Draft guideline

Title OSFI guideline on the regulatory capital and liquidity treatment of crypto-asset exposures (Banking) – Draft guideline

Date July 31, 2023

Table of Contents

Consultation status: Closed

Consultation closed September 20, 2023. We'll keep this draft on the site until the final guideline is released.

Introduction

1. This guideline on the regulatory capital and liquidity treatment of crypto-assets sets out the Office of the Superintendent of Financial Institution's (OSFI) expectations for federally regulated deposit-taking institutions' exposures to crypto-assets.[1] It is effective fiscal Q1 2025 and will replace the interim OSFI advisory on crypto-assets released on August 18, 2022.

Scope of application

2. Crypto-assets 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.[2] [SCO60.1 Crypto-asset exposures]

3. Dematerialized securities (securities that have been moved from physical certificates to electronic bookkeeping) that are issued through DLT or similar technologies are considered to be within the scope of this guideline and are referred to as **tokenized traditional assets**, whereas those dematerialized securities that use electronic versions of traditional registers and databases, which are centrally administered, are not within scope. [SCO60.2 Crypto-asset exposures]

4. The regulatory capital and liquidity treatment of central bank digital currencies (CBDCs) is not included in the scope of this guideline. [SCO60.3 Crypto-asset exposures]

5. For the purposes of this guideline, the term "exposure" includes on or off-balance sheet amounts that give rise to credit, market, operational and liquidity risks.[3] The operational risk requirements, and the risk management section, are also applicable to banks' crypto-asset activities, such as custodial services involving the safekeeping or administration of client crypto-assets on a segregated basis, that do not generally give rise to credit, market, or liquidity requirements. [SCO60.4 Crypto-asset exposures]

Simplified and comprehensive regulatory treatment options

6. **Simplified approach** - A simplified capital and liquidity treatment is available to banks with limited crypto-asset exposures, or to banks wishing to streamline or bypass classification determination detailed in the section that follows. These banks should apply a capital deduction to common equity tier 1 (CET1) capital for all their crypto-asset exposures (i.e. treat all their crypto-asset exposures as Group 2b exposures). For liquidity purposes, banks should apply the same treatment as other non-HQLA applicable assets in the liquidity coverage ratio (LCR) and net stable funding ratio (NSFR) standards.[4]

7. **Comprehensive approach** - Banks that do not use the simplified approach should categorize their crypto-asset exposures into one of four categories (i.e. Group 1a, 1b, 2a or 2b) introduced in the next section of this guideline, and detailed thereafter including in Annex 1 and Annex 3.

8. **Additional risk considerations (simplified and comprehensive approaches)** - All banks, whether applying the simplified or comprehensive approach, must consider credit valuation adjustment (CVA), counterparty credit risk (CCR), operational risk, leverage, and large exposure risk. Dedicated sections in this document provide guidance to banks on each of these areas with respect to their crypto-asset exposures.

9. Table 1 below summarizes the simplified and comprehensive approaches to the treatment of crypto-asset exposures.

Table 1: Simplified and comprehensive treatment for crypto-asset exposures

Simplified approach	Comprehensive approach
◦ Deduct all crypto-asset exposures from CET1 capital ◦ Crypto-assets are considered non-HQLA in the LCR and NSFR standards	◦ Capital and liquidity treatments vary depending on crypto-asset classification (i.e. Group 1a, 1b, 2a or 2b)
Other considerations include CVA, CCR, operational risk, leverage, and large exposures	

Categorization of crypto-assets

10. For the purposes of credit, market and liquidity risk, the regulatory capital and liquidity treatment of a bank's crypto-asset exposures varies according to the prudential classification of the crypto-assets. To determine the prudential classification, crypto-assets should be assessed on an ongoing basis and classified into two broad groups:

    1. **Group 1 crypto-assets** are those crypto-assets that meet the classification conditions set out in Annex 1. Group 1 crypto-assets consist of:

        1. Group 1a: Tokenized traditional assets that meet the classification conditions in Annex 1.

        2. Group 1b: Crypto-assets with effective stabilization mechanisms that meet the classification conditions. This includes stablecoins, which are crypto-assets that aim to maintain a stable value relative to a specified asset, or a pool or basket of assets, as measured by the criteria in this document.5

    2. **Group 2 crypto-assets** are those crypto-assets that fail to meet the classification conditions set out in Annex 1. Group 2 crypto-assets consist of:

        1. Group 2a: Crypto-assets (including tokenized traditional assets, stablecoins, and unbacked crypto-assets) that fail to meet the classification conditions set out in Annex 1, but pass the Group 2a hedging recognition criteria in Annex 3.

2. Group 2b: All other crypto-assets (i.e. tokenized traditional assets, stablecoins, and unbacked crypto-assets) that fail to meet the classification conditions set out in Annex 1 and fail the Group 2a hedging recognition criteria in Annex 3.

[SCO60.6 Crypto-asset exposures]

11. Figure 1 below summarizes the categorization of crypto-assets and their regulatory treatment. The capital requirements for crypto-asset exposures should be consistent with the requirements in the Capital Adequacy Requirements (CAR) and the Liquidity Adequacy Requirements (LAR), unless stated otherwise in this guideline.

Figure 1: Different categorizations of crypto-assets

Group 1

- **1a: Tokenized crypto-assets**
  - Consistent with the CAR and LAR treatment of the related asset
- **1b: Stablecoins**
  - Similar to 1a, but with additional criteria on the effectiveness of an asset's stabilization mechanism in Annex 1

Group 2

- **2a: Hedged crypto-assets**
  - Fails the classification conditions for Group 1, but satisfies the hedging recognition criteria in Annex 3
- **2b: Other crypto-assets**
  - Exposures will be fully deducted from CET1 capital

12. Banks, on an ongoing basis, are responsible for assessing whether the crypto-assets to which they are exposed are compliant with the classification conditions set out in Annex 1. Banks should fully document the information used in determining compliance with the classification conditions and make this available to OSFI upon request. OSFI may override banks' classification decisions if it does not agree with the assessments undertaken by banks. [SCO60.20 Crypto-asset exposures]

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

13. Chapter 9 of CAR should be used to determine the allocation of crypto-assets between the banking book and trading book, subject to the following specifications and exceptions:

    1. Group 1a crypto-assets should be assigned to the banking book or trading book based on the application of the boundary criteria to the non-tokenized equivalent traditional assets.

    2. Group 1b crypto-assets should 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 crypto-assets should be treated according to the proposed market risk rules, independent of whether they stem from trading or banking book instruments (i.e. similar to foreign currencies and commodities risk). As such, if a bank does not adhere to the market risk framework in Chapter 9 of CAR, its crypto-asset exposures are not eligible for this categorization.

