Thematic Review Assessing the Implementation of IOSCO Recommendations for Crypto and Digital Asset Markets

FINAL REPORT

The Board of the
International Organization of Securities Commissions

FR/13/25 October 2025

Copies of publications are available from
The International Organization of Securities Commissions website

iosco.org

Table of Contents

Chapter 1 – Executive Summary

The International Organization of Securities Commissions (IOSCO) published in 2023 a set of 18 policy recommendations for the regulation of crypto and digital assets (CDA Recommendations) in accordance with principle of 'same activity, same risk, same regulation/regulatory outcome.' These policy recommendations are designed to support greater consistency with respect to regulatory frameworks and oversight in IOSCO Member Jurisdictions to address concerns related to market integrity and investor protection arising from crypto-asset activities. These Recommendations were intentionally designed to be principles-based and outcomes-focused[1]. This report (Thematic Review, or Report) reviews progress of selected IOSCO jurisdictions (Participating Jurisdictions) in implementing a suite of the CDA Recommendations (Assessed Recommendations).

In parallel to IOSCO's efforts, the Financial Stability Board (FSB) has also undertaken a thematic peer review to examine its members and select non-member jurisdictions in implementing the FSB Global Regulatory Framework for Crypto-asset Activities[2]. Together these reports consider the progress to implement regulatory frameworks covering financial stability risks, investor protection and market integrity.

Overall findings and conclusions

Overall, the Thematic Review has concluded that significant progress is being made in relation to the implementation of the key elements of the Assessed Recommendations, focusing on market integrity and investor protection. This progress is being made through Participating Jurisdictions implementing legal and regulatory frameworks in line with the CDA Policy Recommendations. While some have adapted existing legislation to crypto-asset service

[1] *IOSCO Policy Recommendations for Crypto and Digital Asset Markets Final Report*, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD747.pdf, p.3 ("Each jurisdiction should implement the Recommendations, as they deem appropriate, within their existing or developing frameworks considering each Regulator's role within those existing or developing frameworks, and the outcomes achieved through the operation of the frameworks in each jurisdiction."); p.4-5 (" …Chapter 1 further clarifies the intent of the Recommendations. This operative provision, that informs all 18 Recommendations while underscoring the need to promote optimal regulatory consistency across member jurisdictions, also acknowledges, and provides for, appropriate principles, and outcomes-based flexibility in their domestic implementation.")

[2] *Thematic Review on FSB Global Regulatory Framework for Crypto Asset Activities*, https://www.fsb.org/2025/10/thematic-review-on-fsb-global-regulatory-framework-for-crypto-asset-activities

providers (CASPs)[3], others have introduced new regulations for this area. Both scenarios may present challenges, including on the scope of coverage for crypto-assets.

It is encouraging to note that the steps that Participating Jurisdictions have taken are generally designed to address investor protection and market integrity risks. However, jurisdictions must continue to monitor and address emerging and developing risks, and ensure such frameworks remain fit for purpose. While the Thematic Review has not considered the efficacy of regulatory frameworks in addressing the risks to investor protection and market integrity posed by crypto-assets, crypto-assets are increasing their footprint across the world, and there has been a change in approach to crypto-asset services by a number of jurisdictions. However, there is much more to do by Participating Jurisdictions, especially as new crypto-asset business models are being developed, existing risks are changing, and various new risks are emerging.

The regulatory frameworks of the Participating Jurisdictions are still developing with the majority in the process of making further reforms to their regulatory frameworks, notably to proactively address new risks from market developments in their jurisdictions, and go beyond the key elements of the Assessed Recommendations. Generally, the additional steps being taken by Participating Jurisdictions are aimed at further strengthening their capacities to apply risk-based regulations, support responsible innovation, and ensure effective and adaptive regulatory oversight. Jurisdictions need to continue strengthening their ability to respond to the fast-evolving nature of crypto-asset markets.

While noting the progress achieved by all Participating Jurisdictions, particularly with respect to custody-related recommendations, risks to investor protection and market integrity remain within the fast-evolving crypto-asset ecosystem. Jurisdictions should take steps to monitor the risks in their jurisdiction and seek to fully implement all of the elements of the 18 CDA Policy Recommendations, as early as possible. As set out in the FSB Report, "While financial stability risks from crypto-assets appear limited at present, monitoring financial stability risks in crypto asset markets, including specific use cases and interconnections, is critical for authorities to fulfil their financial stability mandates."

