Group 2 cryptoassets must not exceed 2% of the bank's Tier 1 capital and should generally be lower than 1%. Banks breaching the 1% limit

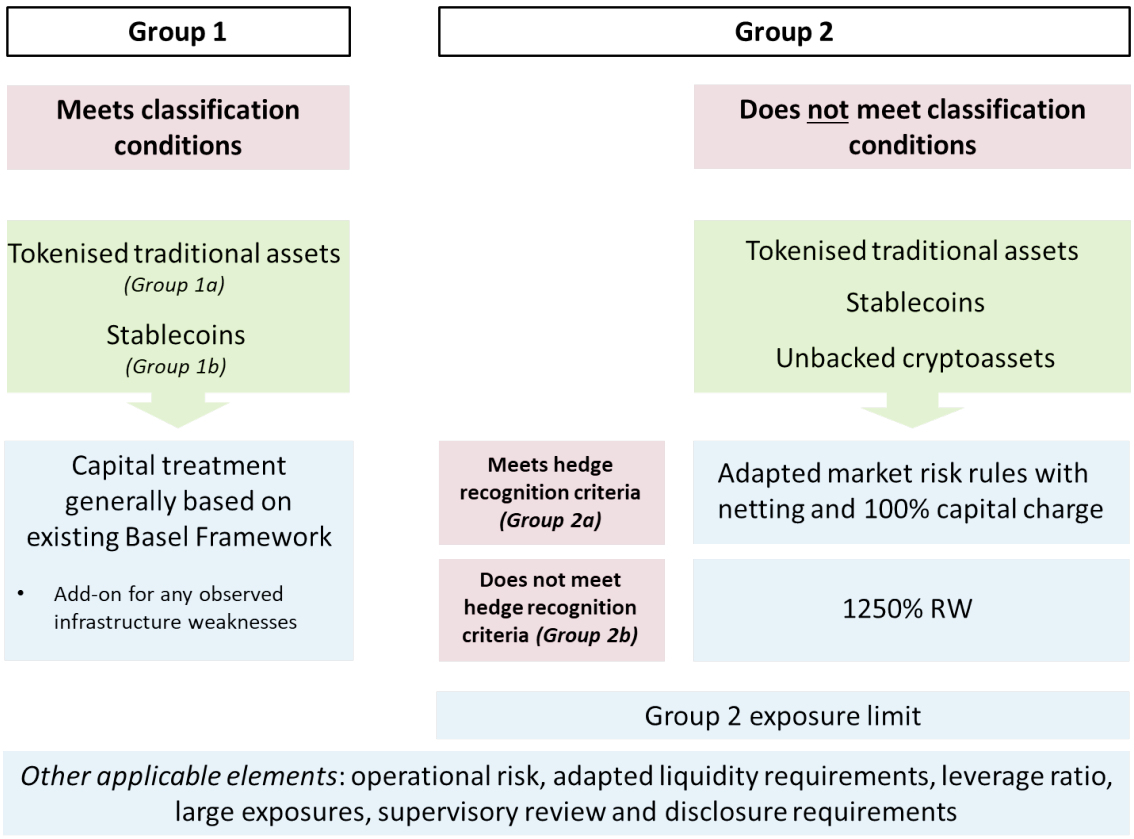
[1] Available at https://www.bis.org/bcbs/publ/d533.htm

[2] Algorithm-based stablecoins or those stablecoins that use protocols to maintain their value are not eligible for Group 1.

will apply the more conservative Group 2b capital treatment to the amount by which the limit is exceeded. Breaching the 2% limit will result in the whole of Group 2 exposures being subject to the Group 2b capital treatment.

- **Other elements:** Other elements of the standard include descriptions of how the operational risk, liquidity, leverage ratio and large exposures requirements should be applied to banks' cryptoasset exposures. The supervisory review process and a specific set of disclosure requirements are also prescribed.

The following diagram illustrates the structure described above:



3. Changes relative to the proposal in the second consultation

Reflecting on stakeholders' feedback on the proposed standard and market developments in cryptoassets, the Committee agreed to make the changes described in this section in the final standard relative to the proposal that was set out in the second consultation.

Infrastructure risk add-on

In the second consultation the add-on for infrastructure risk was proposed as a fixed add-on to RWA set at 2.5% of the exposure value for all Group 1 cryptoassets. The Committee agreed to replace this with a more flexible approach that allows authorities to initiate and increase an add-on based on any observed weaknesses in the infrastructure that underlies specific cryptoassets. Such an approach should incentivise banks to actively address infrastructure risks to avoid the imposition of an add-on at a future point.

Basis risk test, redemption risk test and the supervision/regulation requirement

The Group 1 classification conditions set out in the second consultation included a requirement that cryptoassets with stabilisation mechanisms must pass a redemption risk test and a basis risk test. The objective of the redemption risk test is to ensure that the reserve assets are sufficient to enable the cryptoassets to be redeemable at all times, including during periods of extreme stress, for the amount to which the cryptoasset is pegged (the "peg value"). The basis risk test, which is a quantitative test based on the market value of the cryptoasset, aims to ensure that the holder of a cryptoasset can sell it in the market for an amount that closely tracks the peg value. The Committee noted in the second consultation that it was considering as an alternative to the basis risk and redemption risk tests a requirement for stablecoins to be supervised and regulated by a supervisory authority that applies prudential capital and liquidity requirements.

After reflecting on the merits of these different approaches, the Committee decided not to implement the basis risk test at this time. As noted in Section 4 below, 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 for inclusion in Group 1b. Furthermore, the Committee agreed that the supervision/regulation requirement should apply *in addition to* the requirement to pass the redemption risk test. For cryptoassets that are pegged to one or more currencies, the redemption risk test now also includes a requirement that the reserve assets must be comprised of assets with minimal market risk and credit risk. The Committee will further study the appropriate composition of reserve assets for the purpose of the redemption risk test.

Group 2 exposure limit

The proposed requirement for banks to keep their aggregate exposures to Group 2 cryptoassets below a threshold of 1% of their Tier 1 capital has been retained in the final standard, subject to certain modifications. The first modification will result in exposures being measured as the higher of the gross long and gross short position in each cryptoasset, rather than the aggregate of the absolute values of long and short exposures, as proposed in the second consultation. This change will ensure that banks that take steps to hedge exposures are not penalised under the limit. The second modification relates to the capital consequences of a breach of the limit. To reduce cliff effects, the Committee has agreed that the consequence of breaching the limit will be for the Group 2b capital treatment to apply to only the amount by which the limit is exceeded, rather than to all Group 2 exposures. However, to ensure that banks have a strong incentive to not significantly exceed the 1% threshold, a new 2% limit will be introduced which, if breached, will result in the whole of Group 2 exposures being subject to the Group 2b capital treatment.

Responsibility for assessing the classification conditions

Under the second consultation proposal, banks were required to assess their cryptoassets against the classification conditions and seek prior supervisory approval to finalise the classification. The Committee agrees with feedback to the consultation that this process could be unnecessarily burdensome, particularly in cases where the compliance or breach of the conditions is clear. As a result, the required process has been modified to remove the supervisory pre-approval element; instead, in the final standard banks are required to notify supervisors of classification decisions and supervisors will have the power to override these decisions if they disagree with a bank's assessment.

Custodial assets

Respondents to the second consultation raised concerns about the application of the standard in relation to customer assets where a bank is acting as a custodian. Respondents were concerned that the standard may imply the application of credit, market and liquidity risk requirements to those customer assets. This

was not the intention of the standard. The standard has therefore been revised to clarify which elements are applicable to custodial services provided by banks.

4. Elements subject to specific monitoring and review

The Committee plans to closely monitor the implementation and effects of the cryptoasset standard. Given the rapid pace of market developments, the Committee will likely issue additional refinements and clarifications over time. These may be needed to ensure a consistent understanding and implementation of the standard, or to address emerging risks. As part of its surveillance efforts, the Committee will continue to collect data from banks as part of its regular Basel III monitoring exercise, monitor and exchange information on the implementation of the standard and market developments, and actively engage with other standard setting bodies.

In addition to the overall monitoring of the standard, the Committee has agreed on a set of issues that will be subject to specific monitoring and review. The issues are as follows:

- **Statistical tests and redemption risk test**: 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 for inclusion in Group 1b. The Committee will also further study the appropriate composition of reserve assets for the purpose of the redemption risk test.
- **Permissionless blockchains**: The Committee will continue to reflect on whether the risks posed by cryptoassets that use permissionless blockchains can be sufficiently mitigated to allow for their inclusion in Group 1 and, if so, what adjustments to the classification conditions would be needed.
- **Group 1b cryptoassets received as collateral**: Under the final standard, Group 1b cryptoassets that a bank receives as collateral are not permitted to be recognised as eligible collateral for the purposes of calculating regulatory capital requirements. The Committee intends to continue to monitor this treatment and assess whether any Group 1b cryptoassets have the required characteristics to receive recognition as collateral for capital requirements purposes.
- **Group 2a criteria and degree of hedge recognition**: The "hedging recognition criteria" in the final standard are in line with the proposals set out in the second consultation proposal. Cryptoassets that meet these criteria will be allocated to Group 2a and will be eligible to receive a limited amount of recognition. The criteria include various thresholds, relating to the market capitalisation, trading volume and price observations for cryptoassets to meet to be included in Group 2a. The Committee intends to monitor closely the specification of these thresholds and the degree of hedge recognition that the Group 2a classification permits.
- **Calibration of the Group 2 exposure limit**: The Group 2 exposure limit is based on thresholds set at 1% and 2% of banks' Tier 1 capital. These thresholds aim to safeguard the banking sector against the potentially significant risks posed by Group 2 cryptoassets. As the cryptoasset market develops, the Committee will reassess the appropriateness of these thresholds.

5. Text of the standard on banks' exposures to cryptoassets

Below is the text of a new chapter of the Basel Framework (SCO60) that sets out the prudential treatment of banks' exposures to cryptoassets. The implementation date is 1 January 2025 and all cross references to other chapters of the framework relate to the chapters that will be in effect at that date. The consolidated version of the Basel Framework will shortly be updated to include the new chapter set out below.