    4. Group 2b crypto-assets should be treated according to the standardized conservative regulatory capital and liquidity treatment outlined in the capital requirements for group 2b crypto-assets of this guideline.

    [SCO60.23 Crypto-asset exposures]

14. CAR determines whether Group 1 crypto-asset exposures are treated according to standardized approach (SA) or internal ratings based (IRB) approaches to credit and market risk respectively. IRB approaches cannot be applied to Group 2 crypto-assets. [SCO60.24 Crypto-asset exposures]

15. Crypto-asset exposures are not subject to the deduction requirement that applies to intangible assets set out in Chapter 2 of CAR including in cases where the crypto-asset is classified as an intangible asset under IFRS. [SCO60.25 Crypto-asset exposures]

Capital requirements for credit risk of Group 1 crypto-assets

16. This section describes how the minimum risk-based capital requirements for credit risk are to be applied to Group 1 crypto-asset exposures, subject to an add-on for Group 1 crypto-assets set out in the add-on for infrastructure risk for Group 1 crypto-assets section below. [SCO60.26 Crypto-asset exposures]

Group 1a

17. Group 1a crypto-assets held in the banking book will generally be subject to the same expectations to determine credit risk-weighted assets (RWA) as non-tokenized traditional assets. For example, a tokenized corporate bond held in the banking book will be subject to the same risk weight as the non-tokenized corporate bond held in the banking book. [SCO60.27 Crypto-asset exposures]

18. The treatment outlined 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 should separately assess the tokenized traditional asset against these expectations, and not assume qualification for a given treatment simply because the traditional (non-tokenized) asset qualifies. For example, a tokenized asset may have different market liquidity characteristics than the traditional (non-

tokenized) asset. This could arise because the pool of potential investors that are able to hold tokenized assets might be different than for non-tokenized assets. [SCO60.28 Crypto-asset exposures]

19. Chapter 4 of CAR sets out the list of eligible forms of financial collateral for the purposes of recognition as a credit risk mitigant under the SA to credit risk. The list is also the basis of eligible financial collateral under the internal ratings-based approach. Only Group 1a crypto-assets that are tokenized versions of the instruments included on the list of eligible financial collateral set out in CAR may qualify for recognition as eligible collateral (subject to also meeting the expectations described above). [SCO60.30 Crypto-asset exposures]

20. The potential for market liquidity characteristics and market values of tokenized assets to differ from non-tokenized assets is important in considering whether Group 1a crypto-assets meet the expectations for the purposes of credit risk mitigation within the credit risk standards. Also, the speed with which a secured creditor could take possession of crypto-asset collateral may be different than for a traditional asset. Therefore, before such assets are recognized as collateral for the purposes of credit risk mitigation, banks should separately assess whether they comply with the relevant eligibility requirements for collateral recognition, such as whether the collateral can be liquidated in a timely manner and meet legal certainty requirements. In addition to assessing whether tokenized assets held as collateral are eligible to be recognized as credit risk mitigation, banks should analyze the period over which they can be liquidated and the depth of market liquidity during a period of downturn. Crypto-assets shall only be recognized as collateral when 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 crypto-asset 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. [SCO60.29 Crypto-asset exposures]

Group 1b

21. As a result of the classification conditions, Group 1b crypto-assets should 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 crypto-asset arrangement should include a sufficient pool of reserve assets to ensure the redemption claims

of crypto-asset holders can be met. Aside from these common elements, Group 1b crypto-assets may be structured in a variety of different ways. Banks that have banking book exposures to Group 1b crypto-assets should analyze their specific structures and identify all risks that could result in a loss. Each credit risk exposure should be separately capitalized by banks using the credit risk standards set out in CAR. For examples of this treatment, please refer to Annex 2. That 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. [SCO60.31 Crypto-asset exposures]

Capital requirements for market risk of Group 1 crypto-assets

22. This section describes how the minimum risk-based capital requirements are to be applied to Group 1 crypto-asset exposures under the SA and the IRB. [SCO60.40 Crypto-asset exposures]

Application of the SA to Group 1 crypto-assets

23. Group 1 crypto-assets should be mapped to the current risk classes set out in the sensitivities-based method. Specifically:

    1. Each tokenized instrument in Group 1 should be decomposed into the same risk factors as the traditional asset it digitally represents. For the tokenized asset, its sensitivity 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 in Group 1 should be decomposed into the same risk factors as the traditional asset(s) that it references. Its sensitivity to the traditional risk factors should be identical to those of the traditional asset(s) that it references within the current risk classes.

    [SCO60.43 Crypto-asset exposures]

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

[SCO60.44 Crypto-asset exposures]

25. If present in a Group 1b crypto-asset, 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. [SCO60.45 Crypto-asset exposures]

Application of the IRB approach to Group 1 crypto-assets

26. When calculating market risk capital requirements for Group 1 crypto-assets under the market risk framework, as defined in CAR, banks should apply the specifications set out in in the following paragraphs. [SCO60.46 Crypto-asset exposures]

27. To determine the aggregate capital requirement under the IRB, banks need to calculate a DRC requirement and an aggregate non-DRC requirement accordingly. For the latter, the bank will need to determine an aggregate stressed expected shortfall (SES) capital measure for the non-modellable risk factors and an aggregate capital requirement for modellable risk factors (IMCC). [SCO60.47 Crypto-asset exposures]

28. The use of the market risk framework for instruments referencing Group 2 crypto-assets is not permitted. [SCO60.48 Crypto-asset exposures]

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

    1. Each tokenized 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 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.

    [SCO60.49 Crypto-asset exposures]

30. For the DRC requirement, tokenized assets and non-tokenized assets are regarded as different instruments to the same obligor. Similarly, traditional assets referenced by stablecoins and the assets themselves are

regarded as different instruments to the same obligor. The DRC requirement should account for different losses in the different instruments. Differences in instruments should be reflected in LGD estimates. Maturity mismatches between tokenized and non-tokenized assets, and between stablecoins and the traditional assets they reference, need to be captured based on the market risk framework. [SCO60.50 Crypto-asset exposures]

31. If present in a Group 1b crypto-asset, 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. [SCO60.51 Crypto-asset exposures]

Add-on for infrastructure risk for Group 1 crypto-assets

32. The technological infrastructure that underlies crypto-assets, such as DLT, is integral to the asset itself, relatively new, and may pose various additional risks even in cases where the crypto-assets meet the classification conditions of Group 1. This is not the case for traditional financial assets (though information technology and other operational procedures are also important for their transactional and safekeeping administration). Therefore, a 2.5% add-on to RWA will apply to address the emerging nature of the infrastructure on which crypto-assets are based. As industry and market experience with this asset class increases over time, this add-on may be adjusted by OSFI accordingly.