The Review Team (RT) has observed that the majority of the Participating Jurisdictions have adopted varying approaches to comply with the key elements of the Assessed Recommendations and has highlighted some of the approaches that Participating Jurisdictions have taken to implement the Assessed Recommendations throughout this Report. The regulatory measures introduced may not always be the same, with nuances tailored to the most predominant risks as seen in the relevant jurisdiction or to other aspects of the applicable regulatory framework. Due to ongoing implementation efforts across jurisdictions and the continued evolution of crypto-asset markets, it is still too early to evaluate

[3] CASP is defined in the *IOSCO Policy Recommendations for Crypto and Digital Asset Markets Final Report* as "service providers that conduct a wide range of activities relating to crypto-assets, including but not limited to, admission to trading, trading (as agent or principal), operating a market, custody, and other activities such as services relating to lending/staking of crypto-assets and the promotion, marketing and distribution of crypto-assets on behalf of others

the effectiveness of these varying approaches. Nevertheless, it may be useful for jurisdictions to understand the variety of approaches observed to date. It is also important for jurisdictions to be cognisant of this variety of approaches, especially where there are firms operating across a number of jurisdictions. At the same time, a number of jurisdictions continue to face different types and degrees of challenges in adopting all the key elements of the CDA Recommendations and achieve the outcomes sought. With a view to promoting compliance with the CDA Recommendations, IOSCO will look to enhance its capacity building programme to facilitate knowledge sharing and different approaches to CDA risks across IOSCO Member Jurisdictions and other jurisdictions with whom they interact.

The RT also recognised that most of the Participating Jurisdictions have mechanisms to facilitate cross-border cooperation, although in some instances there are hurdles to the effective use of these mechanisms. Jurisdictions should therefore consider enhancements consistent with the CDA recommendations to ensure that they are able to effectively share relevant information in practice.

As Participating Jurisdictions are still in the process of developing and implementing their regulatory frameworks for cross-border cooperation consistent with the CDA Recommendations, the use of existing mechanisms in place to permit information sharing across jurisdictions relating to crypto-asset markets has been relatively limited to date. This is however work in progress and will continue to evolve as part of ongoing implementation efforts.

In line with the CDA Recommendations, jurisdictions "should have the ability to share information and cooperate with regulators and relevant authorities in other jurisdictions with respect to [...] crypto-asset issuance, trading, and other activities." Furthermore, the CDA Recommendation states that available co-operation arrangements and/or other mechanisms "should accommodate the authorization and on-going supervision of regulated CASPs and enable broad assistance in enforcement". With most major CASPs having a global footprint, there is an increasing need for enhancements to the current level of cross-border cooperation. The Review Team encourages IOSCO and other relevant SSBs to monitor developments in the space while ensuring that there are no barriers to information sharing in enforcement, supervision and other regulatory contexts. The Review Team recommends that IOSCO explore potential enhancements, in line with the CDA Recommendations, and where relevant, in collaboration with other SSBs and other international organizations with a role in providing technical assistance to promote understanding of crypto-asset activities and regulatory requirements.

Key Findings by Assessed Recommendations

Recommendation 2: Governance and disclosure of conflicts of interest. All Participating Jurisdictions have made progress, in varying degrees, in implementing this Recommendation. Ten have put in place relevant requirements on governance that are already in force. Notwithstanding, two of them are proposing to introduce different additional measures in their existing framework to further enhance CASPs' governance and organisational requirements. For the remaining ten, two of them are in the process of consulting on their draft framework

and eight of them have not yet published implementation measures or have not proposed measures that fully address all the elements of this Recommendation.

Recommendation 3: Disclosure of Role, Capacity and Trading Conflicts. The majority of the Participating Jurisdictions have made progress in implementing this Recommendation. Eleven have final implementation measures in force, meeting all key elements of this Recommendation. Three jurisdictions have published draft implementation measures. The remaining six jurisdictions have not published implementation measures for at least one key element, but four jurisdictions have further reforms underway. Some of the challenges observed include inadequate conflict of interest management systems, variability in disclosure requirements and a lack of requirements for ongoing disclosure.

Recommendation 8: Fraud and Market Abuse. Most of the Participating Jurisdictions have implemented this Recommendation. Twelve of them have final implementation measures in force, meeting all key elements of this Recommendation. Five jurisdictions are on the path towards full implementation, having published draft measures but have yet to finalise their policies. The remaining three jurisdictions have not published implementation measures for at least one key element, but one has further reforms underway. Some of the challenges highlighted include limits in enforcement authority beyond CASPs.

Recommendation 11: Enhanced Regulatory Cooperation. All Participating Jurisdictions are signatories to the IOSCO MMoU, and some of them to the IOSCO EMMoU, and therefore have at least one information sharing framework in place that can be used to exchange crypto-asset information. The MMoU and EMMoU focus on enforcement proceedings to a large extent, and fit-and-proper information at the authorisation stage to some extent. As stated by the CDA Recommendation, in addition to broad assistance in enforcement, the available co-operation arrangements and/or other mechanisms "should accommodate the authorization and on-going supervision of regulated CASPs". Almost all the Participating Jurisdictions (19) have additionally put in place regional or bilateral cooperation arrangements, covering supervisory information sharing at large or thematic topics on innovation and fintech matters. Gaps for this Recommendation exist largely because some Participating Jurisdictions have indicated that there are legal barriers to facilitating cross-border cooperation. Separately, despite the existence of cooperation mechanisms, their use remains fairly limited, and enhancements should be considered to promote cross-border information sharing and account for the evolving crypto-assets sector, including considerations of enhanced cooperation mechanisms beyond the enforcement context, to support authorization and ongoing supervision of regulated CASPs operating across multiple jurisdictions.

