

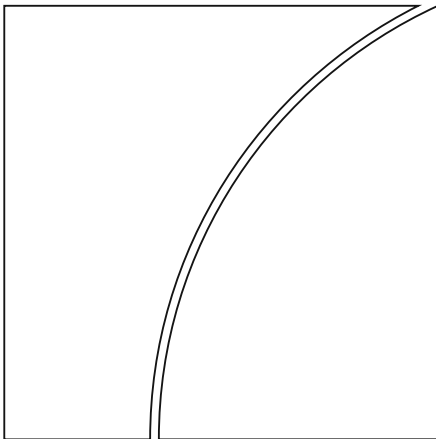
Basel Committee on Banking Supervision

Consultative Document

Disclosure of cryptoasset exposures

Issued for comment by 31 January 2024

17 October 2023



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

© *Bank for International Settlements 2023. All rights reserved. Brief excerpts may be reproduced or translated provided the source is stated.*

ISBN 978-92-9259-698-9 (online)

Contents

- 1. Introduction 1
- 2. Structure of proposed disclosure requirements..... 1
- 3. Implementation date..... 2
- 4. Request for feedback 2
- Annex 1: Proposed text of *DIS55 – Cryptoasset exposures* 3
- Annex 2: Potential additional qualitative disclosures 12

1. Introduction

In December 2022, the Basel Committee published *Prudential treatment of cryptoasset exposures*,¹ which sets out the prudential requirements for banks' exposures to cryptoassets. The requirements are specified in a new chapter of the consolidated Basel Framework (SCO60), with an implementation date of 1 January 2025. Paragraphs SCO60.128 to SCO60.130 describe the disclosure requirements that apply to banks' exposures to cryptoassets.

To facilitate consistency of disclosures, the Committee has developed a set of standardised disclosure templates. The templates incorporate the requirements of SCO60.128 to SCO60.130 and are set out in a new chapter of the Basel Framework: *DIS55 Cryptoasset exposures*. The Basel Committee expects that the use of common disclosure templates for banks' cryptoasset exposures will support the exercise of market discipline and contribute to reducing information asymmetry amongst banks and market participants.

As a new chapter of the disclosure standard in the Basel Framework, DIS55 will be subject to the overarching requirements of chapter DIS10, such as scope of application, reporting location and frequency and timing of disclosures and assurance of Pillar 3 data.

The Committee welcomes comments from the public and market participants, including Pillar 3 disclosure users and preparers, on all aspects of this consultative document.

Comments must be submitted by 31 January 2024 using the following link <https://www.bis.org/bcbs/commentupload.htm>. Comments will be published on the Bank for International Settlements website, unless the respondent specifically requests confidential treatment.

2. Structure of proposed disclosure requirements

The proposal for DIS55 is set out in Annex 1 to this publication and contains the following table and templates:

- Table CAEA: Qualitative disclosure on a bank's activities related to cryptoassets and the approach used in assessing the classification conditions.
- Template CAE1: Cryptoasset exposures and capital requirements.
- Template CAE2: Accounting classification of exposures to cryptoassets and cryptoliabilities.
- Template CAE3: Liquidity requirements for exposures to cryptoassets and cryptoliabilities.

When finalised, DIS55 will replace paragraphs SCO60.128 to SCO60.130 of the Basel Framework. In addition to incorporating the requirements of SCO60.128 to SCO60.130, DIS55 will require banks to disclose the sources of information that they have used to assess whether the cryptoassets to which they are exposed comply with the cryptoasset classification conditions set out in SCO60 and includes standardised disclosures relating to liquidity requirements.

In *Prudential treatment of cryptoasset exposures*, the Committee noted various elements of the cryptoasset standard that are subject to specific monitoring and review (eg statistical tests, composition of reserve assets for the purpose of the redemption test, permissionless blockchains). As these reviews

¹ www.bis.org/bcbs/publ/d545.htm.

conclude, the Committee will consider whether any adjustments to the proposed disclosure requirements set out in this consultation will be necessary.

3. Implementation date

The proposed requirements set out in DIS55 will apply to internationally active banks at the top consolidated level. The Committee proposes an implementation date of 1 January 2025 for DIS55, consistent with SCO60.