Capital requirements for Group 2

Group 2a

33. For Group 2a crypto-assets the SA will include a separate risk class with its capital requirement determined based on the specifications set out below. [SCO60.66 Crypto-asset exposures]

34. All risk factors, including those related to derivatives and off-balance sheets positions that are affected by changes in Group 2a crypto-asset prices should be included. [SCO60.67 Crypto-asset exposures]

35. Banks should first express each Group 2a crypto-asset position in terms of its quantity, and then convert it at their current spot price into the bank's reporting currency. [SCO60.68 Crypto-asset exposures]

36. The sensitivity between different exposures should be calculated separately for long positions and short positions as gross consolidated values. Some types of hedging and diversification benefits are allowed between instruments referencing the same crypto-asset, including those traded in different markets or exchanges.6 Basis risk resulting from different forms of the same crypto-asset being referenced in a hedging relationship (e.g. crypto ETF positions hedged with futures referencing the underlying exposure) should be captured, tracked, and capitalized by banks. Additionally, only the products listed in Annex 3 may be used for the purposes of offsetting, hedging, and for calculating the net capital set out below. Other products that reference Group 2a crypto-assets are subject to the capital requirements that apply to Group 2b crypto-assets.

37. The computation of the sensitivities-based method for Group 2a crypto-assets includes new specifications of delta, vega, and curvature risk factors. The sensitivity definitions are also extended to include that of Group 2a crypto-assets. Finally, a new bucket structure is introduced, composed of multiple buckets, one for each Group 2a crypto-asset, containing only its respective sensitivity. [SCO60.70 Crypto-asset exposures]

38. **Group 2a crypto-asset delta spot specification**: the sensitivity is measured by changing the Group 2a crypto-asset spot price by 1 percentage point (i.e. 0.01 in relative terms) and dividing the resulting change in the market value of the instrument V_i by 0.01 (i.e. 1%) as follows, where:

    1. k is a given Group 2a crypto-asset;

    2. $CRYPTO(G2a)_k$ is the market value of the Group 2a crypto-asset k; and

    3. V_i is the market value of instrument i as a function of the price of the Group 2a crypto-asset k.

    $$S_k = \left(V_i\left(1.01 \times CRYPTO(G2a)_k\right) - V_i\left(CRYPTO(G2a)_k\right)\right) \div 0.01$$

    [SCO60.71 Crypto-asset exposures]

39. **Group 2a crypto-asset vega specification**: the option-level vega risk sensitivity to a given Group 2a crypto-asset should be determined as prescribed by Chapter 9 of CAR. [SCO60.72 Crypto-asset exposures]

40. **Bucket structure**: the new risk class will comprise "n" buckets, where each bucket corresponds to the aggregate positions in a specific Group 2a crypto-asset.

Table 2: Structure of delta and vega risk weight buckets

Delta crypto-asset buckets and risk weights

Bucket number	Group 2a crypto-asset	Risk weight
1	Crypto-asset X_1	100%
...	...	...
n	Crypto-asset X_n	100%

Vega crypto-asset buckets and risk weights

Bucket number	Group 2a crypto-asset	Risk weight
1	Crypto-asset X_1	100%
...	...	...
n	Crypto-asset X_n	100%

[SCO60.73 Crypto-asset exposures]

41. **Delta (vega) capital requirements**: Delta sensitivities should be determined based on a risk factor structure considering two dimensions:[7]

    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.

[SCO60.74 Crypto-asset exposures]

42. For vega sensitivities, no differentiation by exchange or underlying maturity is considered. Group 2a crypto-asset 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. [SCO60.75 Crypto-asset exposures]

43. In order to calculate the delta (or vega) capital requirements for a single bucket, please use b p kl = 94% [SCO60.76 Crypto-asset exposures]

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

K b = Max (0 , Σ k WS k 2 + Σ k Σ k ≠ 1 p kl WS k WS l

[SCO60.77 Crypto-asset exposures]

45. The delta capital requirement for the Group 2a crypto-asset risk class is Σ b K b , taking into account that there is no recognition of diversification benefits between different Group 2a crypto-assets. [SCO60.78 Crypto-asset exposures]

46. **Curvature capital requirements**: for the curvature risk capital requirement, the delta buckets specified above should be used. The curvature sensitivities should be calculated by shifting all tenors in parallel (i.e. 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 crypto-asset, 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. [SCO60.79 Crypto-asset exposures]

47. For aggregating curvature risk positions within a bucket, the following formula should be used:

K b = max (K b - , K b +) K b - = Σ k | CVR k - | K b + = Σ k | CVR k + |

[SCO60.80 Crypto-asset exposures]

48. Curvature risk cannot be diversified across buckets. The total curvature risk capital across the entire portfolio is Σ b K b . [SCO60.81 Crypto-asset exposures]

49. Group 2a crypto-assets 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 should be treated in line with the minimum risk-based capital requirements for credit risk in CAR. [SCO60.82 Crypto-asset exposures]

Group 2b

50. There is no separate trading book and banking book treatment for Group 2b crypto-assets. This treatment is intended to capture both credit and market risk, including CVA risk. For consistency, the RWA calculated under this approach should be reported as part of the bank's credit RWA. In addition to direct exposures, the regulatory capital and liquidity treatment set out below also applies to:

    1. Funds of Group 2b crypto-assets (e.g. Group 2b crypto-asset ETFs) and other entities, the material value of which is primarily derived from the value of Group 2b crypto-assets.

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

    [SCO60.83 Crypto-asset exposures]

51. For each separate Group 2b crypto-asset to which they are exposed, banks must apply a capital deduction equal to the greater of the absolute value of the aggregate long positions and the absolute value of the aggregate short positions in the crypto-asset. That is, RWA for each separate crypto-asset to which the bank is exposed is calculated as follows:

    CET1 deduction = Max [abs (long exposure) , abs (short exposure)]

    [SCO60.84 Crypto-asset exposures]

52. For each crypto-asset derivative (i.e. a derivative with a Group 2b crypto-asset as the underlying asset), the exposure value used in the above formula is the value of its underlying crypto-assets. For leveraged derivatives (i.e. a derivative that returns a multiple of the value of the underlying), the exposure value of the underlying position should 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 crypto-asset derivative. [SCO60.85 Crypto-asset exposures]

53. The formula also applies a capital deduction to short positions. Banks will be responsible for demonstrating the materiality of these risks under the supervisory review of crypto-assets and whether risks are materially underestimated. In those cases, the capital add-on will be calibrated by requiring banks to calculate aggregate capital requirements under the market risk framework (applying a 100% risk weight for delta, vega, and curvature) and CVA risk framework and to use this amount if the result is higher than the capital deduction above. [SCO60.86 Crypto-asset exposures]