Recommendations 12: Overarching Custody Recommendation. Twelve Participating Jurisdictions have final implementation measures in force – these include a combination of existing frameworks extended and/or amended to cover CASPs that hold or safeguard crypto-assets, and new frameworks. Three Participating Jurisdictions have published consultative implementation measures, and five have not published implementation measures or have gaps in one or more key elements. Some gaps have been identified both in existing and new frameworks. Overall, existing regulatory frameworks have provided a good basis for the implementation of Recommendation 12, with the exception of one framework lacking coverage

of the specific aspects related to securing the private keys that grant access to crypto-assets. At the same time, gaps were also found in new frameworks in two jurisdictions.

Recommendation 13: Segregation and Handling of Client Monies and Assets. Most of the Participating Jurisdictions have made considerable progress and have now met some or all the requirements under this Recommendation. Fourteen of them have final implementation measures in force whereas four of them have not published implementation measures. However, in certain cases, the respective jurisdictions already meet one or two key elements of the Recommendation. Some of those jurisdictions also have reforms underway whereas two jurisdictions have not published any measures to implement the key elements. Two jurisdictions have draft implementation measures published that address all key elements of the Recommendation.

Recommendation 14: Disclosure of Custody and Safekeeping Arrangements. Eleven Participating Jurisdictions have met all five elements under this Recommendation, which covers specific custody and safekeeping disclosure requirements for CASPs. Notwithstanding, not every local framework provides for the same level of granularity when it comes to these disclosure requirements. One jurisdiction has published draft implementation measures covering all key elements. Five Participating Jurisdictions partially fulfil this Recommendation, i.e. their framework meeting at least one of the five elements of the Recommendation. Three Participating Jurisdictions currently have not implemented any elements of this Recommendation, but some of them have further reforms underway.

Recommendation 15: Client Asset Reconciliation and Independent Assurance. Fourteen Participating Jurisdictions have fully implemented this Recommendation. While three of the Participating Jurisdictions do not have any legislation in force or finalized implementation measures related to this Recommendation, another three Participating Jurisdictions are currently in the process of drafting legislation. For one jurisdiction, there is no regulation in place when the crypto-asset does not classify as a financial product.

Recommendation 16: Securing client money and assets. Twelve Participating Jurisdictions have final implementation measures in force across the two key elements for this Recommendation. Gaps for this Recommendation exist largely where jurisdictions have limited or no frameworks that secure client money and assets.

Recommendation 18: Retail Client Appropriateness and Disclosure. Eight Participating Jurisdictions have fully implemented this Recommendation. Three Participating Jurisdictions have not implemented any of the key elements for the Recommendation. The elements of this Recommendation that were the most implemented across jurisdictions related to systems, policies and procedures for providing disclosures, particularly ongoing disclosures. In terms of challenges, regulations were often seen to lack requirements or clarity on the application of suitability or appropriateness tests when CASPs execute client orders.

Chapter 2 – Background

In 2023, IOSCO, under the stewardship of the Fintech Task Force (FTF), finalised two sets of policy recommendations focused on Crypto and Digital Asset Markets ("CDA Policy Recommendations") and Decentralized Finance Recommendations ("DeFi"), together with an Umbrella Note explaining the interaction between these two sets of Recommendations.

IOSCO's Implementation Roadmap

Considering the risk to investors and market integrity present in the crypto-asset markets, the IOSCO Board in December 2023 agreed that an IOSCO program to monitor and promote implementation of the CDA and DeFi Recommendations in a timely manner was necessary. This was set out in IOSCO's Crypto-Asset Implementation Roadmap which was approved by the Board in December 2023 ("Implementation Roadmap").

In its 2023-2024 Work Programme, the IOSCO Board prioritized a program to monitor and promote timely implementation of the CDA Policy Recommendations by IOSCO members and approved in December 2023 a multi-phase CDA Roadmap, in light of the global and fast evolving nature of crypto-asset markets, the risks of regulatory arbitrage due to uneven pace of regulation, and the risks of harm to which consumers and the market are being exposed.

The initial focus set out in the Implementation Roadmap was the assessment of implementation of the CDA Recommendations. This is mainly due to the more proximate risks to investor protection and market integrity posed by the growing size of the CDA markets and the increasing complexity and scale of centralised activities conducted by CASPs. The implementation work in this context aims to:

- Support public awareness of the initiatives being taken in jurisdictions to develop new domestic regulatory regimes where gaps exist or to supervise and enforce existing securities regulatory regimes (where appropriate);
- Encourage dialogue within and across Member Jurisdictions to focus on the issues raised by IOSCO's CDA Recommendations and work on steps forward, appropriate to each jurisdiction;
- Encourage Member Jurisdictions to move promptly towards meeting the CDA Recommendations, either through supervising and enforcing existing regimes, or where gaps exist, through developing new domestic regulatory regimes; and
- Complement the efforts of the FSB and the SSBs in delivering a global, holistic approach to regulation of CDA markets.

