Draft guideline

Title OSFI guideline on the regulatory capital treatment of crypto-asset exposures (Insurance) – 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 treatment of crypto-assets sets out the Office of the Superintendent of Financial Institution's (OSFI) expectations for reporting insurers' 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.

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.

4. The regulatory capital treatment of central bank digital currencies (CBDCs) is not included in the scope of this guideline.

5. For the purposes of this guideline, the term "exposure" includes on or off-balance sheet amounts that give rise to credit, market, operational or liquidity risks.2 The operational risk requirements, as well as the risk management section, are also applicable to insurers' crypto-asset activities, that do not generally give rise to credit or market requirements.

Simplified and comprehensive capital treatment options

6. **Simplified approach** - A simplified capital treatment approach is available to insurers with limited crypto-asset exposures, or to insurers wishing to streamline or bypass classification determination detailed in the sections that follow. These insurers should deduct all their crypto-asset exposures from Gross Tier 1 or capital available (i.e. treat all their crypto-asset exposures as Group 2 exposures).

7. **Comprehensive approach** - Insurers 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 insurers, whether applying the simplified or comprehensive approach, must consider operational risk, large exposure risk, and foreign insurance branch requirements. Dedicated sections in this document provide guidance to insurers on each of these areas with respect to their crypto-asset exposures.

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

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

Simplified approach	Comprehensive approach
○ Deduct all crypto-asset exposures from Gross Tier 1 or capital available	○ Capital treatment varies depending on crypto-asset classification (i.e. Group 1a, 1b, 2a or 2b)
Other considerations include operational risk, large exposures, and foreign insurance branch requirements	

Categorization of crypto-assets

10. For the purposes of credit and market risk, the capital treatment of an insurer'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 be 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.

        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.[3]

    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 consists 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.[4]

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.

11. Figure 1 below summarizes the categorization of crypto-assets and their capital treatment. The capital requirements for crypto-asset exposures should be consistent with the requirements in the Life Insurance Capital Adequacy Test (LICAT), the Minimum Capital Test (MCT), and the Mortgage Insurer Capital Adequacy Test (MICAT), unless stated otherwise in this guideline.

Figure 1: Different categorizations of crypto-assets

Group 1

- **1a: Tokenized crypto-assets**
  - Consistent with the LICAT, MCT and MICAT treatment of the related assets
- **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 Gross Tier 1 or capital available

12. Insurers, 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. Insurers should fully document

the information used in determining compliance with the classification conditions and make this available to OSFI upon request. OSFI may override insurers' classification decisions if it does not agree with the assessments undertaken by insurers.

Accounting classification

13. Crypto-asset exposures are not subject to the deduction requirement that applies to intangible assets set out in Chapter 2 of the LICAT, MCT, and MICAT including in cases where the crypto-asset is classified as an intangible asset under IFRS.

Capital treatment for Group 1 crypto-assets

14. No adjustments are required to Available Capital under the LICAT and capital available under the MCT and MICAT for Group 1 crypto-assets.

Capital requirement for credit risk for Group 1 crypto-assets

15. This section describes how capital requirements for credit risk are to be applied to 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.

Group 1a crypto-assets (tokenized traditional assets)

16. Group 1a crypto-assets will generally be subject to the same expectations to determine credit risk capital requirements as non-tokenized traditional assets. For example, a tokenized corporate bond will be subject to the same risk factor as the non-tokenized corporate bond.

17. 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. Insurers 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.

18. Chapter 3 of the LICAT for life insurers, Chapter 6 of the MCT for property and casualty (P&C) insurers, and Chapter 4 of the MICAT for mortgage insurers sets out the list of eligible forms of financial collateral for the purposes of recognition as a credit risk mitigant.[5] Only Group 1a crypto-assets that are tokenized versions of the instruments included on the list of eligible financial collateral set out in the LICAT, MCT or MICAT may qualify for recognition as eligible collateral (subject to also meeting the expectations described in this section).

19. 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 set out in the LICAT, MCT, or MICAT. 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, insurers should separately assess whether they comply with the relevant eligibility requirements for collateral recognition, including 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, insurers should analyze the period of time 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 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.

Group 1b crypto-assets (crypto-assets with stabilization mechanisms)

20. 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. Insurers that have 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 insurers using the credit risk standards set out in the LICAT, MCT, or MICAT. For examples of this treatment, please refer to Annex 2. That list is not exhaustive, and it is the responsibility of insurers to comprehensively assess and document the full range of risks arising from each of its exposures.