SCO60: Cryptoasset exposures

Introduction

60.1 This chapter sets out how the Basel Framework is to be applied in respect of banks' exposures to cryptoassets. Cryptoassets are defined as private digital assets that depend on cryptography and distributed ledger technologies (DLT) or similar technologies. Digital assets are a digital representation of value, which can be used for payment or investment purposes or to access a good or service.

60.2 Dematerialised securities (securities that have been moved from physical certificates to electronic book-keeping) that are issued through DLT or similar technologies are considered to be within the scope of this chapter and are referred to as tokenised traditional assets, whereas those dematerialised securities that use electronic versions of traditional registers and databases which are centrally administered are not within scope.

60.3 The prudential treatment of central bank digital currencies (CBDCs) is not described within the Basel Framework. The Committee will give further consideration to the treatment of CBDCs as they are issued.

60.4 For the purposes of this chapter, the term "exposure" includes on- or off-balance sheet amounts that give rise to credit, market, operational and/or liquidity risks. Certain parts of the chapter, such as the operational risk requirements and the risk management and supervisory review sections, are also applicable to banks' cryptoasset activities, such as custodial services involving the safekeeping or administration of client cryptoassets on a segregated basis, that do not generally give rise to credit, market or liquidity requirements.

60.5 The remainder of this chapter is organised according to the following sections:

(1) Classification conditions: [SCO60.6] to [SCO60.22].

(2) Banking/trading book boundary, use of internal models and accounting classification: [SCO60.23] to [SCO60.25].

(3) Minimum capital requirements for credit risk for Group 1 cryptoassets: [SCO60.26] to [SCO60.39].

(4) Minimum capital requirements for market risk for Group 1 cryptoassets: [SCO60.40] to [SCO60.51].

(5) Add-on for infrastructure risk for Group 1 cryptoassets: [SCO60.52] to [SCO60.53].

(6) Minimum capital requirements for Group 2 cryptoassets: [SCO60.54] to [SCO60.86].

(7) Minimum capital requirements for credit valuation adjustment (CVA) risk: [SCO60.87] to [SCO60.92].

(8) Minimum capital requirements for counterparty credit risk: [SCO60.93] to [SCO60.99].

(9) Minimum capital requirements for operational risk: [SCO60.100].

(10) Minimum liquidity risk requirements: [SCO60.101] to [SCO60.112].

(11) Leverage ratio requirements: [SCO60.113] to [SCO60.114].

(12) Large exposure requirements: [SCO60.115].

(13) Group 2 exposure limit: [SCO60.116] to [SCO60.119].

(14) Bank risk management and supervisory review: [SCO60.120] to [SCO60.127].

(15) Disclosure requirements: [SCO60.128] to [SCO60.130].

(16) Definitions: [SCO60.131].

Classification conditions

60.6 In certain areas of this chapter, most notably for the purposes of credit, market and liquidity risk, the prudential treatment of a bank's cryptoasset exposures varies according to the prudential classification of the cryptoassets. To determine the prudential classification, cryptoassets must be screened on an ongoing basis and classified into two broad groups:

(1) *Group 1 cryptoassets* are those cryptoassets that meet the classification conditions set out in [SCO60.8] to [SCO60.19]. Group 1 cryptoassets consist of:

(a) Group 1a: Tokenised traditional assets[1] that meet the classification conditions.

(b) Group 1b: Cryptoassets with effective stabilisation mechanisms that meet the classification conditions.

(2) *Group 2 cryptoassets* are those cryptoassets that fail to meet the classification conditions set out in [SCO60.8] to [SCO60.19]. Group 2 cryptoassets consist of:

(a) Group 2a: Cryptoassets (including tokenised traditional assets, stablecoins and unbacked cryptoassets) that fail to meet the classification conditions, but pass the Group 2a hedging recognition criteria.

(b) Group 2b: All other cryptoassets (ie tokenised traditional assets, stablecoins and unbacked cryptoasset that fail to meet the classification conditions and fail the Group 2a hedging recognition criteria).

Footnotes

[1] Traditional assets are those assets that are captured within the Basel Framework that are not classified under this chapter as cryptoassets.

60.7 To be classified as Group 1a or Group 1b, cryptoassets must meet on an ongoing basis the classification conditions in [SCO60.8] to [SCO60.19] below.

Classification condition 1

60.8 *Classification condition 1*: The cryptoasset is either: (i) a tokenised traditional asset; or (ii) has a stabilisation mechanism that is effective at all times in linking its value to a traditional asset or a pool of traditional assets (ie reference asset(s)).

60.9 Tokenised traditional assets will only meet classification condition 1 if they satisfy all of the following requirements:

(1) They are digital representations of traditional assets using cryptography, DLT or similar technology to record ownership.

(2) They pose the same level of credit and market risk as the traditional (non-tokenised) form of the asset. In practice, this means the following for tokenised traditional assets:

(a) *Bonds, loans, claims on banks (including in the form of deposits),[2] equities and derivatives*. The cryptoasset must confer the same level of legal rights as ownership of these traditional forms of financing (eg rights to cash flows, claims in insolvency etc). In addition, there must be no feature of the cryptoasset that could prevent obligations to the bank being paid in full when due as compared with a traditional (non-tokenised) version of the asset.

(b) *Commodities*. The cryptoasset must confer the same level of legal rights as traditional account-based records of ownership of a physical commodity.

(c) *Cash held in custody*. The cryptoassets must confer the same level of legal rights as cash held in custody.

Footnotes

[2] In certain jurisdictions bank-issued tokenised payment assets that are backed by the general assets of the bank and not by a pool of reserve assets may be referred to as "stablecoins." Notwithstanding how they may generally be referred to within the jurisdiction, these assets may be included in Group 1a provided they meet all the requisite conditions and would not be assigned to Group 1b based solely on their commonly used local name.

60.10 Cryptoassets do not meet the condition set out in [SCO60.9](2) above if they:

(1) first need to be redeemed or converted into traditional assets before they receive the same legal rights as direct ownership of traditional assets; or

(2) through their specific construction, they involve additional counterparty credit risks relative to traditional assets.

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

(1) The cryptoasset is designed to be redeemable for a predefined amount of a reference asset or assets (eg 1 USD, 1 oz gold) or cash equal to the current market value of the reference asset(s) (eg USD value of 1 oz gold). The value of the reference asset(s) to which one unit of the cryptoasset is designed to be redeemable is referred to as the "peg value".

(2) The stabilisation mechanism is designed to minimise fluctuations in the market value of the cryptoassets relative to the peg value. In order to satisfy the "effective at all times" condition, banks must have a monitoring framework in place verifying that the stabilisation mechanism is functioning as intended.

(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. 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) There exists sufficient information that banks use to verify the ownership rights of the reserve assets upon which the stable value of the cryptoasset is dependent. In the case of underlying physical assets, banks must verify that these assets are stored and managed appropriately. This monitoring framework must function regardless of the cryptoasset issuer. Banks may use the assessments of independent third parties for the purposes of verification of ownership rights only if they are satisfied that the assessments are reliable.

(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

60.12 *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) *Value and composition of reserve assets*. The value of the reserve assets (net all non-cryptoasset claims on these assets) must at all times, including during periods of extreme stress, equal or exceed the aggregate peg value of all outstanding cryptoassets. If the reserve assets expose the holder to risk in addition to the risks arising from the reference assets,[4] the value of the reserve assets must sufficiently overcollateralise the redemption rights of all outstanding cryptoassets. The level of overcollateralisation must be sufficient to ensure that even after stressed losses are incurred on the reserve assets, their value exceeds the aggregate value of the peg of all outstanding cryptoassets.

(2) *Asset quality criteria for reserve assets*. For cryptoassets that are pegged to one or more currencies, the reserve assets must be comprised of assets with minimal market and credit risk. The assets shall be capable of being liquidated rapidly with minimal adverse price effect. For example, these assets may be defined as Level 1 HQLA as stipulated in LCR30.41. Further, 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.

(3) *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) The composition and value of the reserve assets are publicly disclosed on a regular basis. The value must be disclosed at least daily and the composition must be disclosed at least weekly.

(e) The reserve assets 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.

60.13 Stabilisation mechanisms that: (i) reference other cryptoassets as underlying assets (including those that reference other cryptoassets that have traditional assets as underlying); or (ii) use protocols to increase or decrease the supply of the cryptoasset[5] do not meet classification condition 1.

Footnotes

[5] Cryptoassets that use protocols to maintain their value are in some cases referred to as "algorithm-based stablecoins".

Classification condition 2

60.14 *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. 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.

60.15 To meet classification condition 2, the following requirements must be met:

(1) At all times the cryptoasset arrangements must ensure full transferability and settlement finality. In addition, cryptoassets with stabilisation mechanisms must provide a robust legal claim against the issuer and/or underlying reserve assets and must ensure full redeemability (ie the ability to exchange cryptoassets for amounts of pre-defined assets such as cash, bonds, commodities, equities or other traditional assets) at all times and at their peg value. In order for a cryptoasset arrangement to be considered as having full redeemability, it must allow for the redemption to be completed within 5 calendar days of the redemption request at all times.

(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 timeframe 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 key financial risks are 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.

Classification condition 3

60.16 *Classification condition 3*: The functions of the cryptoasset and the network on which it operates, including the distributed ledger or similar technology on which it is based, are designed and operated to sufficiently mitigate and manage any material risks.

60.17 To meet classification condition 3, the following requirements must be met:

(1) The functions of the cryptoasset, such as issuance, validation, redemption and transfer of the cryptoassets, and the network on which it runs, do not pose any material risks that could impair the transferability, settlement finality or, where applicable, redeemability of the cryptoasset. To this end, entities performing activities associated with these functions[6] must follow robust risk governance and risk control policies and practices to address risks including, but not limited to: credit, market and liquidity risks; operational risk (including outsourcing, fraud and cyber risk) and risk of loss of data; various non-financial risks, such as data integrity; operational resilience (ie operational reliability and capacity); third-party risk management; and Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT).