Under the first phase of the Implementation Roadmap, the IOSCO FTF conducted a stocktake in 2024 across Member Jurisdictions to understand the efforts made to implement the CDA Recommendations[4]. Following the finalisation of the Stocktake Note, the next phase of the

[4] This note was internal to IOSCO for the purpose of, amongst other things, providing input into this Thematic Review

Implementation Roadmap as agreed by IOSCO Board was to conduct a pilot Thematic Review in 2025, in coordination with the FSB.

IOSCO's Thematic Review

The Thematic Review is an initial pilot assessment of the CDA Recommendations. It aims to assess the progress made by a selected list of jurisdictions ("Participating Jurisdictions") in implementing a selected set of the CDA Recommendations, building on the findings of the 2024 Stocktake. The Thematic Review focused on the implementation of the Assessed Recommendations and their application to CDA markets in relation to crypto-assets generally. While the CDA Recommendations also apply to stablecoins, the development of regulatory frameworks in relation to stablecoins was a focus of the FSB Report and so not focused upon in this Report, although developments within the stablecoin market have been noted.

The list of Participating Jurisdictions includes certain FSB jurisdictions and selected non-FSB jurisdictions with material crypto-asset activity and takes into consideration the implementation progress, amount of crypto-asset activity, jurisdictional scope, and overall diversity of crypto-asset frameworks. The jurisdictions were selected on the basis of whether licenses, registrations, authorizations or equivalent have been issued by IOSCO members to CASPs with respect to regulatory frameworks that address investor protection and market integrity issues. The list of Participating Jurisdictions also reflects a diverse geographic representation.

Based on the initial analysis, ten CDA Recommendations were selected for this Thematic Review – primarily due to their focus of investor protection and market integrity that could result in significant investor harm. These 10 recommendations are as follows:

- Recommendation 2: Organizational Governance
- Recommendation 3: Disclosure of Role, Capacity and Trading Conflicts
- Recommendation 8: Fraud and Market Abuse
- Recommendation 11: Enhanced Regulatory Cooperation
- Recommendations 12 to 16: Custody of Client Monies and Assets
- Recommendation 18: Retail Client Appropriateness and Disclosure

See **Appendix 1** for the full list of the CDA Recommendations.

Based on the IOSCO Board approved Terms of Reference (ToR), the review focused on the progress made by Participating Jurisdictions in implementing the Assessed Recommendations, namely including –

- Key observations of the status of Participating Jurisdictions' implementation of the Assessed Recommendations, including potential gaps in implementation;

- A comparative analysis of Participating Jurisdictions' state of implementation of the Assessed Recommendations;

- A summary chart indicating the degrees of implementation for each Assessed Recommendation, in accordance with the agreed rating scale;

- A description of any challenges faced in developing and implementing reforms (including lessons learned as examples of current practices); and

- If appropriate, any recommendations identified by the RT on capacity building.

To ensure a risk-based approach when conducting the Review, the RT has also taken into account the latest market developments since the publication of the CDA Recommendations. The analysis and key findings of the Review will serve as material input in developing the full assessment methodology for the CDA Recommendations in 2026, for regular consistency assessments by IOSCO's Assessment Committee (AC) starting afterwards.

Coordination with the Financial Stability Board (FSB)

In parallel to IOSCO's efforts, the FSB has published its Report following a thematic peer review, assessing progress by FSB jurisdictions and some other jurisdictions who volunteered to participate, in implementing the FSB high-level recommendations for the regulation, supervision and oversight of crypto-asset markets and activities (CA recommendations) and revised high-level recommendations for the regulation, supervision and oversight of global stablecoin arrangements (GSCs) (GSC recommendations).

The FSB Global Regulatory Framework for Crypto-Asset Activities consists of high-level recommendations for the regulation, supervision and oversight of crypto-asset markets and activities and global stablecoin arrangements. The FSB Recommendations are aimed at ensuring that financial stability risks are considered at the heart of the development of regulatory frameworks for crypto-assets and stablecoins. The CDA Recommendations are a more detailed set of Recommendations, providing key features which IOSCO recommends that jurisdictions implement to regulate crypto-assets. The CDA Recommendations were designed to address investor protection and market integrity risks. The FSB and CDA Recommendations work together to provide a baseline of consistent regulation for crypto-asset markets across the membership base of each organisation. The Recommendations dovetail together and complement each other, with some crossover, in particular in relation to regulatory cooperation and information sharing.

To avoid duplication, ensure complementarity, and give a consistent and solid message globally, IOSCO and the FSB worked collaboratively in conducting their respective Reviews. In that regard, while the IOSCO Review focuses on investor protection and market integrity, the FSB Review focuses on financial stability, and also focuses on globally systemic stablecoins.