Derivatives

21. Derivatives of Group 1a or Group 1b crypto-assets will generally be subject to the same rules as non-tokenized traditional assets, subject to the considerations in this credit risk section.

Collateral

22. 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 crypto-assets are not eligible forms of collateral and therefore when insurers 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, life insurers that lend Group 1b crypto-assets as part of a securities financing transaction (SFT) must apply the same haircut to the exposure that is used for equities that are traded on a recognized exchange but not part of a main index.6 P&C and mortgage insurers that lend Group 1b crypto-assets as part of an SFT will receive no recognition for the purposes of the net exposure calculation to the counterparty.

Capital requirement for market risk for Group 1 crypto-assets

23. Group 1a crypto-assets will generally be subject to the same rules to determine market risk capital requirements as non-tokenized traditional assets, which are set out in the market risk chapter of the LICAT, MCT, and MICAT.

24. Group 1 crypto-assets should account for the current risk classes (e.g. interest rate, equity, real estate, domestic and foreign currency, etc.) set out in the market risk chapter of the LICAT, MCT, or MICAT. Specifically:

    1. Each tokenized instrument in Group 1 should account for the same risk factors as the traditional asset it digitally represents.

    2. Each stablecoin in Group 1 should account for the same risk factors as the traditional asset(s) that it references.

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 capital requirements for credit risk in the LICAT, MCT or MICAT.

26. Long positions in Group 1 crypto-assets may be offset with short positions in the same crypto-asset to reduce the risk exposure.

Capital requirements for operational risk for Group 1 crypto-assets

27. The operational risk resulting from crypto-asset activities should generally be captured by the operational risk approach in the LICAT, MCT, and MICAT.

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

28. 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 should be applied to the risk factor, which is determined by summing the various risks calculated as if the insurer held the equivalent traditional asset, 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 treatment for Group 2 crypto-assets

29. For the purposes of the capital framework, insurers should fully deduct Group 2 crypto-assets from the insurer's Gross Tier 1 under the LICAT, and capital available under the MCT and MICAT. Assets that are deducted from Available Capital under the LICAT and capital available under the MCT and MICAT will be subject to a 0% risk factor for capital required purposes.

Group 2a crypto-assets

30. Insurers 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 insurer's reporting currency.

31. Long positions in Group 2a crypto-assets may be offset with short positions in the same crypto-asset to reduce the risk exposure.

32. 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.[7] 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 insurers. Additionally, only the products listed in Annex 3 may be used for the purposes of offsetting and hedging. Other products that reference Group 2a crypto-assets are subject to the capital treatment that apply to Group 2b crypto-assets.

Group 2b crypto-assets

33. In addition to direct exposures, the capital treatment set out above 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.

Derivatives

34. Derivatives of Group 2a crypto-assets will be subject to the treatment of derivatives in LICAT, MCT and MICAT, 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 credit exposure (PFE) add-on, a new asset class "crypto" will be created.

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

        2. The calculation of the adjusted notional will be set to the crypto-asset's notional expressed in the domestic fiat currency of each insurer. For the case of a cryptocurrency priced in another cryptocurrency, the larger of the two adjusted notionals will apply.[8]

        3. 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.

35. For the purpose of determining the Group 2 exposure limit 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), 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. 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.

Collateral

36. Group 2a and Group 2b crypto-assets are not eligible forms of collateral, and when received by an insurer, they cannot be recognized under the net exposure calculation for the counterparty collateral. As with all non-eligible collateral, life insurers that lend Group 2a or Group 2b crypto-assets as part of an SFT must apply the same haircut to the exposure that is used for equities that are traded on a recognized exchange but not part of a main index. P&C and mortgage insurers that lend Group 2a or Group 2b crypto-assets as part of an SFT will receive no recognition for the purposes of the net exposure calculation to the counterparty.

37. Collateral used as a financial resource to reduce capital requirements cannot include Group 2a or 2b crypto-asset exposures (e.g. earthquake reserve and collateral used for unregistered reinsurance).

Group 2 exposure limit

38. Insurers' exposures to Group 2 crypto-assets will be subject to an exposure limit. Insurers should apply the exposure limit to their aggregate Group 2 exposures.

39. An insurer's total gross exposure to Group 2 crypto-assets should not generally be higher than 1% of the insurer's Gross Tier 1 capital (for life insurers) or capital available (for P&C and mortgage insurers) and must not exceed 2% of Gross Tier 1 capital or capital available.