(2) All key elements of the network must be well-defined such that all transactions and participants are traceable. Key elements include: (i) the operational structure (ie whether there is one or multiple entities that perform core function(s) of the network); (ii) degree of access (ie whether the network is restricted or un-restricted); (iii) technical roles of the nodes (including whether there is a differential role and responsibility among nodes); and (iv) the validation and consensus mechanism of the network (ie whether validation of a transaction is conducted with single or multiple entities).

Footnotes

[6] Examples of these entities include but are not limited to: issuers, operators of the transfer and settlement systems for the cryptoasset; administrators of the cryptoasset stabilisation mechanism and custodians of any underlying assets supporting the stabilisation mechanism.

Classification condition 4

60.18 *Classification condition 4*: 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.

60.19 Entities subject to condition 4 include operators of the transfer and settlement systems for the cryptoasset, wallet providers and, for cryptoassets with stabilisation mechanisms, administrators of the stabilisation mechanism and custodians of the reserve assets. Node validators may be subject to appropriate risk management standards as an alternative to being regulated and supervised.

Responsibilities for determining and monitoring compliance with the classification conditions

60.20 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) Regarding cryptoassets to which a bank is already exposed on the implementation date of [SCO60], the bank must inform their supervisor of the classification decisions they have reached for each cryptoasset. This information should ideally be sent well before

the implementation date of [SCO60]. If providing the information is not possible in advance of implementation of [SCO60], it must be sent as soon as practical afterwards. Specifically, it must be sent with sufficient time for the supervisor to review and, if necessary, override the classification decision reached by the bank prior to the publication of the bank's first set of Pillar 3 disclosures after the implementation of [SCO60]. Authorities may wish to specify a suitable deadline for banks in their jurisdiction with cryptoasset exposures that takes into consideration available supervisory resources and bank reporting schedules.

(2) Regarding cryptoassets that a bank may wish to acquire after the implementation date of [SCO60], in advance of any acquisition of cryptoassets the bank must inform their supervisor of their classification assessment of the cryptoassets. This must occur with sufficient time for the supervisor to review and, if necessary, override the classification decision reached prior to the bank's acquisition of the cryptoasset. Authorities may wish to specify a suitable time period for such notifications that takes into consideration available supervisory resources.

60.21 Supervisors are responsible for: (i) reviewing and assessing banks' analysis and risk management and measurement approaches; and (ii) reviewing banks' classification decisions (as outlined in [SCO60.20]). A bank's supervisor may rely on other regulators or supervisors overseeing the entities' management of risks attributable to the functions mentioned above; as well as independent third-party assessors determined to have the required expertise and skills, to evaluate the specific risk characteristics of cryptoasset arrangements. Supervisory authorities must also have the power to override banks' classification decisions, if they do not agree with the assessments undertaken by banks. The override should be exercised in a consistent way across banks. The override may be used at any time by the supervisory authority. In certain cases, authorities may wish to set a future date at which the override comes into effect, to allow banks time to prepare for its impact.

60.22 To ensure consistent application across jurisdictions, authorities will routinely compare and share their supervisory information on banks' assessments of cryptoassets against the classification conditions.

Banking/trading book boundary, use of internal models and accounting classification

60.23 [RBC25] must be used to determine the allocation of cryptoassets between the banking book and trading book, subject to the following specifications and exceptions:

(1) Group 1a cryptoassets must be assigned to the banking book or trading book based on the application of the boundary criteria to the non-tokenised equivalent traditional assets.

(2) Group 1b cryptoassets must be assigned to the banking book or trading book based on the application of the boundary criteria to the reference asset(s).

(3) Group 2a cryptoassets must be treated according to the proposed market risk rules, independent of whether they stem from trading or banking book instruments (ie similar to FX and commodities risk).

(4) Group 2b cryptoassets must be treated according to the standardised conservative prudential treatment outlined in [SCO60.83] to [SCO60.86].

60.24 [CRE] and [MAR] are used to determine whether Group 1 cryptoasset exposures are treated according to standardised or internal model-based approaches to credit and market risk respectively. Models-based approaches must not be applied to Group 2 cryptoassets.

60.25 Cryptoasset exposures are not subject to the deduction requirement that applies to intangible assets set out in [CAP30.7] and [CAP30.8], even in cases where the cryptoasset is classified as an intangible under the applicable accounting standard.

Minimum capital requirements for credit risk for Group 1 cryptoassets

60.26 This section describes how the minimum risk-based capital requirements for credit risk ([CRE]) are to be applied to cryptoasset exposures.

Group 1a cryptoassets (tokenised traditional assets)

60.27 Group 1a cryptoassets (tokenised traditional assets) held in the banking book will generally be subject to the same rules to determine credit risk-weighted assets (RWA) as non-tokenised traditional assets (ie the rules set out in the credit risk standard [CRE]). For example, a tokenised corporate bond held in the banking book will be subject to the same risk weight as the non-tokenised corporate bond held in the banking book.

60.28 The treatment outlined in [SCO60.27] above is based on the assumption that if two exposures confer the same level of legal rights (to cash flows, claims in insolvency, ownership of assets etc) and the same likelihood of paying the owner all amounts due on time (including amounts due in case of default), they will likely have very similar values and pose a similar risk of credit losses. However, there are areas of the credit standards that aim to capture risks that are not directly related to the legal rights of an asset held by a bank or likelihood of timely payment. Banks must separately assess the tokenised traditional asset against these rules, and not assume qualification for a given treatment simply because the traditional (non-tokenised) asset qualifies. For example, a tokenised asset may have different market liquidity characteristics than the traditional (non-tokenised) asset. This could arise because the pool of potential investors that are able to hold tokenised assets might be different to non-tokenised assets.

60.29 The potential for market liquidity characteristics and market values of tokenised assets to differ from non-tokenised assets is important in considering whether Group 1a cryptoassets meet the requirements for the purposes of credit risk mitigation within the credit risk standards. Also, the speed with which a secured creditor could take possession of cryptoasset collateral may be different than for a traditional asset. Therefore, before such assets are recognised as collateral for the purposes of credit risk mitigation, banks must separately assess whether they comply with the relevant eligibility requirements for collateral recognition, such as whether the collateral can be liquidated promptly and legal certainty requirements ([CRE22.9]). In addition to assessing whether tokenised assets held as collateral are eligible to be recognised as credit risk mitigation, banks must analyse the period of time over which they can be liquidated and the depth of market liquidity during a period of downturn. Cryptoassets shall only be recognised as collateral where volatility in values and holding periods under distressed market conditions can be confirmed to not be materially increased compared with the traditional asset or pool of traditional assets. Otherwise the cryptoasset shall not be eligible for recognition of credit risk mitigation unless a bank has received permission from its supervisor for reflecting any material increase in relevant parameters as part of own LGD estimates under the IRB approach.

60.30 [CRE22] sets out the list of eligible forms of financial collateral for the purposes of recognition as a credit risk mitigant under the standardised approach to credit risk. The list is also the basis of eligible financial collateral under the foundation internal ratings-based approach. 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 (subject to also meeting the requirements described above).

Group 1b cryptoassets (cryptoassets with stabilisation mechanisms)

60.31 As a result of the classification conditions, Group 1b cryptoassets must be designed to be redeemable for a predefined amount of a reference asset or assets, or cash equal to the value of the reference asset(s). In addition, the cryptoasset arrangement must include a sufficient pool of reserve assets to ensure the redemption claims of cryptoasset holders can be met. Aside from these common elements, Group 1b cryptoassets may be structured in a variety of different ways. Banks that have banking book exposures to Group 1b cryptoassets must analyse their specific structures and identify all risks that could result in a loss. Each credit risk must be separately capitalised by banks using the credit risk standards set out in [CRE]. Paragraphs [SCO60.32] to [SCO60.39] below describe various ways in which credit risks may arise from banks' exposures to Group 1b cryptoassets and the capital requirements that would apply in each case. The list is not exhaustive, and it is the responsibility of banks to comprehensively assess and document the full range of risks arising from each of its exposures to Group 1b cryptoassets.

60.32 *Risk from reference asset*. If the reference asset for a Group 1b cryptoasset gives rise to credit risk (eg a bond), banks may suffer a loss from the default of the reference asset's issuer. Banks must therefore include in credit RWA the RWA that would apply under [CRE] to a direct holding of the reference asset. If the reference asset gives rise to foreign exchange or commodities risk (eg foreign currency denominated financial assets or physical commodities), banks must calculate market RWA for the exposure equal to the market RWA that would apply under [RBC20.9](1) to a direct holding of the underlying traditional asset.

60.33 For Group 1b cryptoassets that reference a pool of traditional assets, banks must apply the requirements applicable to equity investments in funds (see [CRE60]) to determine the RWA applicable for a direct holding of the referenced pool of traditional assets, as required in [SCO60.32] above. The look-through approach and the mandate-based approach of [CRE60] are available for cryptoassets that fulfil all requirements for these approaches. Otherwise, the fall-back approach (ie a 1250% risk weight) must be applied.

60.34 *Risk of default of the redeemer*. Group 1b cryptoassets must be redeemable and if the entity that performs the redemption function (the "redeemer") fails, the cryptoassets may become worthless. The capital treatment[7] of banks' exposures to the redeemer depends on the nature of the exposures:

(1) If the bank holding the cryptoasset has an unsecured claim on the redeemer in case of default, the bank must calculate credit RWA for its exposure to the redeemer. The credit RWA in this case must be equal to the RWA that would apply under [CRE] to a direct unsecured loan to the redeemer. For this purpose the loan amount should equal the redemption claim (ie peg value) of the cryptoasset.

(2) If the bank holding the cryptoasset has a secured claim on the redeemer in case of default, the bank must calculate credit RWA for its exposure to the redeemer. The credit RWA in this case must be equal to the RWA that would apply under CRE to a direct secured loan to the redeemer. For this purpose the loan amount, before any recognition of credit risk mitigation, should equal the redemption claim (ie peg value) of the cryptoasset. All conditions on the eligibility of collateral for the purposes of recognising credit risk mitigation set out in [CRE] apply.