With a focus on ensuring the Reviews give a more complete picture of the status of development and implementation of regulatory frameworks to address CDA risks, there was cooperation and coordination between the RT leadership, the secretariats, and the review teams themselves. This was important to ensure consistency in assessments of jurisdictions which are covered by the two Reports as well as for common themes for assessment (e.g. cross-border cooperation).

Similarly to the findings set out in this Report, the FSB Report concluded that notable progress has been made in implementing the FSB Global Regulatory Framework for Crypto-asset Activities; however, the implementation remains incomplete. Likewise, this Thematic Review concludes that there has been progress made in implementing regulatory frameworks addressing the key features of the Assessed Recommendations. However, as noted in the FSB

Report, the divergence of regulatory approaches has highlighted concerns around increased opportunities for regulatory arbitrage and complication, in an already complex landscape. Given the developing nature of the markets, neither report considered the effectiveness of the regulatory regimes, although consideration was given to progress of designing and implementing supervision and enforcement.

The difference of approaches to similar risks has been highlighted in the FSB Report which also notes that regulatory divergences not only heighten the risk of regulatory arbitrage but also pose challenges to global financial stability.

Both reports have considered in detail regulatory cooperation and information sharing, with similar conclusions that, although some regulatory mechanisms are in place to enable information sharing, these are not sufficiently covering all of the regulatory cycle activities, consistent with the fact that regulatory frameworks are still emerging. The FSB Report also highlights the importance for domestic cooperation amongst regulators who cover different aspects of the crypto-asset markets, whereas this Report focuses on international information sharing, which is the scope of IOSCO Recommendation 11. Both reports conclude that more needs to be done in this area, as well as exploring whether new and/or crypto-specific mechanisms would solve some of the identified gaps and challenges.

In conclusion, both IOSCO and FSB Reports highlight a call to action to all jurisdictions, to address the risks and opportunities for regulatory arbitrage and risks of financial stability, investor protection and market integrity by implementing all of the applicable Recommendations without delay.

Chapter 3 – Methodology

3.1 Scope of the Review

In line with the decisions by the IOSCO Board, the Review focused on the implementation of the following ten prioritised CDA Recommendations that are most directly relevant to investor protection and market integrity objectives:

- Recommendation 2: Organizational Governance
- Recommendation 3: Disclosure of Role, Capacity and Trading Conflicts
- Recommendation 8: Fraud and Market Abuse
- Recommendation 11: Enhanced Regulatory Cooperation
- Recommendations 12 to 16: Custody of Client Monies and Assets
- Recommendation 18: Retail Client Appropriateness and Disclosure

3.2 Participating Jurisdictions

Participating Jurisdictions were selected based on evidence of registering, licensing or authorising of major CASPs by IOSCO Members Jurisdictions with respect to their investor protection and market integrity frameworks and associated cross-border activities. In addition, the final list of jurisdictions sought to achieve diverse geographic representation.

Twenty IOSCO Member Jurisdictions have taken part in this Review: Abu Dhabi, AIFC[5] Astana, Australia, Bahamas, Bermuda, Brazil, Canada[6], France, Georgia, Gibraltar, Hong Kong, Japan, Republic of Korea, Liechtenstein, Malta, South Africa, Singapore, Switzerland, Thailand and the United Kingdom.[7]

3.3 Review Team

The Review has been conducted by a Review Team (RT). The RT is composed of experts from both the FTF and AC from the following IOSCO members: ASIC Australia, CVM Brazil, AMF France, BaFin Germany, SFC Hong Kong, Central Bank of Ireland, Consob Italy, CSSF Luxembourg, AMMC Morocco, MAS Singapore, UK FCA, U.S. CFTC, U.S. SEC, the International

[5] Astana International Financial Centre.

[6] Responses provided by the Autorité des marchés financiers (Quebec) and the Ontario Securities Commission.

[7] Of these 20 IOSCO Member Jurisdictions, nine of them are not FSB members. They are: Abu Dhabi, AIFC Astana, Bahamas, Bermuda, Georgia, Gibraltar, Liechtenstein, Malta, and Thailand.

Monetary Fund, and the World Bank. The RT is co-led by Laurent van Burik, CSSF Luxembourg and AC Chair, and Matthew Long, UK FCA and FTF Implementation Working Group (IWG) Chair.

3.4 Review Approach and Rating Scale

The main objective of this Thematic Review was to assess the progress made by the Participating Jurisdictions as of **31 July 2025** in implementing the Assessed Recommendations, including identifying gaps in implementation, as well as to identify examples of lessons learned and areas where capacity building efforts could be directed. The Review seeks to identify differences in approach to, and in progress of, implementation, or proposed implementation, of regulatory reforms, with commentary on the drivers for these differences.

The Review also took into account global market and regulatory developments since the publication of the CDA Recommendations.