4. Request for feedback

The Committee welcomes feedback on all aspects of the proposals set out in this consultation. In addition, it would welcome feedback on the following issues:

- *Classification condition assessment detail:* For Group 1 cryptoasset exposures, Table CAEA requires banks to disclose the approach they have used to assess compliance with each of the four Group 1 classification conditions, including any public information used but excluding any confidential and proprietary information. The Committee is considering whether to add more detail on the information that banks should disclose for each classification condition. This additional information is set out in Annex 2, and the Committee would welcome feedback from stakeholders on the usefulness of this potential addition to Table CAEA.
- *Window-dressing:* The period-end amounts that banks report under the proposals may not give an accurate picture of the risk to which banks are exposed if the exposure values during the reporting period are significantly different to the period end values. As such, the Committee sees merit in requiring banks to disclose the amounts in Template CAE1 using daily average values in addition to the period-end values.
- *Materiality:* Table CAEA and Template CAE1 include disclosure requirements for banks' "material" cryptoasset exposures. The Committee is considering whether to define what constitutes a material exposure in this context of cryptoasset exposures disclosure and, if so, the appropriate threshold. For example, an exposure could be considered material if it exceeds 5% of the bank's total cryptoasset exposures. The Committee would welcome feedback on the usefulness and specification of any potential materiality definition.

Annex 1: Proposed text of *DIS55 – Cryptoasset exposures*

55.1 The disclosure requirements under this section are:

- (1) Table CAEA: Qualitative disclosure on a bank's activities related to cryptoassets and the approach used in assessing the classification conditions.
- (2) Template CAE1: Cryptoasset exposures and capital requirements.
- (3) Template CAE2: Accounting classification of exposures to cryptoassets and cryptoliabilities.
- (4) Template CAE3: Liquidity requirements for exposures to cryptoassets and cryptoliabilities.

Table CAEA: Qualitative disclosure on a bank's activities related to cryptoassets and the approach used in assessing the classification conditions

<p>Purpose: To provide an overview of the bank's activities related to cryptoassets and main risks related to its cryptoasset exposures as well as the approach used in assessing the classification conditions.</p>
<p>Scope of application: The template is mandatory for all banks with exposures to cryptoassets or cryptoliabilities.</p>
<p>Content: Qualitative information.</p>
<p>Frequency: Annual.</p>
<p>Format: Flexible.</p>
<p>Banks must describe:</p>
<p>(a) Their business activities related to cryptoassets, including inter alia owning cryptoassets directly, trading of cryptoassets on clients' accounts, equity investments in cryptoasset activities (eg cryptoasset exchanges and fund managers of cryptoasset exchange-traded funds) and the issuance of cryptoassets by the bank (ie cryptoliabilities of the bank). Banks must explicitly state if the bank is a member of cryptoasset arrangements as described in [SCO60.36] acting as an intermediary in the redemption of cryptoasset. In such cases, banks must describe their role and the extent of any commitments to redeem or purchase back cryptoassets that may result from those activities.</p>
<p>(b) For each activity in (a), how the activity translates into components of the bank's risk profile (including, but not limited to, credit, market, operational and/or liquidity risks) and the associated risk management policies (including, but not limited to, strategies and processes to manage, hedge and mitigate risks that arise from the bank's business activities and the processes for monitoring the continuing effectiveness of hedges and mitigants).</p>
<p>(c) Scope and main content of the bank's reporting related to cryptoassets, including, but not limited to, how business activities result in the bank having cryptoasset exposures covered under the scope of the prudential treatment of cryptoassets and/or any material exposures to specific cryptoassets.</p>
<p>(d) The most significant current risk(s) associated with the bank's activities related to cryptoassets and the bank's cryptoasset exposures and how this current risk is being managed.</p>
<p>(e) The most significant emerging risk(s) associated with the bank's activities related to cryptoassets and the bank's cryptoasset exposures and how this emerging risk is being managed.</p>
<p>(f) For exposures to Group 1 cryptoassets, the bank's approach to assessing each of the following classification conditions for each cryptoasset, including any public information used but excluding any confidential and proprietary information:</p> <ul style="list-style-type: none"> i) Classification Condition 1 [SCO60.8] to [SCO60.13] ii) Classification Condition 2 [SCO60.14] to [SCO60.15] iii) Classification Condition 3 [SCO60.16] to [SCO60.17] iv) Classification Condition 4 [SCO60.18] to [SCO60.19]

Template CAE1: Cryptoasset exposures and capital requirements

Purpose: To provide an overview of a bank's exposures to cryptoassets according to the prudential classification of the cryptoassets (Group 1a, 1b, 2a and 2b) and the related capital requirements.