Footnotes

[7] The capital requirements outlined in this section relate to the calculation of credit RWA. The sections of [SCO60] relating to market risk RWA note that credit RWA must be calculated for instruments in the trading book that give rise to credit risk as a result of potential default of the redeemer.

60.35 Certain Group 1b cryptoassets may be structured to avoid the cryptoasset holders being exposed to the credit risk (either directly or indirectly) of the redeemer. Banks are not required to calculate credit RWA in respect of the risk outlined in [SCO60.34] above if the following conditions are met:

(1) The underlying reserve assets are held in a bankruptcy remote special purpose vehicle (SPV) on behalf of the holders of cryptoassets who have direct claims on the underlying reserve asset(s).

(2) The bank has obtained an independent legal opinion for all laws relevant to involved parties, including the redeemer, the SPV and custodian, affirming that relevant courts would recognise underlying assets held in a bankruptcy remote manner as those of the cryptoasset holder.

60.36 *Risks arising when intermediaries perform the redemption function*. Group 1b cryptoassets may be structured such that only a subset of holders ("members") are allowed to transact directly with the redeemer to redeem the cryptoasset. Holders that cannot transact directly with the redeemer ("non-member holders") are therefore reliant on the members for the cryptoassets to maintain their value relative to the reference asset. This type of structure itself may include variants, for example:

(1) The members may issue a legally binding commitment to buy cryptoassets from non-member holders at a price equal to the reference asset(s).

(2) The members may not make a commitment, but may be incentivised to purchase the cryptoassets from non-member holders because they know they can exchange them with the redeemer for cash/assets (as long as the redeemer does not fail).

60.37 Banks that are members of cryptoasset arrangements as described in [SCO60.36] above ("member banks"), must calculate risk weighted assets for their own cryptoasset holdings in the same way as required for holders in cryptoassets arrangements in which all holders can deal directly with the redeemer (ie as set out in [SCO60.34] to [SCO60.35] above). In addition, member banks may be exposed to the risk that the redeemer fails and they are committed to purchase cryptoassets from non-member holders. In such cases, a member bank must also include the RWA that would apply if the bank held all of the cryptoassets that it could be obliged to purchase (ie as set out in [SCO60.36](1) above). Even if there is no legal obligation for a member bank to purchase cryptoassets from non-member holders, banks and supervisors must consider whether in practice the member bank would be obliged to step-in and purchase them in order to satisfy the expectations of non-member holders and protect the bank's reputation. Where such step-in risk exists, banks must include within RWA the amount that would apply if legally binding commitments have been made. Exceptions would only be made if the bank can demonstrate to the supervisor that such step-in risk does not exist.

60.38 The risks to bank holders of cryptoassets that cannot deal directly with the redeemer (ie non-member holders) depend on whether the members have committed to purchase cryptoassets from all non-member holders in unlimited amounts (ie they have made a standing and irrevocable offer to purchase all outstanding cryptoassets from non-member holders):

(1) If members have committed to buy cryptoassets in unlimited amounts, the non-member holders are exposed to: (i) the risk arising from the changing value or potential default of the reference asset; and (ii) the risk that all members default, leaving non-member holders with no way to redeem their cryptoassets. When banks are non-member holders they must sum the RWA calculated for the two risks. The first risk must be calculated as the RWA that would arise from a direct exposure to the underlying (see [SCO60.32]). The calculation of the RWA for the default of the members is more complex given that there may potentially be multiple members that have made commitments to purchase

the cryptoassets (ie the holder can choose whether to sell the cryptoasset to any one of a number of members). If there is just one member, the RWA must be calculated as the cryptoasset holding multiplied by the risk weight applicable to an unsecured loan to the member. If there are multiple members, the risk weight to be used must be the risk weight that would be applicable to an unsecured loan to the member with the highest credit rating (ie lowest risk weight).[8]

(2) If members have not committed to purchase cryptoassets in unlimited amounts from all non-member holders, the latter are exposed to: (i) the risk arising from the changing value or potential default of the reference asset; (ii) the risk that all the members default, leaving non-member holders with no way to redeem their cryptoassets assets; and (iii) the risk that the redeemer defaults (because if it failed, the members would no longer have the incentive to purchase the cryptoassets from the non-member holders). In such cases, the non-member bank holder must include in RWA the sum of RWA for all three separate exposures. The RWA for the first two risks must be calculated in the same way as described in (1) above. The RWA for the third risk must be calculated as the RWA that would arise from a direct loan to the redeemer.

Footnotes

[8] For example, consider the situation in which there is only one member and it has a high credit rating (and therefore a low risk weight). Its low risk weight should be used to determine the credit risk of non-member holders. Now consider an additional member is added that has a low credit rating (and therefore a high risk weight). The addition of this new member does not increase the risk to non-member holders (in fact it decreases it by giving them more options for redeeming their assets). Thus, the low risk weight of the first member can continue to be used to determine the credit risk to non-member holders.

60.39 Group 1b cryptoassets, including those that can be redeemed for traditional instruments that are included on the list of eligible financial collateral, are not eligible forms of collateral in themselves for the purposes of recognition as credit risk mitigation. This is because, as outlined above, the process of redemption may add counterparty risk that is not present in a direct exposure to a traditional asset.

Minimum capital requirements for market risk for Group 1 cryptoassets

60.40 This section describes how the minimum risk-based capital requirements for market risk ([MAR]) are to be applied to Group 1 cryptoasset exposures under the Simplified Standardised Approach ([MAR40]), the Standardised Approach ([MAR20] to [MAR23]), and the Internal Models Approach ([MAR30] to [MAR33]).

Application of the Simplified Standardised Approach to Group 1 cryptoassets

60.41 When calculating market risk capital requirements for Group 1 cryptoassets under the Simplified Standardised Approach, as defined in [MAR40], banks must apply the following specifications:

(1) All instruments, including derivatives and off-balance sheets positions that are affected by changes in Group 1 cryptoassets prices must be included;

(2) Banks will first have to express each Group 1 cryptoasset position in terms of their quantity, then convert at the current spot price into the bank's reporting currency;

(3) Banks must consider for Group 1 cryptoassets the same risk classes as the one used for traditional assets they digitally represent (ie interest rate risk, equity risk, FX risk and commodities risk), as defined in [MAR40.3] to [MAR40.73].

(4) Banks must consider for Group 1 cryptoassets the same treatment for options as the one defined for traditional assets they digitally represent (see [MAR40.74] to [MAR40.86]).

(5) Netting and hedging are recognised between Group 1a cryptoassets and the traditional assets they digitally represent, and both must be mapped to the same risk class. Netting and hedging are recognised between Group 1b cryptoassets and the traditional asset that the cryptoasset references, and both must be mapped to the same risk class.

(6) If present in a Group 1b cryptoasset, the risk of default of the redeemer and the risks arising when intermediaries perform the redemption function should be treated in line with the minimum risk-based capital requirements for credit risk.

Application of the Standardised Approach to Group 1 cryptoassets

60.42 When calculating market risk capital requirements for Group 1 cryptoassets under the Standardised Approach, as defined in [MAR20] to [MAR23], banks must apply the specifications set out in [SCO60.43] to [SCO60.45] below.

60.43 Group 1 cryptoassets must be mapped to the current risk classes set out in the sensitivities-based method. Specifically:

(1) Each tokenised instrument in Group 1 should be decomposed into the same risk factors as the traditional asset it digitally represents. For the tokenised asset, its sensitivities to the traditional risk factors should be identical to those of the traditional asset it digitally represents within the respective current risk classes.

(2) Each stablecoin instrument in Group 1 should be decomposed into the same risk factors as the traditional asset(s) that it references. Its sensitivities to the traditional risk factors should be identical to those of the traditional asset(s) that it references within the current risk classes.

60.44 For the default risk capital (DRC) requirement, Group 1 cryptoassets should have its gross jump-to-default (JTD) considered as equivalent to those from the traditional asset it digitally represents or references.

60.45 If present in a Group 1b cryptoasset, the risk of default of the redeemer and the risks arising when intermediaries perform the redemption function should be treated in line with the minimum risk-based capital requirements for credit risk.

Application of the Internal Models Approach to Group 1 cryptoassets

60.46 When calculating market risk capital requirements for Group 1 cryptoassets under the Internal Models Approach (IMA), as defined in [MAR30] to [MAR33], banks must apply the specifications set out in [SCO60.47] to [SCO60.51] below.

60.47 To determine the aggregate capital requirement under the IMA banks need to calculate a default risk capital (DRC) requirement according to [MAR33.21] and an aggregate non-DRC requirement according to [MAR33.41]. For the latter, the bank will need to determine an aggregate stressed expected shortfall (SES) capital measure according to [MAR33.17] for the non-modellable risk factors and an aggregate capital requirement for modellable risk factors (IMCC) according to [MAR33.15].

60.48 The use of the IMA for instruments referencing Group 2 cryptoassets is not permitted.

60.49 The capital treatment prescribed for the non-DRC requirement allows mapping of exposures to risk factors as follows:

(1) Each tokenised instrument in Group 1 must be decomposed into the same risk factors as the traditional asset it digitally represents within the respective current risk classes.

(2) Each stablecoin instrument in Group 1 must be decomposed into the same risk factors as the traditional asset(s) that they reference within the respective current risk classes.

60.50 For the DRC requirement, tokenised asset and non-tokenised asset are regarded as different instruments to the same obligor. Similarly, traditional assets referenced by stablecoins and the stablecoin themselves are regarded as different instruments to the same obligor. The DRC requirement must account for different losses in the different instruments based on [MAR33.25]. Differences in instruments should be reflected in LGD estimates. Maturity mismatches between tokenised and non-tokenised assets, and between stablecoins and the traditional assets they reference, need to be captured based on [MAR33.28].