Group 2 exposure limit

54. Banks' exposures to Group 2 crypto-assets are subject to an exposure limit. Banks should apply the exposure limit to their aggregate exposures to Group 2 crypto-assets. [SCO60.116 Crypto-asset exposures]

55. A bank's total gross exposure to Group 2 crypto-assets 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. [SCO60.117 Crypto-asset exposures]

56. Banks must notify OSFI should net short positions approach 1% of Tier 1 capital.

57. Breaches of Group 2 exposure limit should not generally occur and banks should have arrangements in place to ensure adherence with the limit. Any breach that does occur should be communicated immediately to OSFI and should be rapidly rectified. Until adherence with the 1% (gross total exposures) 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 crypto-asset exposures. Finally, if a bank's gross exposures exceed 2% of its Tier 1 capital, all Group 2 crypto-asset exposures will be subject to the capital requirements that apply to Group 2b crypto-asset exposures. [SCO60.118 Crypto-asset exposures]

58. For the purposes of assessing adherence with the Group 2 exposure limit threshold:

    1. Exposures should be measured using the same methodology that applies for determining the Group 2b capital treatment outlined in this guideline. That is, exposures to all Group 2 crypto-assets (both Group 2a and Group 2b) must be measured using the higher of the absolute value of the long and

short exposures in each separate crypto-asset to which the bank is exposed. Derivative exposures should be measured using a delta-equivalent methodology.

2. Tier 1 capital as defined in Chapter 2 of CAR.

[SCO60.119 Crypto-asset exposures]

Capital requirements for credit valuation adjustment risk

59. This section describes how the minimum risk-based capital requirements for CVA risk are to be applied to crypto-asset derivatives exposures and material and fair-valued securities financing transactions (SFTs) referencing crypto-assets, as described in CAR. [SCO60.87 Crypto-asset exposures]

Group 1a

60. Derivatives and SFTs on Group 1a crypto-assets will generally be subject to the same expectations to determine CVA RWA as non-tokenized traditional assets (i.e. the rules set out in the market risk Chapter of CAR). In other words, if a bank holds a derivative or an SFT on a tokenized asset having a price close to the traditional asset and being subject to CVA risk as set out in Chapter 9 of CAR, it will be reflected in the CVA risk charge in the same way as a derivative or SFT on the non- tokenized traditional asset. [SCO60.88 Crypto-asset exposures]

61. Banks should assess the tokenized traditional asset itself against the current expectations set out in CAR. Qualification for a given treatment cannot be derived from the respective traditional (non-tokenized) asset. This requirement of individual assessment includes, but is not limited to, the liquidity characteristics. Different liquidity characteristics between the traditional (non-tokenized) asset and the tokenized 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, (i.e. such tokenized assets are subject to the BA-CVA). [SCO60.89 Crypto-asset exposures]

Group 1b

62. Derivatives of Group 1b crypto-assets will be subject to the same expectations to determine CVA RWA as non-tokenized traditional assets (i.e. the rules set out in the market risk chapter). [SCO60.90 Crypto-asset exposures]

Group 2a

63. Group 2a crypto-assets will be only subject to the expectations set out in Chapter 8 of CAR. BA-CVA must be used for derivatives and SFTs referencing Group 2a crypto-assets. [SCO60.91 Crypto-asset exposures]

Group 2b

64. The treatment of CVA risk for Group 2b crypto-assets is covered above in the Capital requirements Group 2b crypto-assets section. [SCO60.92 Crypto-asset exposures]

Capital requirements for counterparty credit risk

65. For SFTs, banks should apply the comprehensive approach formula set out in the credit risk mitigation section of the SA to credit risk in Chapter 4 of CAR. As noted in earlier, only Group 1a crypto-assets that are tokenized versions of the instruments included on the list of eligible financial collateral may qualify for recognition as eligible collateral. Group 1b, Group 2a and Group 2b crypto-assets are not eligible forms of collateral in the comprehensive approach, and when received by a bank they cannot be recognized under the net exposure calculation for the counterparty collateral. As with all non-eligible collateral, banks that lend Group 1b, Group 2a or Group 2b crypto-assets as part of an SFT must apply the same haircut that is used for equities that are not traded on a recognized exchange (i.e. a haircut of 30%). [SCO60.94 Crypto-asset exposures]

Group 1a

66. Derivatives of Group 1a crypto-assets will generally be subject to the same expectations to calculate CCR as non-tokenized traditional assets, which includes the Internal Models Method (IMM), where the same expectations apply for tokenized assets as for traditional assets. [SCO60.95 Crypto-asset exposures]

67. For the cases described in the CVA risk section of this guideline, especially in presence of significant valuation differences between the traditional and the tokenized 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 crypto-assets. [SCO60.96 Crypto-asset exposures]

Group 1b

68. Derivatives of Group 1b crypto-assets will be subject to the same expectations to determine CCR RWA as non-tokenized traditional assets (i.e. the rules set out in the credit risk standards). [SCO60.97 Crypto-asset exposures]

Group 2a

69. Derivatives of Group 2a crypto-assets will be subject to the SA-CCR (i.e. the rules set out in the credit risk standard), 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 of Group 2a crypto-assets.

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

1. 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.

2. There are separate hedging sets for each cryptocurrency priced in applicable fiat currencies or in another Group 2a cryptocurrency.

3. 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%.

4. The calculation of the adjusted notional will be set to the crypto-asset'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.[8]

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

6. 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.

[SCO60.98 Crypto-asset exposures]

Group 2b

70. For the purpose of calculating counterparty credit risk for derivative exposures that have Group 2b crypto-assets as the underlying or that are priced in units of a Group 2b crypto-asset, the exposure will be the replacement cost (RC) plus the potential future exposure (PFE), both multiplied by the alpha factor specified in CAR, 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 crypto-assets.[9] Netting sets containing both derivatives related to Group 2b crypto-assets and other asset transactions, should be split into two: one containing the derivatives related to crypto-assets; and one

containing derivatives related to the other asset transactions. When calculating the PFE for Group 2b crypto-assets, the 50% of the gross notional amount should be applied per transaction - Group 2b crypto-assets must not form part of any hedging set. [SCO60.99 Crypto-asset exposures]

Capital requirements for operational risk

71. The operational risk resulting from crypto-asset activities should generally be captured by the operational risk standardized approach through the **Business Indicator**. This value should include income and expenses resulting from activities relating to crypto-assets, and through the **Internal Loss Multiplier**, which accounts for operational losses resulting from crypto-asset activities.