Scope of application: The template is mandatory for all banks with exposures to cryptoassets.

Content: Exposures and capital requirements applicable to the bank's cryptoasset exposures excluding liquidity requirements which are contained in Template CAE3.

Frequency: Semiannual.

Format: Flexible.

Accompanying narrative:

- Due to the difficulty of disaggregating operational risk RWA only related to cryptoasset exposures, banks are expected to supplement the template to explain their policies and risk mitigation used in their management of operational risk related to cryptoasset exposures.
- Banks are expected to supplement the template with a narrative commentary to explain any significant changes over the reporting period and the key drivers of such changes.
- When authorities apply the infrastructure add-on outlined in [SCO60.52] to [SCO60.53] to Group 1 cryptoassets, banks must disclose the RWA amount resulting from these requirements.

	a	b	c		d	e		f	g	
			Credit risk			Market risk				Cryptoassets under custody
			Total exposure	Exposure/EAD		RWA	Long exposure			
1	Group 1a									
2	Group 1b									
2.a	Of which: Cryptoasset XXX									
2.b	Of which: Cryptoasset YYY									
	...									
3	Group 2a									
3.a	Of which: Cryptoasset XXX									
3.b	Of which: Cryptoasset YYY									

....												
4	Group 2b											
4.a	Of which: Cryptoasset XXX											
4.b	Of which: Cryptoasset YYY											
...												
5	TOTAL											

a. Additional information

6	Operational risk losses	
7	Group 2 exposure limit – direct holdings	
8	Group 2 exposure limit – indirect holdings	
9	Group 2 exposure limit – exposure above the 1% limit	
10	Group 2 exposure limit – RWA above the 1% limit	
11	Total RWA for Group 2 as a result of breaching the 2% limit	

Instructions:

- The balance sheet and regulatory amounts reported in the template should reflect the values as at the reporting period end. [Banks should also complete this template using daily average values calculated over the reporting period.]
- In addition to the separate disclosure requirements set out in this template that apply to all Group 1a, Group 1b, Group 2a and Group 2b cryptoassets, banks must include exposures to Group 1 cryptoassets in the relevant existing disclosure templates that apply to traditional assets (eg for credit risk and market risk).
- For cryptoassets belonging to Groups 1b, 2a and 2b, additional rows should be added for each material exposure to stablecoins and unbacked cryptoassets by individual cryptoasset. Any tokenised traditional asset included in Group 2a or Group 2b as a result of not meeting the classification conditions does not need to be separately disclosed, but the relevant amounts must be reported in the total rows for Group 2a and Group 2b (ie row (3) and row (4)).
- Given that RWA for counterparty credit risk (CCR) and credit valuation adjustment risk (CVA) are calculated on a portfolio basis, it is not possible to separately identify the amounts related to cryptoassets. The CCR and CVA amounts are therefore excluded from the scope of this template.

Columns:

- **(a) Total exposure:** on- and off-balance sheet items that give rise to a credit risk exposure according to the finalised Basel Framework. The amount must be gross of any credit conversion factor (CCF) or credit risk mitigation (CRM) techniques.
- **(b) Exposures/EAD post CRM and post CCF:** the exposure amount or EAD relevant for the capital requirements calculation.
- **(c) Credit risk RWA:** RWA according to the credit risk standard of the Basel Framework (CRE). For Group 2b cryptoassets, total RWA will be reported in this cell, as in compliance with [SCO60.83] there is no separate trading book and banking book treatment for Group 2b cryptoassets. The conservative treatment is intended to capture both credit and market risk, including CVA risk. For consistency, the RWA calculated under this approach must all be reported as part of the bank's credit RWA. Nevertheless, for Group 2b cryptoassets banks must report aggregated market value of gross long and short positions in the trading book in columns (d) and (e), respectively, since to compute RWA banks must apply the risk weight of 1,250% to the greater of the absolute value of the aggregate long positions and the absolute value of the aggregate short positions in the cryptoasset.
- **(d) Market risk – long exposure:** aggregated market value of gross long positions in the trading book by cryptoasset group and activity type.
- **(e) Market risk – short exposure:** aggregated market value of gross short positions in the trading book by cryptoasset group and activity type.
- **(f) Market risk – RWA:** includes the market risk RWA calculated for trading book and banking book exposures that are subject to market risk capital requirements in [MART10] to [MAR40], taking into account the requirements of [SCO60]. Since the market risk framework does not refer to RWA, banks should indicate the derived RWA number (ie by multiplying the capital charge by 12.5). As market risk is calculated on a portfolio basis, it will not always be possible to calculate standalone market RWA for Group 1a and Group 1b cryptoassets, and so the relevant cells in this column have been greyed out. Similarly, for Group 2b cryptoassets SCO60.83 requires the RWA to be reported as credit risk, and so these cells are also greyed out. By contrast, the dedicated market risk treatment for Group 2a cryptoassets should allow RWA amounts for these exposures to be reported.
- **(g) Cryptoassets under custody:** the market value of cryptoassets that the bank holds in custody for clients at the end of the reporting period.