60.51 If present in a Group 1b cryptoasset, the risk of default of the redeemer and the risks arising when intermediaries perform the redemption function must be treated in line with the minimum risk-based capital requirements for credit risk.

Add-on for infrastructure risk for Group 1 cryptoassets

60.52 The technological infrastructure that underlies all cryptoassets, such as the DLT, is still relatively new and may pose various additional risks even in cases where the cryptoassets comply with the Group 1 classification conditions. Therefore, authorities must have the power to apply an add-on to the capital requirement for exposures to Group 1 cryptoassets.

60.53 The add-on for infrastructure risk described above will initially be set as zero but will be increased by authorities based on any observed weakness in the infrastructure used by Group 1 cryptoassets.

Minimum capital requirements for credit and market risk for Group 2 cryptoassets

60.54 Group 2 cryptoassets are divided into:

(1) Group 2a: cryptoassets that meet the hedging recognition criteria set out in [SCO60.55] below. Group 2a cryptoassets are subject to modified versions of the Simplified Standardised Approach or the Standardised Approach to market risk set out in [SCO60.57] to [SCO60.82] below. The treatment permits some recognition of hedging. The Internal Models Approach is not applicable to Group 2a cryptoassets.

(2) Group 2b: cryptoassets that do not meet the hedging recognition criteria. Group 2b cryptoassets are subject to a new conservative treatment set out in [SCO60.83] to [SCO60.86] below, which does not permit banks to recognise hedging. A Group 2 cryptoasset must be classified as Group 2b, unless a bank demonstrates to the supervisor that the cryptoasset meets hedging recognition criteria.

Group 2a hedging recognition criteria

60.55 Group 2 cryptoassets that are assessed to meet all three of the following hedging recognition criteria, will be classified as Group 2a:

(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.

(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.

(2) The bank's cryptoasset exposure, or the cryptoasset referenced by the derivative or ETF/ETN, is highly liquid. Specifically, both of the following must apply:

(a) The average market capitalisation was at least USD10 billion over the previous year.

(b) The 10% trimmed mean of daily trading volume with major fiat currencies is at least USD50 million over the previous year.

(3) Sufficient data is available over the previous year. Specifically, both of the following must apply:

(a) There are at least 100 price observations over the previous year. The price observations must be "real" as defined in the four criteria of [MAR31.12].

(b) There are sufficient data on trading volumes and market capitalisation.

60.56 The capital requirements for Group 2a cryptoassets may be calculated according to:

(1) a modified version of the Simplified Standardised Approach (SSA) in the market risk standard set out in [SCO60.57] to [SCO60.65] below; or

(2) a modified version of the Standardised Approach (SA) in the market risk standard set out in [SCO60.66] to [SCO60.82] below.

Capital requirements Group 2a cryptoassets: simplified standardised approach (SSA)

60.57 For Group 2a cryptoassets, the SSA ([MAR40]) will include a separate risk class with its capital requirement determined based on the specifications set out in [SCO60.58] to [SCO60.65] below.

60.58 All instruments, including derivatives and off-balance sheets positions that are affected by changes in Group 2a cryptoasset prices must be included.

60.59 Banks must first express each Group 2a cryptoasset position in terms of its quantity, and then convert it at the current spot price into the bank's reporting currency.

60.60 When consolidated, positions for each Group 2a cryptoasset in different markets or exchanges must not be offset, meaning those sensitivities will be calculated as separate long and short gross consolidated positions. In addition, only the products listed in [SCO60.55](1) may be used for the purposes of offsetting and for the purposes of calculating the net position set out in [SCO60.61] below. Other products that reference Group 2a cryptoassets are subject to the capital requirements that apply to Group 2b cryptoassets.

60.61 For each Group 2a cryptoasset a net position must be determined based on the following formula:

$$Net\ position_k = Max(Long\ position_k, |Short\ position_k|) - 0.65 * Min(Long\ position_k, |Short\ position_k|)$$

60.62 The capital requirement for position risk of a Group 2a cryptoasset will be 100% of its respective net position.

60.63 The total capital requirement for position risk consists of the simple sum of all Group 2a cryptoasset capital requirements.

60.64 Options with a Group 2a cryptoasset as their underlying asset must be treated under the scenario approach, in accordance with [MAR40.81] to [MAR40.86], using ±100% for the underlying price change and ±100% for the relative volatility change.

60.65 The Group 2a risk class total capital requirement must be aggregated in accordance with [MAR40.2]. Instead of the scaling factors in [MAR40.2], a scaling factor of 1 shall apply to the Group 2a risk class total capital requirement.

Capital requirements Group 2a cryptoassets: standardised approach (SA)

60.66 For Group 2a cryptoassets the SA ([MAR20] to [MAR23]) will include a separate risk class with its capital requirement determined based on the specifications set out in [SCO60.67] to [SCO60.82] below.

60.67 All risk factors, including those related to derivatives and off-balance sheets positions that are affected by changes in Group 2a cryptoasset prices must be included.

60.68 Banks must first express each Group 2a cryptoasset position in terms of its quantity, and then convert it at their current spot price into the bank's reporting currency.

60.69 When consolidated, sensitivities for each Group 2a cryptoasset in different markets or exchanges must not be offset, meaning those sensitivities will be calculated as separate long and short gross consolidated sensitivities. In addition, only the products listed in [SCO60.55](1) may be used for the purposes of offsetting and for the purposes of calculating the net capital set out in [SCO60.71] to [SCO60.82] below. Other products that reference Group 2a cryptoassets are subject to the capital requirements that apply to Group 2b cryptoassets.

60.70 The computation of the sensitivities-based method for Group 2a cryptoassets includes new specifications of delta, vega and curvature risk factors. The sensitivity definitions are also extended to include that of Group 2a cryptoassets. Finally, a new bucket structure is introduced, composed of multiple buckets, one for each Group 2a cryptoasset, containing only its respective sensitivities.

60.71 *Group 2a cryptoasset delta spot specification*: the sensitivity is measured by changing the Group 2a cryptoasset spot price by 1 percentage point (ie 0.01 in relative terms) and dividing the resulting change in the market value of the instrument V_i by 0.01 (ie 1%) as follows, where:

(1) k is a given Group 2a cryptoasset;

(2) $CRYPTO(G2a)_k$ is the market value of the Group 2a cryptoasset k; and

(3) V_i is the market value of instrument i as a function of the price of the Group 2a cryptoasset k.

$$s_k = \frac{V_i(1.01 \cdot CRYPTO(G2a)_k) - V_i(CRYPTO(G2a)_k)}{0.01}$$

60.72 *Group 2a cryptoasset vega specification*: the option-level vega risk sensitivity to a given Group 2a cryptoasset must be determined as prescribed by [MAR21.25].

60.73 *Bucket structure*: the new risk class will comprise "n" buckets, where each bucket corresponds to the aggregate positions in a specific Group 2a cryptoasset; this is reflected in the following tables.

Delta cryptoasset buckets and risk weights		
Bucket number	*Group 2a cryptoasset*	*Risk weight*
1	Cryptoasset X_1	100%

…	…	…
n	Cryptoasset X_n	100%

Vega cryptoasset buckets and risk weights		
Bucket number	*Group 2a cryptoasset*	*Risk weight*
1	Cryptoasset X_1	100%
…	…	…
n	Cryptoasset X_n	100%

60.74 *Delta (vega) capital requirements*: Delta sensitivities must be determined based on a risk factor structure ([MAR21.13]) considering two dimensions[9]:

(1) Exchange; and

(2) time to maturity, at the following tenors: 0 years, 0.25 years, 0.5 years, 1 year, 2 years, 3 years, 5 years, 10 years, 15 years, 20 years and 30 years.

Footnotes

[9] That is, distinct risk factors need to be considered for identical contracts traded on different exchanges or at different tenors, so that no perfect offsetting is permitted between risk factors arising from different exchanges or different tenors.

60.75 For vega sensitivities, no differentiation by exchange or underlying maturity is considered. Group 2a cryptoasset vega risk factors are defined along one dimension, the maturity of the option, mapped to one or more of the following tenors: 0.5 years, 1 year, 3 years, 5 years and 10 years.

60.76 In order to calculate the delta (or vega) capital requirements for a single bucket b $\rho_{kl} = 94\%$.

60.77 The delta capital requirement, K_b, for a single bucket b is calculated as follows:

$$K_b = \sqrt{max\left(0, \sum_k WS_k^2 + \sum_k \sum_{k \neq l} \rho_{kl} WS_k WS_l\right)}$$

60.78 The delta capital requirement for the Group 2a cryptoasset risk class is $\sum_b K_b$, taking into account that there is no recognition of diversification between different Group 2a cryptoassets.

60.79 *Curvature capital requirements*: for the curvature risk capital requirement, the delta buckets specified above must be used. The curvature sensitivities must be calculated by shifting all tenors in parallel (ie no term structure decomposition is required). For calculating the net curvature risk capital requirement CVR_k for the risk factor k for the Group 2a cryptoasset, the curvature risk weight, which is the size of a shock to the given risk factor, is a relative shift equal to the delta risk weight.

60.80 For aggregating curvature risk positions within a bucket, the following formula must be used:

$$K_b = max(K_b^+, K_b^-), where$$
$$K_b^+ = \sum_k |CVR_k^+|$$
$$K_b^- = \sum_k |CVR_k^-|$$

60.81 Curvature risk cannot be diversified across buckets. The total curvature risk capital across the entire portfolio is $\sum_b K_b$.

60.82 Group 2a cryptoassets are not subject to the DRC capital requirement. In case of a stablecoin included in Group 2a, the risk of default of the redeemer and the risks arising when intermediaries perform the redemption function must be treated in line with the minimum risk-based capital requirements for the credit risk (CRE) section.

Capital requirements Group 2b cryptoassets

60.83 There is no separate trading book and banking book treatment for Group 2b cryptoassets. The conservative treatment is intended to capture both credit and market risk, including credit valuation adjustment (CVA) risk. For consistency, the RWA calculated under this approach must all be reported as part of the bank's credit RWA. In addition to direct exposures, the conservative prudential treatment set out in [SCO60.84] to [SCO60.86] below also applies to:

(1) Funds of Group 2b cryptoassets (eg Group 2b cryptoasset ETFs) and other entities, the material value of which is primarily derived from the value of Group 2b cryptoassets.