40. Insurers must notify OSFI should net short positions approach 1% of Tier 1 capital.

41. Breaches of the Group 2 exposure limit should not generally occur and insurers 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 insurer'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 an insurer's gross exposures exceed 2% of its Gross Tier 1 capital (for life insurers) or capital available (for P&C and mortgage insurers), all Group 2 crypto-asset exposures will be subject to the capital requirements that apply to Group 2b crypto-asset exposures.

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

    1. 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 insurer is exposed. Derivative exposures should be measured using the delta equivalent value of the hedged positions.

    2. Gross Tier 1 capital and capital available are defined in Chapter 2 of the LICAT, MCT and MICAT respectively.

43. For client products with characteristics that increase the insurer's risk exposure to more than 100% of the investment, the increase in exposure is considered entirely attributable to crypto-assets, even for partial exposures, and should be deducted in the same manner as the base exposure (i.e. a 100% deduction of exposure from Gross Tier 1 capital for life insurers and capital available for P&C and mortgage insurers).

    Example: Minimum guarantee for a savings contract

    The insurer provides a client with a $100 savings contract, invested entirely in crypto-assets, with a minimum guaranteed return of 3% over the term of the contract. The deduction would be

$103 (i.e. $100 × (100% + 3%)).

Example: Reset option for a segregated fund contract

The insurer provides a client with a $100 segregated fund contract, invested 25% in crypto-assets and 75% in stocks, with reset. The reset option has been exercised and the guaranteed value of the contract has increased to $120. The deduction in connection with crypto-assets would be $45 (i.e. the base amount of $100 × 25% + the guarantee amount of $20).

Large exposures requirements

44. 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 for life, P&C, and mortgage insurers. 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 insurer should identify and apply the large exposure limits to each specific counterparty or group of connected counterparties to which it is exposed. Where the crypto-asset exposes the insurer to the risk of default of more than one counterparty, the insurer 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 insurer must follow the existing large exposures rules applicable to transactions with underlying assets. Crypto-assets that do not expose insurers 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 credit risk exposures to counterparties arising from derivative contracts that reference crypto-assets with no issuer will fall in the scope of the large exposure requirement.

Foreign insurance branch requirements

45. Foreign insurance branches are not permitted to vest crypto-asset exposures.

Insurer risk management

46. Crypto-asset exposures and activities introduce novel risks and increase certain traditional risks. Annex 4 sets out insurer 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).
- 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 insurers (including in the form of equities and derivatives)**.[9] 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, etc.). In addition, there should be no feature of the crypto-asset that could prevent obligations to the insurer 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.

- 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 credit risks to a counterparty relative to traditional assets.

- 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, insurers 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 insurers 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, insurers should verify that these assets are stored and managed appropriately. This monitoring framework should function regardless of the crypto-asset issuer. Insurers 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.

- 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 insurer 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.10 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. 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.

- 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.[11]

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. Insurers 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.

- 1.8 To meet classification condition 2, the following requirements 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.

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.

- 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).12

    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 unrestricted); (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).

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.

- 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.

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), insurers may suffer a loss from the default of the reference asset's issuer. Insurers should therefore include the credit risk factor that would apply under the LICAT, MCT, or MICAT to a direct holding of the reference asset. If the reference asset gives rise to foreign exchange or commodities risk (e.g. foreign currency denominated financial assets or physical commodities), insurers must apply the same market risk treatment for the exposure as the market risk treatment that would apply under the LICAT, MCT and MICAT to a direct holding of the underlying traditional asset.

- 2.2 For Group 1b crypto-assets that reference a pool of traditional assets, insurers should apply the expectations applicable to equity investments in funds (to determine the risk factor applicable for a direct holding of the referenced pool of traditional assets), as required above.

- 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 insurers' exposures to the redeemer depends on the nature of the exposures:

    1. If the insurer holding the crypto-asset has an unsecured claim on the redeemer in case of default, the insurer should apply the credit risk factor for its exposure to the redeemer. The credit risk factor in this case should include the risk factor that would apply to the credit rating or the exposure to the

redeemer, as applicable under the LICAT, MCT, and MICAT. For this purpose, the exposure should equal the redemption claim (i.e. peg value) of the crypto-asset.

2. If the insurer holding the crypto-asset has a secured claim on the redeemer in case of default, the insurer should account for the credit risk factor for its exposure to the redeemer. The credit risk factor in this case should include the risk factor that would apply to the credit rating or the exposure to the redeemer, as applicable under the LICAT, MCT, and MICAT. For this purpose, the exposure, 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 recognizing credit risk mitigation set out in the LICAT, MCT and MICAT apply.