Rows:

- **Group allocation:** this classification relates to the classification of cryptoassets into groups according to [SCO60.6]. The assigned group depends on the type of cryptoasset, and whether the four classification conditions are met. If all four classification conditions are met and the cryptoasset is a tokenised traditional asset, then the relevant amounts must be reported in Group 1a. If all classification conditions are met and the cryptoasset has an effective stabilisation mechanism, the relevant amounts must be reported in the Group 1b row. If at least one of the classification conditions is not met but the cryptoasset passes the Group 2a hedging recognition criteria, the relevant amounts must be reported in the Group 2a row. All other cryptoassets must be reported in the Group 2b row.
- **Rows 2, 3 and 4** are the amounts related to all the cryptoassets belonging to those groups (ie not only the sum of each material individual exposure to stablecoins and unbacked cryptoassets included in the template).

- **Operational risk losses:** total amount of operational losses related to cryptoassets net of recoveries and net of excluded losses within the 10-year window or fewer years in accordance with OPE25.10 that is relevant for the Loss Component calculation. Amounts should be reported if the bank is required to calculate the Loss Component under the standardised approach to operational risk set out in [OPE25].
- **Group 2 exposure limit – direct holding:** aggregate direct holdings of Group 2 cryptoassets subject to the exposure limit according to [SCO.60.116].
- **Group 2 exposure limit – indirect holding:** aggregate indirect holdings of Group 2 cryptoassets subject to the exposure limit according to [SCO.60.116] (eg those via investment funds, ETF/ETN, or any legal arrangements designed to provide exposures to cryptoassets).
- **Group 2 exposure limit – exposure above the 1% limit:** the bank's total exposure to Group 2 cryptoassets above the 1% of the bank's Tier 1 capital.
- **Group 2 exposure limit – RWA above the 1% limit:** the bank's RWA related to its exposures to Group 2 cryptoassets that are in excess of the 1% threshold, but below the 2% of the bank's Tier 1 capital. Until compliance with the 1% limit is restored, the bank's exposures that are in excess of the threshold will be subject to the capital requirements that apply to Group 2b cryptoasset exposures (as set out in [SCO60.83] to [SCO60.85]).
- **Group 2 exposure limit – RWA for Group 2 as a result of breaching the 2% limit:** the bank's RWA of Group 2 cryptoassets when its exposures exceed 2% of its Tier 1 capital. In this case, all Group 2 cryptoasset exposures will be subject to the capital requirements that apply to Group 2b cryptoasset exposures according to [SCO60.118]. For banks breaching this 2% limit, final RWA for all Group 2 cryptoassets must be reported in this column. Consequently, banks breaching the 2% limit must not report RWA figures in columns (b), (c) or (f).

Template CAE2: Accounting classification of exposures to cryptoassets and cryptoliabilities

Purpose: Provide information on the accounting classification and measurement of banks' exposures to cryptoassets and cryptoliabilities.

Scope of application: The template is mandatory for all banks with exposures to cryptoassets or cryptoliabilities.

Content: Carrying values corresponding to the values reported in financial statements but under scope of regulatory consolidation.

Frequency: Semiannual.

Format: Flexible (but the rows must align with the presentation of cryptoassets in the bank's financial report).