Liquidity risk requirements

72. For the LCR and NSFR requirements, crypto-asset exposures, including assets, liabilities and contingent exposures, should generally follow a treatment that is consistent with existing approaches for traditional exposures with economically equivalent risks. At the same time, the treatment should 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 crypto-assets largely relies on the principles and calibrations set forth in the LCR and NSFR (See Chapter 2 and Chapter 3 of LAR). However, guidance requires additional clarification and elaboration to address the novel and unique risks associated with crypto-assets. [SCO60.101 Crypto-asset exposures]

Treatment as high-quality liquid assets (HQLA)

73. Group 1a crypto-assets that are a tokenized version of HQLA as defined in LCR may only be considered as HQLA to the extent both the underlying assets in their traditional form and the tokenized form of the assets satisfy the characteristics of HQLA in LCR.[10] An example of such a Group 1a crypto-asset could be a tokenized bond that meets these HQLA eligibility criteria and temporarily resides on a distributed ledger to facilitate transfer. [SCO60.102 Crypto-asset exposures]

74. Group 1b and Group 2 crypto-assets, by contrast, should not be considered HQLA. [SCO60.103 Crypto-asset exposures]

General considerations for the application of the LCR and NSFR frameworks

75. The appropriate classification and calibration of LCR outflow and inflow rates and NSFR available stable funding (ASF) and required stable funding (RSF) factors of crypto-assets and crypto-liabilities depend on factors such as the structure of the crypto-asset or crypto-liability, its commercial function in practice and the nature of a bank's exposure to the crypto-asset or crypto-liability. [SCO60.104 Crypto-asset exposures]

76. In general, exposures involving Group 1a crypto-assets and crypto-liabilities should be treated the same as exposures involving their equivalent non-tokenized traditional assets and liabilities, including the assignment of inflows, outflows, RSF factors and ASF factors. [SCO60.105 Crypto-asset exposures]

77. As set out below, the LCR and NSFR treatment of exposures involving crypto-assets and crypto-liabilities varies according to whether they are:

    1. tokenized claims on a bank
    2. stablecoins
    3. other crypto-assets

    [SCO60.106 Crypto-asset exposures]

78. **Tokenized claims on a bank**. Group 1a tokenized claims on a bank should 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 should be determined based upon the contractual redemption rights available to the holder.

2. For liabilities from own-issued tokenized claims on a bank:

    1. The bank should 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 LAR.

    2. To the extent the issuing bank can identify, at all times, the holder of the crypto-asset, then the bank should 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 crypto-assets as stable retail deposits. If the issuing bank is unable to identify, at all times, the holder of the crypto-asset, it should treat the liability as unsecured wholesale funding provided by **other legal entity customers**.

    3. Tokenized 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 should follow the categorization methodology in LCR para 73-83. These liabilities are not eligible for the lower outflow rate specified in LCR para 84.

3. When a bank holds another bank's issuance of such a tokenized liability:

    1. The holder should not recognize inflows in the LCR if the crypto-asset is not redeemable within 30 days.

    2. The holder should not recognize inflows in the LCR and should assign a minimum RSF factor of 50% in the NSFR if the crypto-asset is held for operational purposes, in alignment with LAR. The holder may recognize inflows in the LCR and an RSF factor of 15% in the NSFR if the crypto-asset is not held for operational purposes.

4. Notwithstanding the clarifications above, supervisors should apply more stringent LCR and NSFR treatment if, having considered the features and liquidity risk profiles of a tokenized claim on a bank, they conclude that there may be additional liquidity risk inherent in a given liability (e.g. if some

characteristics of the crypto-asset 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 (e.g. reliance on non-regulated entities as wallet providers or third-party blockchain operators and usage characteristics of stablecoins, etc.) and the local circumstances of the banking sector.

[SCO60.107 Crypto-asset exposures]

79. **Value-referenced crypto-assets and other stablecoins**. Group 1b crypto-assets, and certain Group 2 crypto-assets that are fully collateralized by a segregated pool of underlying assets that do not count toward the bank's stock of HQLA, should be treated similar to securities, subject to the following considerations:[11]

    1. When a bank is an issuer of a stablecoin and the asset issuance represents a legally binding claim on the bank:

        1. The issuing bank should recognize 100% outflows in the LCR if the stablecoin crypto-asset is redeemable within 30 days. The issuing bank must assign an ASF factor in accordance with the NSFR based upon the earliest date upon which the asset could be redeemed.

        2. The issuing bank may recognize reduced outflows in the LCR to the extent the stablecoin crypto-asset 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 asset. The reduction in outflows should incorporate the haircuts specified in LCR and should not result in net inflows.

        3. The assets segregated to support the value of the stablecoin should be assigned a minimum RSF factor for encumbered assets as specified in NSFR based upon the earliest date upon which the asset could be redeemed.

    2. When a bank holds a stablecoin on its balance sheet:

1. As non-HQLA these assets should be subject to at least an 85% RSF in the NSFR and not result in inflows under the LCR.

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

[SCO60.108 Crypto-asset exposures]

80. **Other crypto-assets**. The treatment of Group 2 crypto-assets that do not qualify for the treatment outlined above should 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 crypto-assets or loans denominated in these assets on its balance sheet should assign 100% RSF to the carrying value of these assets in the NSFR and must not recognize any inflows associated with the liquidation, redemption, or maturity of these assets.

    2. A bank that has borrowed other Group 2 crypto-assets on an unsecured basis and has an obligation to return these assets within 30 days should apply a 100% outflow rate against the market value of the asset that should 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 crypto-asset. Similarly, borrowings denominated in other Group 2 crypto-assets must be assigned 0% ASF in the NSFR.

    [SCO60.109 Crypto-asset exposures]

81. OSFI may 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 crypto-assets, 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 signaling effects. [SCO60.110 Crypto-asset exposures]

82. These treatments outlined 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 crypto-asset
    2. Secured funding and lending of fiat currency with crypto-assets as collateral
    3. Collateral swaps involving crypto-assets
    4. Commitments to lend crypto-assets

    [SCO60.111 Crypto-asset exposures]

83. For the transactions listed above, the treatment should align with the existing framework, which generally applies consistently for all non-HQLA instruments. [SCO60.112 Crypto-asset exposures]

Leverage ratio requirements

84. Consistent with the leverage ratio guidance, crypto-assets 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 crypto-asset exposure is an off-balance sheet item, a conversion factor of 100% in the leverage ratio framework will apply in calculating the exposure measure (e.g. see paragraph 75 of the Leverage Requirements Guideline). Exposures for crypto-asset derivatives should follow the treatment prescribed in the derivative exposures section of the Leverage Requirements Guideline. [SCO60.113 Crypto-asset exposures]