- 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. Insurers are not required to calculate the risk factor 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 insurer 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.

- 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).

- 2.6 Insurers that are members of crypto-asset arrangements as described above ("member insurers"), must determine risk factors 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 insurers 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 insurer should also include the risk factor that would apply if the insurer held all of the crypto-assets that it could be obliged to purchase. Even if there is no legal obligation for a member insurer to purchase crypto-assets from non-member holders, insurers and supervisors should consider whether in practice the member insurer would be obliged to step-in and purchase them in order to satisfy the expectations of non-member holders and protect the insurer's reputation. Where such step-in risk exists, insurers should include within the risk exposure the amount that would apply if legally binding commitments have been made. Exceptions would only be made if the insurer can demonstrate to the lead supervisor that such step-in risk does not exist.

- 2.7 The risks to insurer 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 insurers are non-member holders they must sum the risk factors determined for the two risks. The first risk should be determined using the risk factor that would arise from a direct exposure to the underlying. The determination of the risk factor 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 risk factor should be applied to the exposure, or based on the credit rating, to the member, as applicable under the LICAT, MCT and MICAT. If there are multiple members, the risk factor to be used should be the risk factor that would be applied to the exposure, or based on the credit rating, to the member with the highest credit rating (i.e. lowest risk factor), as applicable under the LICAT, MCT and MICAT.[13]

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 insurer holder should include the sum of the risk factors for all three separate exposures. The risk factor for the first two risks must be determined in the same way as described in (i) above. The risk factor for the third risk must be determined in the same way as the risk factor that would be applied to an exposure, or based on the credit rating, to the redeemer, as applicable under the LICAT, MCT and MICAT.

3. 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.

Annex 3: Group 2a hedging recognition criteria

- 3.1 Insurers that have not obtained OSFI confirmation to use Group 2a classification 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 an insurer has received OSFI confirmation, may be classified as Group 2a:

    1. The insurer'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 insurer'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.

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

Annex 4: Insurer risk management

- 4.1 Crypto-asset activities introduce new kinds of risk and increase certain traditional risks. Insurers 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, and market risks) related to crypto-assets or related activities on an ongoing basis. Insurers' 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 and provide services to crypto-asset operators should be fully consistent with the insurer's risk appetite and strategic objectives as set down and approved by the board, as well as with senior management's assessment of the insurer's risk management capabilities, in particular for market and counterparty credit risk and operational risk.

- 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 credit risk, insurers 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 insurer 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.

- 4.3 Insurers 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.

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

1. **Crypto-asset technology risk**: Insurers 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.

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**: An insurer 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 insurers' 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 insurers that take crypto-assets as collateral can take possession in the event of default/margin call.

    3. **Disclosure and consumer protection**: Insurers that provide services involving 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**: Financial institutions in their role of providing 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 insurers.

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 insurers in a variety of contexts tied to mispricing due to inadequate operational processes.

- 4.5 OSFI may impose additional capital charges on individual insurers 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 insurer's risk management of crypto-assets is considered inadequate. OSFI may request insurers to provision for losses related to crypto-assets where such losses are foreseeable and estimable. Finally, OSFI may impose mitigation measures on insurers, such as requiring an insurer to establish an internal limit to contain the risks not adequately identified or assessed in the insurer's risk management framework.

1 For the purposes of this guideline, the term "insurers" refers to all federally regulated insurers, including Canadian branches of foreign life and property and casualty companies, fraternal benefit societies, regulated insurance holding companies and non-operating insurance companies.

2 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).

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

4 Insurers should seek a confirmation from OSFI prior to using the Group 2a classification.

5 For the purposes of this guideline, "life insurers" includes all federally regulated life insurers, including Canadian branches of foreign life companies, fraternal benefit societies, regulated life insurance holding companies and non-operating life insurance companies; "property and casualty insurers" includes all federally regulated property and casualty insurance companies, and foreign property and casualty companies operating in Canada on a branch basis.

6 Securities financing transactions (SFT) are transactions such as repurchase agreements, reverse repurchase agreements, security lending and borrowing, and wholesale margin lending transactions, where the value of the transactions depends on the market valuations and the transactions are often subject to margin agreements.

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

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

9 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.

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

10 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.

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

12 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.

13 For example, consider the situation in which there is only one member and it has a high credit rating (and therefore a low risk factor). Its low risk factor 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 factor). 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 factor of the first member can continue to be used to determine the credit risk to non-member holders.