(2) Equity investments, derivatives or short positions in the above funds or entities.

60.84 For each separate Group 2b cryptoasset to which they are exposed, banks must apply a risk weight of 1250% to the greater of the absolute value of the aggregate long positions and the absolute value of the aggregate short positions in the cryptoasset. That is, RWA for each separate cryptoasset to which the bank is exposed is calculated as follows:

$$RWA = RW \times \max[\text{abs (long exposure)}, \text{abs (short exposure)}]$$

60.85 For each cryptoasset derivative (ie a derivative with a Group 2b cryptoasset as the underlying asset), the exposure value used in the above formula is the value of its underlying cryptoassets. For leveraged derivatives (ie a derivative that returns a multiple of the value of the underlying), the exposure value of the underlying position must be adjusted upward to take account of the leverage. The exposure value calculated according to this paragraph can be capped at the maximum possible loss on the cryptoasset derivative.

60.86 The application of the 1250% risk weight set out in [SCO60.84] will ensure that banks are required to hold minimum risk-based capital at least equal in value to their Group 2b cryptoasset exposures. For simplicity, the formula also applies the 1250% risk weight to short positions. Theoretically, short positions and certain other types of exposures could lead to unlimited losses. Thus, in some circumstances, the formula could require capital that is insufficient to cover potential future losses. Banks will be responsible for demonstrating the materiality of these risks under the supervisory review of cryptoassets and whether risks are materially underestimated. Supervisors will be responsible for considering an additional capital charge in the form of a Pillar 1 add-on in cases where banks have material exposures to short positions in cryptoassets or to cryptoasset derivatives that could give rise to losses that exceed the capital required by the 1250% risk weight. In those cases, the capital add-on will be calibrated by requiring banks to calculate aggregate capital requirements under the Committee's market risk framework (applying a 100% risk weight for delta, vega, and curvature) and Basic CVA risk framework (BA-CVA) and to use this amount if the result is higher than the requirement based on a 1250% risk weight.

Minimum capital requirements for Credit Valuation Adjustment (CVA) risk

60.87 This section describes how the minimum risk-based capital requirements for CVA risk ([MAR]) are to be applied to cryptoasset derivatives exposures and material and fair-valued securities financing transactions (SFTs) referencing cryptoassets, as described in [MAR50].

Group 1a (tokenised traditional assets)

60.88 Derivatives and SFTs on Group 1a cryptoassets will generally be subject to the same rules to determine CVA RWA as non-tokenised traditional assets (ie the rules set out in the market risk

standard [MAR50]). In other words, if a bank holds a derivative or an SFT on a tokenised asset having a price close to the traditional asset and being subject to CVA risk as set out in [MAR 50], it will be reflected in the CVA risk charge in the same way as a derivative or SFT on the non-tokenised traditional asset.

60.89 Banks must assess the tokenised traditional asset itself against the rules set out in [MAR50]. Qualification for a given treatment cannot be derived from the respective traditional (non-tokenised) asset. This requirement of individual assessment includes, but is not limited to, the liquidity characteristics. Different liquidity characteristics between the traditional (non-tokenised) asset and the tokenised asset could result in a higher basis risk between the two. In case of insufficient data availability to model the impact of these different liquidity characteristics on their market values, especially of the exposure underlying CVA, the SA-CVA cannot be applied for calculating CVA risk, ie such tokenised assets are subject to the BA-CVA.

Group 1b cryptoassets (cryptoassets with stabilisation mechanisms)

60.90 Derivatives on Group 1b cryptoassets will be subject to the same rules to determine CVA RWA as non-tokenised traditional assets (ie the rules set out in the market risk standard [MAR50]).

Group 2a cryptoassets

60.91 Group 2a cryptoassets will be only subject to the rules set out in the market risk standard [MAR50.1] to [MAR50.26]. The use of SA-CVA is not permitted to be used for derivatives and SFTs referencing Group 2a cryptoassets.

Group 2b cryptoassets

60.92 The treatment of CVA risk for Group 2b cryptoassets is covered in [SCO60.83] to [SCO60.86] above.

Minimum capital requirements for Counterparty Credit risk (CCR)

60.93 This section describes how the minimum risk-based capital requirements for counterparty credit risk (CCR) are to be applied to derivatives referencing cryptoassets.

60.94 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 haircut that is used for equities that are not traded on a recognised exchange (ie a haircut of 25%).

Group 1a (tokenised traditional assets)

60.95 Derivatives on Group 1a cryptoassets will generally be subject to the same rules to determine CCR as non-tokenised traditional assets (ie the rules set out in [CRE50] to [CRE56]), which includes the Internal Models Method (IMM), where the same requirements apply for tokenised assets as for traditional assets.

60.96 For the cases described in [SCO60.89] for CVA risk, especially in presence of significant valuation differences between the traditional and the tokenised asset and in presence of significant basis

risk, there could be limitations to apply the IMM in case of missing data or too short history or in presence of data quality problems, which then requires to apply the SA-CCR as described below for Group 2a cryptoassets.

Group 1b cryptoassets (cryptoassets with stabilisation mechanisms)

60.97 Derivatives on Group 1b cryptoassets will be subject to the same rules to determine CCR RWA as non-tokenised traditional assets (ie the rules set out in the credit risk standards [CRE50] to [CRE56]).

Group 2a cryptoassets

60.98 Derivatives on Group 2a cryptoassets will be subject to the SA-CCR (ie the rules set out in the credit risk standard [CRE52]), amended by the following:

(1) The replacement cost (RC) takes legally enforceable netting of all transaction types in the netting set into account, which may include derivatives on Group 2a cryptoassets.

(2) In order to calculate the potential future exposure (PFE) add-on, a new asset class "crypto" will be created in the SA-CCR.

(a) The mathematical structure for calculating the PFE add-on for this asset class will be in line with the structure used in the foreign exchange asset class, but with different parameters.

(b) There are separate hedging sets for each crypto currency priced in applicable fiat currencies or in another Group 2a crypto currency.

(c) The supervisory factor calibrated in line with those for traditional assets in SA-CCR will be 32% for all cryptocurrency-fiat currency and cryptocurrency-cryptocurrency pairs, and the supervisory option volatilities will equal [120%].

(d) The calculation of the adjusted notional will be set to the cryptoasset's notional expressed in the domestic fiat currency of each bank. For the case of a cryptocurrency priced in another cryptocurrency, the larger of the two adjusted notionals will apply.[10]

(e) The calculation of the supervisory delta adjustment and the maturity factor will be the same as for the other asset classes.

(f) The aggregation of the hedging sets PFE add-ons of class "crypto" will be the same as for the other asset classes by summing up.

Footnotes

[10] If pairs to the domestic currency are not liquidly traded, the most liquid fiat currency needs to be taken with FX spot rates against the domestic fiat currency.

Group 2b cryptoassets

60.99 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)[11] 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. 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

[11] The replacement cost is subject to a floor of zero.

Minimum capital requirements for operational risk

60.100 The operational risk resulting from cryptoasset activities should generally be captured by the operational risk standardised approach (OPE25) through the Business Indicator – which should include income and expenses resulting from activities relating to cryptoassets – and through the Internal Loss Multiplier – which should include the operational losses resulting from cryptoasset activities. To the extent that operational risks relating to cryptoassets are insufficiently captured by the minimum capital requirements for operational risk and by the internal risk management process of the banks, banks and supervisors should take appropriate steps to ensure capital adequacy and sufficient resilience in the context of supervisory review process ([SRP]). Some key dimensions of this issue elaborated in [SCO60.120] to [SCO60.127].

Minimum liquidity risk requirements

60.101 For the liquidity coverage ratio (LCR) and net stable funding ratio (NSFR) requirements, cryptoasset exposures, including assets, liabilities and contingent exposures, must generally follow a treatment that is consistent with existing approaches for traditional exposures with economically equivalent risks. At the same time, the treatment must also appropriately reflect the additional risks that may be present with these assets in comparison to traditional assets, and the relative lack of historical data. Accordingly, the treatment of cryptoassets largely relies on the principles and calibrations set forth in the LCR and NSFR standards (see [LCR] and [NSF]). However, these standards require additional clarification and elaboration to address the novel and unique risks associated with cryptoassets.

Treatment as high-quality liquid assets (HQLA)

60.102 Group 1a cryptoassets that are a tokenised version of HQLA as defined in [LCR30.40] to [LCR30.47] may only be considered as HQLA to the extent both the underlying assets in their traditional form and the tokenised form of the assets satisfy the characteristics of HQLA in [LCR30.2] to [LCR30.12].[12] An example of such a Group 1a cryptoasset could be a tokenised bond that meets these HQLA eligibility criteria and temporarily resides on a distributed ledger to facilitate transfer.

Footnotes

[12] Note that to be considered in the LCR's stock of HQLA, these assets must also satisfy the operational requirements in [LCR30.13] to [LCR30.28].

60.103 Group 1b and Group 2 cryptoassets, by contrast, must not be considered HQLA.

General considerations for the application of the LCR and NSFR frameworks

60.104 The appropriate classification and calibration of LCR outflow and inflow rates and NSFR available stable funding (ASF) and required stable funding (RSF) factors of cryptoassets and cryptoliabilities depend on factors such as the structure of the cryptoasset or cryptoliability, its commercial function in practice and the nature of a bank's exposure to the cryptoasset or cryptoliability.

60.105 In general, exposures involving Group 1a cryptoassets and cryptoliabilities must be treated the same as exposures involving their equivalent non-tokenised traditional assets and liabilities, including the assignment of inflows, outflows, RSF factors and ASF factors.

60.106 As set out in [SCO60.107] to [SCO60.112] below, the LCR and NSFR treatment of exposures involving cryptoassets and cryptoliabilities varies according to whether they are:

(1) Tokenised claims on a bank.