Accompanying narrative: Banks are expected to supplement the template with a narrative commentary to explain any significant changes over the reporting period and the key drivers of such changes. In addition, banks must report if there is any accumulated allowance/impairment on exposure measured at amortised cost.

	a	b	c	d
	Carrying values under scope of regulatory consolidation			
	Group 1a	Group 1b	Group 2a	Group 2b
Assets				
Cash				
Financial assets				
Of which: measured at fair value through profit and loss (FVTPL)				
Of which: measured at fair value through other comprehensive income (FVTOCI)				
Of which: measured at amortised cost (AC)				
Intangibles				
...				
Total assets				
Liabilities				
Financial liabilities				
...				
Total liabilities				

Instructions: Banks must also include Group 1 cryptoassets disclosed in columns (a) and (b) in the relevant templates that apply to traditional assets.

Columns:

- Group allocation: The assigned group depends on the type of cryptoasset, and whether the four classification conditions set out in [SCO60.6] to [SCO60.22] are met. If all four classification conditions are met and the cryptoasset is a tokenised traditional asset, then it must be reported in Group 1a. If all classification conditions are met and the cryptoasset is a cryptoasset with an effective stabilisation mechanism, it must be reported in Group 1b. If at least one of the classification conditions is not met but the cryptoasset passes the Group 2a hedging recognition criteria, it must be reported in Group 2a. All other cryptoassets must be reported in Group 2b.

Rows:

- Rows must include only assets and liabilities that are within the scope of [SCO60]. The rows must follow the balance sheet presentation used by the bank in its financial reporting.

Template CAE3: Liquidity requirements for exposures to cryptoassets and cryptoliabilities

Purpose: To provide an overview of a bank's exposures to cryptoassets and cryptoliabilities according to the liquidity risk classification.

Scope of application: The template is mandatory for all banks with exposures to cryptoassets and cryptoliabilities.

Content: Key liquidity risk parameters for the relevant categories of cryptoasset as described in [SCO60.101] to [SCO60.112]. To note, the categories of cryptoasset and cryptoliability that are relevant for the liquidity prudential treatment are different from the categories used for credit and market risk.

Frequency: Semiannual.

Format: Fixed.

Accompanying narrative: When a single cryptoasset or cryptoliability exposure is considered material, the bank should give individual information about the prudential treatment applied to the exposure.

	a	b	c	d	e	f	g	h	i							
										Exposure amounts			Liquidity risk			
										Cryptoassets		Cryptoliabilities		Cryptoassets		Cryptoliabilities
	Total	Of which: Derivative exposures	Total	Of which: Derivative exposures	LCR HQLA haircut applied	LCR cash inflow rate applied	NSFR RSF factor applied	LCR cash outflow rate	NSFR ASF factor applied							
1	Group 1a															
1.a	Of which: HQLA instrument															
1.b	Of which: tokenised claims on a bank															
1.c	Of which: other tokenised assets															
2	Stablecoins															
2.a	Of which: Group 1b															
2.b	Of which: Group 2															
3	Other Group 2															

Instructions: This template provides an overview of the liquidity risk classification of cryptoasset and cryptoliabilities. Banks must also consider these instruments as part of the relevant disclosure templates for banks' liquidity (see DIS85).

Columns:

Asset and liability exposure amounts are the outstanding values at the end of the reporting period.

Inflow rates, outflow rates, haircuts and NSFR ASF and RSF factors are expressed as the weighted average rates of the cryptoasset and cryptoliability categories (weighted by the exposure amounts).

Rows

Row number	Explanation	Relevant paragraphs of [SCO60]
1	This row is the sum of rows (1.a), (1.b) and (1.c).	[SCO60.102] to [SCO60.108]
1.a	Group 1a cryptoassets that are tokenised versions of HQLA as defined in [LCR30.40] to [LCR30.47]. The calculation and definition of HQLA for LCR and NSFR purposes must align to those in the LCR disclosure standard.	[SCO60.102] to [SCO60.103]
1.b	Group 1a cryptoassets or cryptoliabilities that are tokenised claims on a bank.	[SCO60.107]
1.c	Group 1a cryptoassets or cryptoliabilities which are different from those reported in rows (1.1) and (1.2).	[SCO60.102] to [SCO60.108]
2	Cryptoassets or cryptoliabilities that are fully collateralised by a segregated pool of underlying assets that do not count toward the bank's stock of HQLA. This row is the sum of rows (2.a) and (2.b).	[SCO60.108]
2.a	Stablecoins that qualify as Group 1b.	
2.b	Stablecoins that do not qualify as Group 1b cryptoassets solely due to redemption restrictions (ie minimum notice periods).	
3	Group 2 cryptoassets or cryptoliabilities other than stablecoins reported in row (2.b), ie are subject to the treatment outlined in [SCO60.109].	[SCO60.109]

Annex 2: Potential additional qualitative disclosures

Set out below are a set of potential additional qualitative disclosures that could be added to Table CAEA to provide more detail on the information banks have used to determine that cryptoassets they classify as Group 1 have met the four classification conditions set out in SCO60. The Committee would welcome feedback from stakeholders on the usefulness of this potential addition to Table CAEA.