85. For Group 1b crypto-assets, if the bank is involved in the crypto-asset network as a member who is able to deal directly with the redeemer and has promised to purchase crypto-assets from non-member holders, the member also needs to include the total current value of all the off-balance sheet crypto-assets that the bank could be obliged to purchase from holders (as set out in the Leverage Requirements guideline). [SCO60.114 Crypto-asset exposures]

Large exposures requirements

86. For large exposures purposes, the treatment for crypto-assets will follow the same principles as for other exposures as set out in the B-2 Large Exposure Limits guidelines. Consistent with those expectations, crypto-asset exposures that give rise to a credit risk exposure are included in the large exposure measure according to their accounting value. The bank should 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 crypto-asset exposes the bank to the risk of default of more than one counterparty, the bank should compute for each counterparty the respective amount to which it is exposed to default risk for large exposure purposes. When the crypto-asset 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 expectations applicable to transactions with underlying asset. Crypto-assets that do not expose banks to default risk (such as physical exposures of gold, other commodities or currencies, and exposures of some forms of crypto-assets with no issuer) do not give rise to a large exposures requirement; however, the counterparty credit risk exposures arising from derivative contracts that reference crypto-assets with no issuer will fall in the scope of the large exposure requirement. [SCO60.115 Crypto-asset exposures].

Foreign bank branch deposit requirement

87. Crypto-asset exposures should not be considered qualifying assets under Guideline A-10, and therefore cannot be included in the calculation of the foreign bank branch deposit.

Bank risk management

88. Crypto-asset exposures and activities introduce novel risks and increase certain traditional risks. Annex 4 sets out banks risk management guidance with respect to crypto-asset exposures.

Annex 1: Classification conditions

Classification condition 1

- 1.1 The crypto-asset is either: (i) a tokenized traditional asset; or (ii) has a stabilization mechanism that is effective at all times in linking its value to a traditional asset or a pool of traditional assets (i.e. stablecoins). [SCO60.8 Crypto-asset exposures]
- 1.2 Tokenized traditional assets will only meet classification condition 1 if they satisfy all of the following expectations:

    1. They are digital representations of traditional assets using cryptography and DLT, or similar technology to record ownership.
    2. They pose the same level of credit and market risk as the traditional (non-tokenized) form of the asset. In practice, this means the following for tokenized traditional assets:

        1. **Bonds, loans, claims on banks (including in the form of deposits, equities and derivatives)**. 12 The crypto-asset must confer the same level of legal rights as ownership of these traditional forms of financing (e.g. rights to cash flows, claims in insolvency). In addition, there should be no feature of the crypto-asset that could prevent obligations to the bank being paid in full when due as compared with a traditional (non-tokenized) version of the asset.
        2. **Commodities**. The crypto-asset should confer the same level of legal rights as traditional account-based records of ownership of a physical commodity.
        3. **Cash held in custody**. The crypto-assets should confer the same level of legal rights as cash held in custody.

    [SCO60.9 Crypto-asset exposures]

- 1.3 Crypto-assets do not meet the condition set out 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.

[SCO60.10 Crypto-asset exposures]

- 1.4 Crypto-assets that have a stabilization mechanism will only meet classification condition 1 if they satisfy all of the following expectations:

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

2. The stabilization mechanism is designed to minimize fluctuations in the market value of the crypto-assets relative to the peg value. In order to satisfy the "effective at all times" condition, banks should have a monitoring framework in place verifying that the stabilization mechanism is functioning as intended.

3. The stabilization mechanism enables risk management similar to the risk management of traditional assets, based on sufficient data or experience. For newly established crypto-assets, there may be insufficient data and/or practical experience to perform a detailed assessment of the stabilization mechanism. Evidence should be provided to satisfy supervisors of the effectiveness of the stabilization 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 crypto-asset is dependent. In the case of underlying physical assets, banks should verify that these assets are stored and managed appropriately. This monitoring

framework should function regardless of the crypto-asset 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 crypto-asset passes the redemption risk test set out below 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 crypto-assets with stabilization mechanisms to meet a "basis risk test," but as yet has chosen not to implement this test.13 OSFI 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.

[SCO60.11 Crypto-asset exposures]

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

1. **Value and composition of reserve assets**. The value of the reserve assets (net all non-crypto-asset claims on these assets) should at all times, including during periods of extreme stress, equal or exceed the aggregate peg value of all outstanding crypto-assets. If the reserve assets expose the holder to risk in addition to the risks arising from the reference assets, the value of the reserve assets should sufficiently overcollateralize the redemption rights of all outstanding crypto-assets.14 The level of overcollateralization should 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 crypto-assets.

2. **Asset quality criteria for reserve assets**. For crypto-assets that are pegged to one or more currencies, the reserve assets should 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 LAR. 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 crypto-asset 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 should be comprehensive and transparent. They must ensure that:

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

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

    3. A mandate that describes the types of assets that may be included in the reserve should be publicly disclosed and kept up to date.

    4. The composition and value of the reserve assets are publicly disclosed on a regular basis. The value should be disclosed at least daily and the composition should be disclosed at least weekly.

    5. 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.

[SCO60.12 Crypto-asset exposures]

- 1.6 Stabilization mechanisms that: (i) reference other crypto-assets as underlying assets (including those that reference other crypto-assets that have traditional assets as underlying); or (ii) use protocols to increase or decrease the supply of the crypto-asset do not meet classification condition 1.15 [SCO60.13 Crypto-asset exposures]

Classification condition 2

- 1.7**Classification condition 2**: All rights, obligations and interests arising from the crypto-asset 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 crypto-asset arrangement to ensure this condition is met, and make the review available to their lead supervisors upon request. [SCO60.14 Crypto-asset exposures]
- 1.8 To meet classification condition 2, the following expectations should be met:

    1. At all times the crypto-asset arrangements should ensure full transferability and settlement finality. In addition, crypto-assets with stabilization mechanisms should provide a robust legal claim against the issuer and/or underlying reserve assets and should ensure full redeemability (i.e. the ability to exchange crypto-assets 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 crypto-asset arrangement to be considered as having full redeemability, it should allow for the redemption to be completed within 5 calendar days of the redemption request at all times.

    2. At all times the crypto-asset arrangements are properly documented. For crypto-assets with stabilization mechanisms, crypto-asset arrangements should clearly define which parties have the right to redeem; the obligation of the redeemer to fulfill 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 should also be valid in instances where parties involved in these arrangements may not be located in the same jurisdiction where the crypto-asset is issued and redeemed. At all times, settlement finality in crypto-asset arrangements should 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 should be publicly disclosed by the crypto-asset issuer. If the offering of the crypto-asset to the public has been approved by the relevant regulator on the basis of this public disclosure, this

condition will be considered fulfilled. Otherwise, an independent legal opinion would be needed to confirm this condition has been met.