(2) Stablecoins.

(3) Other cryptoassets.

60.107 *Tokenised claims on a bank*. Group 1a tokenised claims on a bank must be treated as an unsecured funding instrument when they are: (i) issued by a regulated and supervised bank; (ii) represent a legally binding claim on the bank; (iii) redeemable in fiat currency at par value; and (iv) have a stable value supported by the creditworthiness and asset-liability profile of the issuing bank rather than a segregated pool of assets. The treatment as an unsecured funding instrument is subject to the following considerations:

(1) The maturity of the claim on a bank must be determined based upon the contractual redemption rights available to the holder.

(2) For liabilities from own-issued tokenised claims on a bank:

(a) The bank must assign LCR outflow rates and NSFR ASF factors based on the earliest date upon which the liability could be redeemed and the counterparty type of the holder, in accordance with the treatment of retail funding and unsecured wholesale funding in [LCR40] and [NSF30].

(b) To the extent the issuing bank can identify, at all times, the holder of the cryptoasset, then the bank must apply the applicable outflow rate and ASF factor based on the counterparty classification of the funds provider. However, the issuing bank must not treat the liabilities associated with their cryptoassets as stable retail deposits. If the issuing bank is unable to identify, at all times, the holder of the cryptoasset, it must treat the liability as unsecured wholesale funding provided by *other legal entity customers* (see [LCR40.42]).

(c) Tokenised claims on a bank that are used primarily as a means of payment and created as part of an operational relationship between the issuing bank and its wholesale customers must follow the categorisation methodology in [LCR40.26] to [LCR40.35]. These liabilities are not eligible for the lower outflow rate specified in [LCR40.36].

(3) When a bank holds another bank's issuance of such a tokenised liability:

(a) The holder must not recognise inflows in the LCR if the cryptoasset is not redeemable within 30 days.

(b) The holder must not recognise inflows in the LCR and must assign a minimum RSF factor of 50% in the NSFR if the cryptoasset is held for operational purposes, in alignment with [LCR40.89] and [NSF30.29]. The holder may recognise inflows in the LCR and an RSF factor of 15% in the NSFR if the cryptoasset is not held for operational purposes, in alignment with [LCR40.89] and [NSF30.28](2).

(4) Notwithstanding the clarifications above, supervisors must apply more stringent LCR and NSFR treatment if, having considered the features and liquidity risk profiles of a

tokenised claim on a bank, they conclude that there may be additional liquidity risk inherent in a given liability (eg if some characteristics of the cryptoasset may increase the propensity of a holder to seek redemption during a period of stress, or alternatively constrain a holder from redeeming its funds, etc.). For example, this conclusion may be based upon factors including, but not limited to, the technical design of the liability (eg reliance on non-regulated entities as wallet providers or third-party blockchain operators and usage characteristics of stablecoin implementations, etc.) and the local circumstances of the banking sector.

60.108 *Stablecoins*. Group 1b cryptoassets, and certain Group 2[13] cryptoassets that are fully collateralised by a segregated pool of underlying assets that do not count toward the bank's stock of HQLA, must be treated similar to securities, subject to the following considerations:

(1) When a bank is an issuer of such a stablecoin and the stablecoin issuance represents a legally binding claim on the bank:

(a) The issuing bank must recognise 100% outflows in the LCR if the stablecoin is redeemable within 30 days. The issuing bank must assign an ASF factor in accordance with [NSF30.10], [NSF30.13] and [NSF30.14] based upon the earliest date upon which the stablecoin could be redeemed.

(b) The issuing bank may recognise reduced outflows in the LCR to the extent the stablecoin is backed by HQLA that is not included in its eligible HQLA amount, but would be unencumbered and freely available to be liquidated upon a redemption of the stablecoin. The reduction in outflows must incorporate the haircuts specified in [LCR30] and must not result in net inflows.

(c) The assets segregated to support the value of the stablecoin must be assigned a minimum RSF factor for encumbered assets as specified in [NSF30.20] based upon the earliest date upon which the stablecoin could be redeemed.

(2) When a bank holds such a stablecoin on its balance sheet:

(a) As non-HQLA these stablecoins must be subject to at least an 85% RSF in the NSFR and not result in inflows under the LCR.

(b) However, a holder of the stablecoin may recognise inflows in the LCR or a reduced RSF factor in the NSFR to the extent that, similar to a debt security, the stablecoin has a final contractual maturity and the maturity of the stablecoin would result in an inflow of fiat currency within the 30-day or 1-year time horizon. A bank must not assume it exercises an option to redeem the stablecoin prior to any final contractual maturity.

Footnotes

[13] Stablecoins that do not qualify as Group 1b cryptoassets due to redemption restrictions (ie minimum notice periods) will be included in Group 2. They will, however, be eligible for the treatment outlined in this paragraph provided they satisfy all criteria for classification under Group 1b except the requirement to be redeemable at all times, as specified in [SCO60.12].

60.109 *Other cryptoassets*. The treatment of Group 2 cryptoassets that do not qualify for the treatment outlined in [SCO60.107] and [SCO60.108] above must be aligned with the treatment of other non-HQLA applicable in the LCR and NSFR standards, subject to the following considerations:

(1) A bank that holds other Group 2 cryptoassets or loans denominated in these assets on its balance sheet must assign 100% RSF to the carrying value of these assets in the NSFR

and must not recognise any inflows associated with the liquidation, redemption or maturity of these assets.

(2) A bank that has borrowed other Group 2 cryptoassets on an unsecured basis and has an obligation to return these assets within 30 days must apply a 100% outflow rate against the market value of the asset that must be returned to the bank's customer or counterparty, unless the obligation can be settled with certainty from the bank's own unencumbered inventory of the same Group 2 cryptoasset. Similarly, borrowings denominated in other Group 2 cryptoassets must be assigned 0% ASF in the NSFR.

60.110 Supervisors should also consider adjusting outflow rates and stable funding requirements to account for contingent risks that may arise due to a bank's role in issuing or transacting in cryptoassets, such as the risk that a bank may provide non-contractual liquidity support for the redemption of certain stablecoins where it is the issuer or a material service provider to protect its franchise or otherwise avoid negative signalling effects.

60.111 The treatments outlined in [SCO60.108] to [SCO60.110] are not intended to modify the application of the LCR and NSFR frameworks where the types of exposures are not explicitly mentioned. These types of transactions include the following:

(1) Derivatives where the reference asset is a cryptoasset

(2) Secured funding and lending of fiat currency with cryptoassets as collateral

(3) Collateral swaps involving cryptoassets

(4) Commitments to lend cryptoassets

60.112 For the transactions listed in [SCO60.111], the treatment must be aligned with the existing framework, which generally applies consistently for all non-HQLA instruments.

Leverage ratio requirements

60.113 Consistent with the leverage ratio standard, cryptoassets are included in the leverage ratio exposure measure according to their value for financial reporting purposes, based on applicable accounting treatment for exposures that have similar characteristics. For the cases where the cryptoasset exposure is an off-balance sheet item, the relevant credit conversion factor set out in the leverage ratio framework will apply in calculating the exposure measure. Exposures for cryptoasset derivatives must follow the treatment of the risk-based capital framework.

60.114 For Group 1b cryptoassets, if the bank is involved in the cryptoasset network as a member who is able to deal directly with the redeemer and has promised to purchase cryptoassets from non-member holders, the member also needs to include the total current value of all the off-balance cryptoassets that the bank could be obliged to purchase from holders (as set out in [SCO60.37]).

Large exposures requirements

60.115 For large exposures purposes, the treatment for cryptoassets will follow the same principles as for other exposures as set out in [LEX]. Consistent with the requirements set out in [LEX], cryptoasset exposures that give rise to a credit risk exposure are included in the large exposure measure according to their accounting value as set out in [LEX30.2]. The bank must identify and apply the large exposure limits to each specific counterparty or group of connected counterparties to which it is exposed under the risk-based capital framework. Where the cryptoasset exposes the bank to the risk of default of more than one counterparty, the bank must compute for each counterparty the respective amount to which it is exposed to default risk for large exposure purposes. When the cryptoasset also entails a default risk of reference assets, these will be considered for the purpose of the large exposures framework and the bank must

follow the existing large exposures rules applicable to transactions with underlying assets (see [LEX30.42] to [LEX30.54]). Cryptoassets that do not expose banks to default risk (such as physical exposures of gold, other commodities or currencies, and exposures of some forms of cryptoassets with no issuer) do not give rise to a large exposures requirement; however, the counterparty credit risk exposures arising from derivative contracts that reference cryptoassets with no issuer will fall in the scope of the large exposure requirement.

Group 2 exposure limit

60.116 Banks' exposures to Group 2 cryptoassets will be subject to an exposure limit. Banks must apply the exposure limit to their aggregate exposures to Group 2 cryptoassets, including both direct holdings (cash and derivatives) and indirect holdings (eg those via investment funds, ETF/ETN, or any legal arrangements designed to provide exposures to cryptoassets).

60.117 A bank's total exposure to Group 2 cryptoassets should not generally be higher than 1% of the bank's Tier 1 capital and must not exceed 2% of the bank's Tier 1 capital.

60.118 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.

60.119 For the purposes of assessing compliance with the Group 2 exposure limit threshold:

(1) Exposures must be measured using the same methodology that applies for determining the Group 2b capital treatment outlined in [SCO60.83] to [SCO60.85]. That is, exposures to all Group 2 cryptoassets (Group 2a and Group 2b) must be measured using the higher of the absolute value of the long and short exposures in each separate cryptoasset to which the bank is exposed. Derivative exposures must be measured using a delta-equivalent methodology.

(2) Tier 1 capital is defined in [CAP10.2].

Bank risk management and supervisory review

60.120 This section describes how the supervisory review process ([SRP]) is to be applied in the case of banks' exposures to cryptoassets. It considers the responsibilities of both banks and supervisors and sets out potential supervisory actions in cases where risks are not sufficiently covered by minimum requirements or bank risk management is insufficient.