Potential elements to add to Table CAEA

For exposures to Group 1 cryptoassets, banks would be required to disclose the following information relating to the information they used to assess compliance with the four Group 1 classification conditions:

Classification condition 1 [SCO60.8] to [SCO60.13]

If the cryptoasset has a stabilisation mechanism, banks must describe the following relating to the requirements of [SCO60.11]:

- How the stabilisation mechanism functions to minimise fluctuations in the market value of the cryptoasset relative to the peg value.
- The ownership rights of the reserve assets upon which the stable value of the cryptoasset is dependent.
- How underlying physical assets are custodied, stored and managed appropriately.
- The jurisdiction and supervisor of the issuer of cryptoasset (this supervisor must apply prudential capital and liquidity requirements to the issuer).
- Where they have obtained the “public” information to ensure the accuracy of the above elements.

If the cryptoasset has a stabilisation mechanism, banks must describe the following relating to the requirements of the redemption risk test set out in [SCO60.12]:

- The value of the reserve assets (accounting values) and aggregate peg value of all issued tokens.
- The frequency of valuation and disclosure of the reserve assets and the quality of available data.
- The outcome of the required independent external audit to confirm that the disclosed reserves are consistent with the mandate, including whether the audit opinion was qualified in any way.
- A description of the types of assets included in the reserve, including:
 - Percentage of level 1 HQLA of the reserve assets
 - Percentage of other assets
 - Percentage of assets in a different currency than the peg value, including any hedge to cover the currency mismatch.
- Where they have obtained the (public) information to ensure the accuracy of the above elements.
- Whether the redemption function performed by an intermediary and, if so, the credit risk to which the bank is exposed.

Classification condition 2 [SCO60.14] to [SCO60.15]

If the cryptoasset has a stabilisation mechanism, banks must describe the following:

- The arrangements which guarantee that the issuer and/or underlying reserve assets ensure full redeemability at all times at their peg value and within five calendar days of the redemption request.
- Which parties have the right to redeem, the obligation of the redeemer to fulfil the arrangement, the timeframe for this redemption to take place, the traditional assets in the exchange and how the redemption value is determined.
- Where they have obtained the (public) information to ensure the accuracy of the above elements.

Classification condition 3 [SCO60.16] to [SCO60.17]

Banks must describe the following:

- The risks of the network in which the cryptoasset operates and how these are mitigated and managed.
- The risk governance and risk control policies of the entities performing the activities associated with the functions of the cryptoasset, such as issuance, validation, redemption and transfer of the cryptoassets to address the risks described in [SCO60.17](1).
- The key aspects of the network: the operational structure (ie whether there is one or multiple entities that perform core function(s) of the network), the degree of access (ie whether the network is restricted or unrestricted), technical roles of the nodes (ie whether there are differential roles and responsibilities among nodes) and the validation and consensus mechanism of the network (ie whether validation of a transaction is conducted with single or multiple entities).
- Where they have obtained the (public) information to ensure the accuracy of the above elements.

Classification condition 4 [SCO60.18] to [SCO60.19]

Banks must describe the following:

- If applicable, the names of the jurisdiction and supervisor of entities^[1] that execute redemptions, transfers, storage or settlement finality of the cryptoasset, or manage or invest reserve assets. If these entities are not regulated and supervised, the risk management standards they have in place.
- The governance framework of entities that execute redemptions, transfers, storage or settlement finality of the cryptoasset, or manage or invest reserve assets.
- Where they have obtained the (public) information to ensure the accuracy of the above elements.

Footnotes

[1] *Entities include operators of the transfer and settlement systems for the cryptoasset, wallet providers and, for cryptoassets with stabilisation mechanisms, administrators of the stabilisation mechanism and custodians of the reserve assets.*