[SCO60.15 Crypto-asset exposures]

Classification condition 3

- 1.9**Classification condition 3**: The functions of the crypto-asset 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. [SCO60.16 Crypto-asset exposures]
- 1.10 To meet classification condition 3, the following expectations must be met:

    1. The functions of the crypto-asset, such as issuance, validation, redemption and transfer of the crypto-assets, 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 crypto-asset. To this end, entities performing activities associated with these functions should 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 (i.e. operational reliability and capacity); third-party risk management; and Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT).16
    2. All key elements of the network should be well-defined such that all transactions and participants are traceable. Key elements include: (i) the operational structure (i.e. whether there is one or multiple entities that perform core function(s) of the network); (ii) degree of access (i.e. 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 (i.e. whether validation of a transaction is conducted with single or multiple entities).

    [SCO60.17 Crypto-asset exposures]

Classification condition 4

- 1.11**Classification condition 4**: Entities that execute redemptions, transfers, storage or settlement finality of the crypto-asset, or manage or invest reserve assets, must: (i) be regulated and supervised, or subject to appropriate risk management standards; and (ii) have in place and disclose a comprehensive governance framework. [SCO60.18 Crypto-asset exposures]

- 1.12 Entities subject to condition 4 include operators of the transfer and settlement systems for the crypto-asset, wallet providers and, for crypto-assets with stabilization mechanisms, administrators of the stabilization 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. [SCO60.19 Crypto-asset exposures]

Annex 2: Examples of credit risk and capital requirements associated with Group 1b crypto-assets

- 2.1**Risk from reference asset**: If the reference asset for a Group 1b crypto-asset gives rise to credit risk (e.g. a bond), banks may suffer a loss from the default of the reference asset's issuer. Banks should therefore include in credit RWA the RWA that would apply under CAR to a direct holding of the reference asset. If the reference asset gives rise to foreign currencies or commodities risk (e.g. 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 Chapter 9 of CAR to a direct holding of the underlying traditional asset. [SCO60.32 Crypto-asset exposures]

- 2.2 For Group 1b crypto-assets that reference a pool of traditional assets, banks should apply the expectations applicable to equity investments in funds (to determine the RWA applicable for a direct holding of the referenced pool of traditional assets, as required above. The look-through approach and the mandate-based approach of CAR are available for crypto-assets that fulfill all expectations for these approaches. Otherwise, the simplified approach (i.e. a capital deduction) must be applied. [SCO60.33 Crypto-asset

exposures]

- 2.3**Risk of default of the redeemer**. Group 1b crypto-assets must be redeemable and if the entity that performs the redemption function (the "redeemer") fails, the crypto-assets may become worthless. The capital treatment of banks' exposures to the redeemer depends on the nature of the exposures:17

    1. If the bank holding the crypto-asset has an unsecured claim on the redeemer in case of default, the bank should calculate credit RWA for its exposure to the redeemer. The credit RWA in this case should be equal to the RWA that would apply to a direct unsecured loan to the redeemer. For this purpose, the loan amount should equal the redemption claim (i.e. peg value) of the crypto-asset.

    2. If the bank holding the crypto-asset has a secured claim on the redeemer in case of default, the bank should calculate credit RWA for its exposure to the redeemer. The credit RWA in this case should equal to the RWA that would apply 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 (i.e. peg value) of the crypto-asset. All conditions on the eligibility of collateral for the purposes of recognising credit risk mitigation set out in CAR apply.

  [SCO60.34 Crypto-asset exposures]

- 2.4 Certain Group 1b crypto-assets may be structured to avoid the crypto-asset 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 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 crypto-assets 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 recognize underlying assets held in a bankruptcy remote manner as those of the crypto-asset holder.

  [SCO60.35 Crypto-asset exposures]

- 2.5**Risks arising when intermediaries perform the redemption function**. Group 1b crypto-assets may be structured such that only a subset of holders ("members") are allowed to transact directly with the redeemer to redeem the crypto-asset. Holders that cannot transact directly with the redeemer ("non-member holders") are therefore reliant on the members for the crypto-assets 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 crypto-assets from non-member holders at a price equal to the reference asset(s).

    2. The members may not make a commitment, but may be incentivized to purchase the crypto-assets 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).

  [SCO60.36 Crypto-asset exposures]

- 2.6 Banks that are members of crypto-asset arrangements as described above ("member banks"), must calculate risk weighted assets for their own crypto-asset holdings in the same way as required for holders in crypto-assets arrangements in which all holders can deal directly with the redeemer (i.e. as set out above). In addition, member banks may be exposed to the risk that the redeemer fails and they are committed to purchase crypto-assets from non-member holders. In such cases, a member bank should also include the RWA that would apply if the bank held all of the crypto-assets that it could be obliged to purchase. Even if there is no legal obligation for a member bank to purchase crypto-assets from non-member holders, banks and supervisors should 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 should 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 lead supervisor that such step-in risk does not exist. [SCO60.37 Crypto-asset exposures]

- 2.7 The risks to bank holders of crypto-assets that cannot deal directly with the redeemer (i.e. non- member holders) depend on whether the members have committed to purchase crypto-assets from all non-member

holders in unlimited amounts (i.e. they have made a standing and irrevocable offer to purchase all outstanding crypto-assets from non-member holders):

1. If members have committed to buy crypto-assets 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 crypto-assets. When banks are non-member holders they must sum the RWA calculated for the two risks. The first risk should be calculated as the RWA that would arise from a direct exposure to the underlying. 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 crypto-assets (i.e. the holder can choose whether to sell the crypto-asset to any one of a number of members). If there is just one member, the RWA should be calculated as the crypto-asset 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 should be the risk weight that would be applicable to an unsecured loan to the member with the highest credit rating (i.e. lowest risk weight).18

2. If members have not committed to purchase crypto-assets 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 crypto-assets; and (iii) the risk that the redeemer defaults (because if it failed, the members would no longer have the incentive to purchase the crypto-assets from the non-member holders). In such cases, the non-member bank holder should 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 the paragraph above. The RWA for the third risk must be calculated as the RWA that would arise from a direct loan to the redeemer.

[SCO60.38 Crypto-asset exposures]

- 2.8 Group 1b crypto-assets, 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. [SCO60.39 Crypto-asset exposures]

Annex 3: Group 2a hedging recognition criteria

- 3.1 Institutions which do not adhere to the market risk framework in Chapter 9 of CAR should categorize all Group 2 crypto-asset exposures as Group 2b.
- 3.2 Group 2 crypto-assets that meet all three of the following hedging recognition criteria and where a bank adheres to the market risk framework in Chapter 9 of CAR, may be classified as Group 2a:

    1. The bank's crypto-asset exposure is one of the following:

        1. A direct holding of a spot Group 2 crypto-asset 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 crypto-asset.
        2. A derivative or ETF/ETN that references a Group 2 crypto-asset, 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).
        3. A derivative or ETF/ETN that references a derivative or ETF/ETN that meets criterion (b) above.
        4. A derivative or ETF/ETN that references a crypto-asset-related reference rate published by a regulated exchange.