Bank risk management

60.121 Cryptoasset activities introduce new kinds of risk and increase certain traditional risks. Banks with direct or indirect exposures or that provide related services to any form of cryptoasset must establish policies and procedures to identify, assess and mitigate the risks (including operational risks, credit risks, liquidity risks including funding concentration risk and market risks) related to cryptoassets or related activities on an ongoing basis. The policies and procedures followed by banks for cryptoasset activities must be informed by existing Basel Committee statements on operational risk management generally and cryptoassets in particular.[14] In accordance with these policies and procedures, banks' operational risk management practices must include, but are not limited to, conducting assessments of these risks (ie how material these risks are, and how they

are managed) and taking relevant mitigation measures to improve their operational resilience capabilities (specifically regarding information, communication, and technology (ICT) and cyber risks). The decision to hold cryptoassets (either under trading or banking book) and provide services to cryptoasset operators must be fully consistent with the bank's risk appetite and strategic objectives as set down and approved by the board, as well as with senior management's assessment of the bank's risk management capabilities, in particular for market and counterparty risk (including CVA), liquidity risk (including funding concentration risk) and operational risk.

Footnotes

[14] See Principles for the Sound Management of Operational Risk; Principles for Operational Resilience; and Statement on Cryptoassets.

60.122 Considering the particular features of cryptoassets and their markets as well as the potential difficulties in adopting standard arrangements for managing related market risk and counterparty risk including credit valuation adjustment risk, banks must conduct ex-ante a prudent assessment of any cryptoasset exposures they intend to take on and verify the adequateness of existing processes and procedures. The bank must have a sound risk management approach for managing the risks of cryptoassets, including limits and hedging strategies, together with clearly assigned responsibilities for the management of these risks. Particular attention must be paid to the assessment of the effectiveness of any hedging techniques banks may adopt.

60.123 Banks must also inform their supervisory authorities of their policies and procedures, assessment results, as well as their actual and planned cryptoasset exposures or activities in a timely manner and to demonstrate that they have fully assessed the permissibility of such activities, the associated risks and how they have mitigated such risks.

60.124 The mapping of risks relating to cryptoasset activities to the risk categories of the Basel capital framework (credit risk, market risk, and operational risk in particular) depends on how these risks manifest. Many of the risks introduced or increased by cryptoasset activities are covered by the operational risk framework (eg ICT and cyber risks, legal risks, money laundering and financing of terrorism). A mapping of the technological risks of cryptoassets to Basel risk categories would depend on the circumstances. If the triggering event leading to a loss is due to processes or systems outside of the bank's control and the loss to the bank manifests through the value of a bank position in cryptoassets, such losses would be covered by the credit risk framework (for banking book positions) or the market risk framework (for trading book positions). When losses result from inadequate or failed processes, people or systems of the bank (eg loss of a private cryptographic key by the bank), such losses would be operational losses.

60.125 Risks that banks need to consider in their risk management of cryptoassets activities include, but are not limited to, the following:

(1) *Cryptoasset technology risk*: Banks must closely monitor the risks inherent to the supporting technology, whether cryptoasset activities are conducted directly or through third parties, including but not limited to:

(a) *Stability of the DLT or similar technology network*: The reliability of the source code, governance around protocols and integrity of the technology are among key factors related to stability of the network. Key considerations include capacity constraints, whether self-imposed or due to insufficient computing resources; digital storage considerations; scalability of the underlying ledger technology; whether the underlying technology has been tested and had time to mature in a market environment; and robust governance around changes to the terms and conditions of the distributed ledger or cryptoassets (eg so-called 'forks' that change the underlying 'rules' of a protocol). In addition, the type of

consensus mechanism (ie for a transaction to be processed and validated) is an important consideration as it relates to the security of the network and whether it is safe to accept a transaction as 'final'.

(b) *Validating design of the DLT, permissionless or permissioned*: Cryptoassets may rely on a public ('permissionless') ledger, whereby the validation of transactions can be done by any participating agent, or distributed among several agents or intermediaries, which could be unknown to the users. In contrast, a private ('permissioned') ledger restricts and pre-defines the scope of validators, with the validating entities known to the users. On a permissionless ledger, there may be less control of technology and on a permissioned ledger there may be a small group of validators with greater control. Risks related to the validating design of the DLT include the accuracy of the transaction records, settlement failure, security vulnerabilities, privacy/confidentiality, and the speed and cost of transaction processing.

(c) *Service accessibility*: One of the distinguishing features of cryptoassets is its accessibility to holders of these assets. A holder of cryptoassets is assigned a set of unique cryptographic keys, which allow that party to transfer the cryptoassets to another party. If those keys are lost, a holder will generally be unable to access the cryptoassets. This increases the possibility of fraudulent activities such as a third-party gaining access to cryptographic keys and using the keys to transfer the cryptoasset to themselves or another unauthorised entity. Furthermore, the risk of a large-scale cyber-attack could leave banks' customers unable to access or recover cryptoasset funds.

(d) *Trustworthiness of node operators and operator diversity*: Since the underlying technology and node operators facilitate the transfer of cryptoassets and keep records of transactions that take place across the network, their role is essential in designating and sizing the amounts that are held by the holder. Whether nodes are run by a single operator or are distributed among many operators and whether the operators are trustworthy (eg whether the nodes are run by public/ private institutions or individuals) are relevant considerations in third-party risk management.

(2) *General information, communication and technology (ICT) and cyber risks*: A bank holding cryptoassets may be exposed to additional ICT and cyber risks that include but are not limited to cryptographic key theft, compromise of login credentials, and distributed denial-of-service (DDoS) attacks. The results of ICT failure and cyber-threats may lead to consequences such as unrecoverable loss or unauthorised transfers of cryptoassets.

(3) *Legal risks:* Cryptoasset activities are still recent and quickly evolving. Thus, their legal framework remains uncertain and banks' legal exposure is heightened, especially in the following dimensions:

(a) *Accounting*: There may be legal risk arising from a lack of accounting standards for cryptoassets, which could result in fines due to the underpayment of taxes or failure to comply with tax reporting obligations.

(b) *Taking control/ownership*: There is substantial legal uncertainty around cryptoassets, which could raise questions as to whether banks that take cryptoassets as collateral can take possession in the event of default/margin call.

(c) *Disclosure and consumer protection*: Banks that issue/redeem or provide dealer or advisor services for cryptoassets can face legal risk around the disclosures they provide for the cryptoassets (including cryptoassets that are considered to be securities), particularly as regulations and laws continue to evolve (eg those around data privacy and data retention).

(d) *Uncertain legal status*: Jurisdictions can decide (and have decided) to ban cryptoasset mining for a variety of reasons, including its environmental impact. Such developments could reduce the amount of computing power available to secure a network.

(4) *Money laundering and financing of terrorism*: Banks in their role of providing banking services to Virtual Asset Service Providers (VASP) or to customers involved in Virtual Asset activities, or through engaging in VASP activities themselves need to apply the risk-based approach as set out by the Financial Action Task Force (FATF) for the purposes of Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT). Inadequate compliance with AML or CFT laws (including sanctions) and best practices could result in operational losses and reputational damages for banks.

(5) *Valuation*: Many cryptoassets pose valuation challenges, due (among other things) to their volatility and variable pricing on different exchanges, particularly given that most of the cryptoassets are currently traded on unregulated marketplaces. These challenges can result in losses for banks in a variety of contexts tied to mispricing due to inadequate operational processes.

Supervisory review

60.126 *Supervisory review of bank risk identification and assessment*: Under Pillar 2, supervisors evaluate how well banks assess their capital needs relative to their risks and take measures, where appropriate. As cryptoasset activities are relatively recent and evolving, their related risks are also evolving. Supervisory evaluation is therefore particularly relevant regarding these activities. Thus, supervisors should review the appropriateness of banks' policies and procedures for identifying and assessing those risks and the adequacy of their assessment results. Supervisors should exercise their authority to require banks to address any deficiencies in their identification or assessment process of cryptoasset risks. In addition, supervisors may recommend that banks undertake stress testing or scenario analysis to assess risks resulting from cryptoasset exposures. Such analyses can inform assessments of the bank's capital adequacy.

60.127 Upon the identification of capital inadequacy or shortcomings in bank risk management, the specific supervisory action may vary according to the circumstances. The types of response that supervisors may consider include the following:

(1) *Additional capital charges*: Supervisors may impose additional capital charges to individual banks for risks not sufficiently captured under the minimum capital requirements for operational risk, credit risk, or market risk. Also, add-ons may be needed in cases where the bank risk management of cryptoassets is considered inadequate.

(2) *Provisioning*: Supervisors may request banks to provision for losses related to cryptoassets where such losses are foreseeable and estimable.

(3) *Supervisory limit or other mitigation measures*: Supervisors may impose mitigation measures on banks, such as requiring a bank to establish an internal limit to contain the risks not adequately identified or assessed in the bank's risk management framework.

Disclosure requirements

60.128 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.

60.129 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.

60.130 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).

Definitions

60.131 Set out below are definitions of various terms used in [SCO60]:

(1) *Cryptoassets*: private digital assets that depend primarily on cryptography and distributed ledger or similar technology.

(2) *Digital assets*: a digital representation in value which can be used for payment or investment purposes or to access a good or service. This does not include digital representations of fiat currencies.

(3) *Nodes*: typically participants (entities including individuals) in distributed ledger networks that record and share data across multiple data stores (or ledgers).

(4) *Operators*: typically a single administrative authority in charge of managing a cryptoasset arrangement, performing functions that may include issuing (putting into circulation) a centralised cryptoasset, establishing the rules for its use; maintaining a central payment ledger; and redeeming (withdraw from circulation) the cryptoasset.

(5) *Stablecoins*: cryptoasset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets.

(6) *Redeemers*: entities responsible for exchanging the cryptoasset for the traditional asset. It does not necessarily need to be the same as the entity responsible for organising the issuance of the cryptoasset.

(7) *Validators*: an entity that commits transactions blocks to the distributed ledger network.