Participating Jurisdictions provided a self-assessment on their regulatory approach to the subset of Assessed Recommendations. The Review does not fully assess the consistency of implementation measures against the CDA Recommendations, and compliance with a subset of the CDA Recommendations does not suggest compliance with all CDA Recommendations. It does reflect on, among other things, the adoption of reforms and the timeliness of these reforms. The assessment methodology identified the key elements for assessing each Recommendation within the scope of the Review. Twenty Participating Jurisdictions are assessed based on the following scale for each Assessed Recommendation:

Final implementation measures in force	Jurisdiction has taken steps in implementing all elements of the Assessed Recommendation and respective measures are in force
Final implementation measures published, but not in force	Jurisdiction has taken steps in implementing all elements of the Assessed Recommendation and respective measures have been published but are yet to be in force
Draft implementation measures published	Jurisdiction has taken initial steps, e.g. discussion papers on regulations, in implementing all elements of the Assessed Recommendation and respective measures have been drafted but are yet to be finalized or in force
Draft implementation measures not published	No steps have been taken to implement at least one of the key elements of the Assessed Recommendation
Not Applicable	No implementation measures undertaken given the nature of the CDA market and/or relevant structural, legal and institutional considerations.

Given the status of implementation of the CDA Recommendations, ratings have been applied in relation to the least developed area of implementation for the relevant Recommendation

(i.e., if there are four key elements within a Recommendation, then the rating reflects the least progressed element of the Recommendation). This is reflected in the following annotations:

(i) a black triangle (▲) to indicate where a Participating Jurisdiction has further reforms underway.

(ii) a white diamond (◊) to indicate that implementation of key elements of the Recommendation is at different stages. As the rating is based on the least progressed element, a white diamond (◊) also means that at least one key element is more advanced.

(iii) a black triangle and a white diamond (▲◊) to indicate that further reforms are underway, that implementation of the key elements of the Recommendation are at different stages, and the rating is for the least progressed element.

For each of the elements of implementation, proposed or additional reforms underway have been noted. As much as possible and to avoid duplication of efforts, the RT has taken into account the responses received from Participating Jurisdictions to the initial FTF Stocktake as well as subsequent relevant updates and additional information.

The Thematic Review has been conducted as a desktop review based on responses provided by the Participating Jurisdictions. The RT has provided Participating Jurisdictions with an opportunity to fact-check and ensure the accuracy of the conclusions drawn by the RT and/or of any relevant reference in the Report before being submitted to the IOSCO Board for approval.

The RT has considered the EU-wide legislation Markets in Crypto-Assets Regulation (MICAR) and Digital Operational Resilience Act (DORA) for all EU and EEA Participating Jurisdictions.

Chapter 4 – Overview of developments in the Crypto and Digital Asset Markets

4.1 Current Crypto and Digital Asset Markets[8]

Crypto-asset activities

Since the collapse of FTX and the crypto winter in 2022/2023, crypto-asset markets have increased in size. On-chain blockchain analysis indicates that global adoption of crypto-assets continues to grow in 2025. As of 31 July 2025, there was a market cap of USD 3.9tn. There has been an increased momentum to bring in crypto-assets (including the issuance of stablecoins) legislation, instead of relying on existing financial services legislation designed for traditional financial instruments such as securities, derivatives or payments, in regions or jurisdictions in which there is significant crypto-asset activities.

Stablecoins

Similarly, the scale of stablecoin activity has also increased since the adoption of the CDA Recommendations. As of 31 July 2025, the market cap of stablecoins is approximately USD 262.3 billion[9]. The use of stablecoins has also become more diversified, from treasury management to being explored for retail payments, prompting the need for robust investor protection and market integrity measures to be in place. The ability to transfer stablecoins in near real time, with 24/7 settlement, potentially makes stablecoins an attractive means of payment and settlement. As regulatory frameworks and infrastructure develop, there is currently limited interoperability between stablecoins and fiat currencies.

As use cases and innovation develop, stablecoins may be widely adopted in both centralised and decentralised crypto-asset environment, as well as becoming integrated in traditional financial markets. Legislative and regulatory frameworks need to develop to mitigate the risks posed by stablecoins, and to facilitate the potentially beneficial use cases and opportunities they present.

Financial Crime and Market Abuse

While the majority of crypto-asset use remains legitimate, illicit actors continue to make use of crypto-assets (including stablecoins) for financial crime purposes globally, ranging from

[8] This information derives from the original and updated responses to the FTF Stocktake.

[9] https://defillama.com/stablecoins

fraud, money laundering, market abuse to terrorist and proliferation financing as well as sanctions evasion. On-chain analysis indicated that the illicit use of crypto-assets has been on the rise, from an estimated value of USD 11 billion in 2020 to an estimated USD 53.1 billion in 2024. Due to their stabilising feature, stablecoins have become one of the most used crypto-assets for on-chain illicit activities between 2022 to 2024, overtaking bitcoin as the most commonly used crypto-asset in illicit activities.