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

        1. The average market capitalization was at least $10 billion over the previous year.

2. The 10% trimmed mean of daily trading volume with major fiat currencies is at least $50 million over the previous year.

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

    1. There are at least 100 price observations over the previous year. The price observations should be "real" as defined in the criteria of Chapter 9 of CAR.

    2. There are sufficient data on trading volumes and market capitalization.

[SCO60.55 Crypto-asset exposures]

- 3.3 The capital requirements for Group 2a crypto-assets can be calculated according to a modified version of the SA in the market risk standard set out in this guideline. [SCO60.56 Crypto-asset exposures]

Annex 4: Bank risk management

- 4.1 Crypto-asset 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 crypto-asset should 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 crypto-assets or related activities on an ongoing basis. The policies and procedures followed by banks for crypto-asset activities should be informed by existing OSFI guidance on operational risk. In accordance with these policies and procedures, banks' operational risk management practices should include, but are not limited to, conducting assessments of these risks (i.e. how material these risks are, and how they are managed) and taking relevant mitigation measures to improve their operational resilience capabilities (specifically regarding information and communication technology (ICT) and cyber risks). The decision to hold crypto-assets (either under trading or banking book) and provide services to crypto-asset operators should 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. [SCO60.121 Crypto-asset exposures]

- 4.2 Considering the particular features of crypto-assets 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 should conduct ex-ante a prudent assessment of any crypto-asset exposures they intend to take on and verify the adequateness of existing processes and procedures. The bank should have a sound risk management approach for managing the risks of crypto-assets, including limits and hedging strategies, together with clearly assigned responsibilities for the management of these risks. [SCO60.122 Crypto-asset exposures]

- 4.3 Banks should also inform OSFI of their policies and procedures, assessment results, as well as their actual and planned crypto-asset 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. [SCO60.123 Crypto-asset exposures]

- 4.4 The mapping of risks relating to crypto-asset activities to the risk categories depends on how these risks manifest. Many of the risks introduced or increased by crypto-asset activities are covered by the operational risk framework. A mapping of the technological risks of crypto-assets 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 crypto-assets, 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 (e.g. loss of a private cryptographic key by the bank), such losses would be operational losses. [SCO60.124 Crypto-asset exposures]

- 4.5 Risks that banks need to consider in their risk management of crypto-assets activities include, but are not limited to, the following:

1. **Crypto-asset technology risk**: Banks should closely monitor the risks inherent to the supporting technology, whether crypto-asset activities are conducted directly or through third parties, including but not limited to:

    1. **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 crypto-assets (e.g. so-called "forks" that change the underlying "rules" of a protocol). In addition, the type of consensus mechanism (i.e. 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."

    2. **Validating design of the DLT, permissionless or permissioned**: Crypto-assets 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.

    3. **Service accessibility**: One of the distinguishing features of crypto-assets is its accessibility to holders of these assets. A holder of crypto-assets is assigned a set of unique cryptographic keys, which allow that party to transfer the crypto-assets to another party. If those keys are lost, a

holder will generally be unable to access the crypto-assets. This increases the possibility of fraudulent activities such as a third-party gaining access to cryptographic keys and using the keys to transfer the crypto-asset to themselves or another unauthorized entity. Furthermore, the risk of a large-scale cyber-attack could leave banks' customers unable to access or recover crypto-asset funds.

4. **Trustworthiness of node operators and operator diversity**: Since the underlying technology and node operators facilitate the transfer of crypto-assets 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 (e.g. whether the nodes are run by public/private institutions or individuals) are relevant considerations in third-party risk management.

2. **General information and communication technology (ICT) and cyber risks**: A bank holding crypto-assets 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 unauthorized transfers of crypto-assets.

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

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

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

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

4. **Uncertain legal status**: Jurisdictions can decide (and have decided) to ban crypto-asset 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 crypto-assets pose valuation challenges, due (among other things) to their volatility and variable pricing on different exchanges, particularly given that most of the crypto-assets 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.

[SCO60.125 Crypto-asset exposures]

- 4.6 OSFI may impose additional capital charges on 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 crypto-assets is considered inadequate. OSFI may request banks to provision for losses related to crypto-assets where such losses are foreseeable and estimable. Finally, OSFI 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. [SCO60.126 Crypto-asset exposures]

1 For the purposes of this guideline, the term bank(s) may be used in lieu of federally regulated deposit-taking institution(s), including federal credit union(s). Crypto-asset exposures at foreign bank branch deposits will not be considered qualifying assets.

2 This definition is aligned to the scope and definitions paragraph SCO60.1 of "BCBS prudential treatment of cryptoasset exposures" published by the Basel Committee on Banking Supervision (BCBS) on December 16, 2022. Where paragraphs in the remainder of this document align to this BCBS document, they are similarly followed by square brackets commencing with SCO and a number indicating the reference paragraph within the BCBS document.

3 This includes both direct holdings (cash and derivatives) and indirect holdings (e.g. those via investment funds, ETF/ETN, or any legal arrangements designed to provide exposures to crypto-assets).

4 See par. 72-75 for applicable liquidity treatment.

5 Based on the Financial Stability Board's definition of a stablecoin.

6 OSFI notification is required for exposures in foreign exchanges and jurisdictions.

7 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.

8 If pairs to the domestic currency are not liquidly traded, the most liquid fiat currency needs to be taken with foreign exchange spot rates against the domestic fiat currency.

9 The replacement cost is subject to a floor of zero.

10 Note that to be considered in the LCR's stock of HQLA, these assets should also satisfy the operational requirements in the LCR.

That do not qualify as Group 1b crypto-assets due to redemption restrictions (i.e. 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

11 at all times.

12 Bank-issued tokenized 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. 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 name.

13 For a description of the basis risk test, see the Basel Committee on Banking Supervision's Second Consultation on the prudential treatment of cryptoasset exposures. Please note this test may change in the near future.

14 For example, consider a crypto-asset that is redeemable for a given currency amount (i.e. the currency amount is the reference asset) but is backed by bonds denominated in the same currency (i.e. 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.

15 Crypto-assets that use protocols to maintain their value are in some cases referred to as "algorithm-based stablecoins".

16 Example of these entities include, but are not limited to: issuers, operators of the transfer and settlement systems for the crypto-asset; administrators of the crypto-asset stabilization mechanism and custodians of any underlying assets supporting the stabilization mechanism.

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

18 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.