Hacking and stolen funds, as well as scams, remain the key typologies of illicit finance involving crypto-assets. In terms of market abuse and manipulation, wash trading, pump and dump, and rug pulls continue to be the more prevalent typologies. Industry on-chain data has identified that suspected wash trading on blockchain may have accounted for up to USD 2.57billion in trading volume in 2024. In addition, among the more than two million tokens that were launched in the blockchain ecosystem in 2024, close to 4% of them were identified as having linkages to pump-and-dump schemes. Market abuse and manipulation is also witnessing an increasing uptake especially in DeFi exchanges (DEX). In light of these evolving trends and continued use of crypto-assets in market abuse and manipulation activities, jurisdictions will need to strengthen their regulatory frameworks to address risks to market integrity and investor protection, in addition to the introduction of anti-money laundering measures.

Operational Resilience

Given the 24/7 nature of crypto-asset activities, blockchain and ICT-related operational disruptions or failures can have major detrimental impact on the functioning of crypto-asset markets and could lead to serious customer harm and a negative impact on firms, such as the loss of funds or their value. The heavy reliance on wallets and the insufficient segregation or security of consumers' crypto-assets within the wallets, could also amplify the impact of cyberattacks, such as when poor access controls result in the loss or theft of consumer private keys, rendering assets (temporarily) inaccessible. As an example, in March 2025, the crypto-asset exchange ByBit was subject to a hack where crypto-assets of around USD 1.5 billion were stolen by illicit actors. A significant proportion of the stolen assets were later converted to unrecoverable funds. Furthermore, if stablecoins are used more frequently for payments or as an on/off ramp for other crypto-assets then stablecoin operational resilience failures could pose an increased risk of harm to consumers.

4.2 New Products and Emerging risks

As crypto-asset markets develop, we are seeing different business models emerging and crypto-assets being used or traded in different ways.

Staking

An example of this is staking, used in proof-of-stake blockchains, which is a process of locking up crypto-assets to support a blockchain validation and earn rewards in return. As of July 2025, the total value of staked assets on Ethereum reached USD 131.94 billion and those on

Solana protocol reached USD 78.61 billion globally.[10] There are various risks such as the inability to access holdings during validation process should there be volatility in the value of the staked crypto-assets, or risks of slashing[11].

Lending and borrowing

Crypto-assets lending and borrowing are other emerging business models. Crypto-asset lending is an arrangement where a crypto-asset lender transfers ownership of their assets to a third-party, typically a person, firm or platform. This transfer occurs under a contractual agreement which generally sets out that lenders will receive a yield, or reward, and an equivalent value of the assets transferred will be returned to them at the end of the lending arrangement. Crypto-asset borrowing refers to an arrangement in which a person, firm, or platform receives a loan in crypto-assets or fiat from a third-party firm, platform or person with an obligation for the crypto-asset borrower to pay back the loan and any associated fees or interest as per the contractual arrangement. The risks associated with crypto-asset borrowing and lending include liquidity management, counterparty risk, and the loss of assets should the relevant firm fail.

Artificial Intelligence

Artificial Intelligence (AI) is being deployed in relation to crypto-assets services. It is being used in trading and investment, with AI-powered trading bots analysing market data, identifying opportunities and executing trades automatically. AI is being used to automate the execution of smart contracts based on predefined rules and conditions, making the trade more efficient and contributing also to broader DeFi use. AI is also being used in fraud detection – with AI identifying unusual patterns and behaviours in transactions, as well as analysing smart contracts for vulnerabilities and potential exploits. However, AI is also being used for nefarious purposes, with AI scams such as deepfakes and phishing bots being prevalent.

[10] Top Proof of Stake Tokens | Staking Rewards (As of 22 July 2025)

[11] Slashing is a financial penalty applied to crypto-assets that have been locked up for staking, when a validator fails to meet certified pre-defined staking requirements, or behaves dishonestly in a way that negatively affects the blockchain. This will result in losing some or all of the staked crypto-assets, incurring financial loss.

Chapter 5 – Findings and Observations

Overview of Findings

In general, the Participating Jurisdictions have progressed significantly in the implementation of the CDA Recommendations and since the 2024 Stocktake. As of Q2 2024, 63% of all the jurisdictions surveyed in the 2024 Stocktake submitted that they regulated crypto-asset activities (33% fully, 30% partially), while an additional 18% were in the process of developing regulatory regimes. Among the 20 Participating Jurisdictions in the 2025 CDA Thematic Review, 8 reported that they fully regulate crypto-asset activities (40%).[12]

The majority of the Participating Jurisdictions have further reforms underway. While some have adapted existing legislation to CASPs, others have introduced new regulations for this area. Both scenarios present challenges, namely on scope of coverage for crypto-assets. Although not forming part of the Participating Jurisdictions, some jurisdictions have maintained bans on crypto-asset activities.

Some Participating Jurisdictions that have made progress in developing a framework for crypto-assets have adopted an approach that allows them to refine and update their procedures and decision-making frameworks in light of fast-moving market developments. This allows them to enhance their capacity to apply risk-based measures with a view to supporting responsible innovation while ensuring effective and adaptive regulatory oversight.

The dashboard below represents the summary of the ratings for each Assessed Recommendation and for each Participating Jurisdiction. The ratings reflect the desk-based assessment of the RT using the information supplied by the relevant jurisdictions considering their regulatory framework as of **31 July 2025**, when compared against the key elements of the ten Assessed Recommendations.

In line with the Terms of Reference and Scope of this Review approved by the IOSCO Board, this Review does not include any assessment of the effectiveness of the application of the Assessed Recommendations, nor the effectiveness of the crypto-asset regulatory framework of the Participating Jurisdictions throughout the regulatory cycle of authorisation, supervision, and enforcement.

Participating Jurisdiction	Rec 2	Rec 3	Rec 8	Rec 11	Rec 12	Rec 13	Rec 14	Rec 15	Rec 16	Rec 18
Abu Dhabi	▲									◊

[12] Abu Dhabi, AIFC Astana, Bahamas, Bermuda, Gibraltar, Japan, Malta, Thailand.

AIFC Astana										
Australia	◊	▲	▲		▲◊	▲◊	▲◊	▲◊	▲◊	◊
Bahamas	▲◊	◊			◊				◊	◊
Bermuda										
Brazil	▲	▲◊	▲◊					▲		
Canada										
France										◊
Georgia		◊								
Gibraltar	◊	▲◊	▲		◊		◊			
Hong Kong										
Japan	◊		▲◊							
Korea, Republic of	▲	▲		◊			▲◊	▲◊	◊	
Liechtenstein										◊
Malta										◊
South Africa	▲◊	▲◊		◊	◊	◊	◊	▲	◊	◊
Singapore			▲◊							
Switzerland[13]	▲◊	▲◊	▲◊		◊	▲◊	▲	▲◊	◊	▲
Thailand							◊			
United Kingdom	◊	▲◊			▲	▲	▲	▲	▲	▲◊

	Final Implementation Measures in force
	Final Implementation Measures published, but not in force
	Draft implementation measures published
	Draft implementation measures not published
	Not Applicable

Given the status of implementation of the CDA Recommendations, ratings have been applied in relation to the least developed area of implementation for the relevant Recommendation (i.e., if there are four elements within a Recommendation, then the rating reflects the least progressed element of the Recommendation). This is reflected in the following annotations:

[13] Insofar as the offering of the crypto-assets fall within the regulatory scope of banks or financial institutions, the rules of banking regulation or financial institution regulation apply. Accordingly, the listed Recommendations are typically being met when such institutions engage in the offering of crypto-assets. Implementation measures to the extent not already implemented in the existing legal framework are expected to be published later in 2025, which might bring the rating to "Draft Implementation measures published".

(i) a black triangle (▲) to indicate where a Participating Jurisdiction has further reforms underway.

(ii) a white diamond (◊) to indicate that implementation of key elements of the Recommendation is at different stages. As the rating is based on the least progressed element, a white diamond (◊) also means that at least one key element is more advanced.

(iii) a black triangle and a white diamond (▲◊) to indicate that further reforms are underway, that implementation of the key elements of the Recommendation are at different stages, and the rating is for the least progressed element.

The Review's Key Findings are described in the following sections below.

5.1 Recommendation 2: Organizational Governance

Recommendation 2 (Organizational Governance): *Regulators should require a CASP to have effective governance and organizational arrangements, commensurate to its activities, including systems, policies and procedures that would, amongst other things, address conflicts of interest, including those arising from different activities conducted, and services provided, by a CASP or its affiliated entities. These conflicts should be effectively identified, managed and mitigated. A regulator should consider whether certain conflicts are sufficiently acute that they cannot be effectively mitigated, including through effective systems and controls, disclosure, or prohibited actions, and may require more robust measures such as legal segregation of functions and activities, as well as separate registration and regulation of certain activities and functions to address this Recommendation.*

Many CASPs typically engage in multiple functions and activities under "one roof" – including exchange services, operating a trading venue, brokerage, market-making and other proprietary trading, offering margin trading, custody, clearing, settlement, and services relating to lending and/or staking. These CASPs can be organised as a single legal entity or a closely affiliated group of legal entities that are part of a wider group structure, but are generally operated as if they are one legal entity. The Recommendation addresses potential conflicts arising from engaging in these activities and functions by setting out how the conflicts should be effectively identified, managed and mitigated through governance and organisational arrangements.

For the purpose of this Thematic Review, the RT considered the following key elements in their assessment, specifically whether the framework:

1. aligns with IOSCO Principle 31[14];

2. has effective governance and organizational arrangements, including systems, policies and procedures that address conflicts of interest, including those arising from different activities conducted, and services provided, by a CASP or its affiliated entities; and evaluates whether certain conflicts of interest require stricter measures if they cannot be effectively mitigated through effective systems and controls, disclosure and prohibited actions.

To be rated Fully Implemented, all of the above elements have to be demonstrated. Where the legal or regulatory framework in force covers only some of the above elements, the relevant rating of the least progressed element is reflected.

Key Findings

Overall Progress

All Participating Jurisdictions have made progress, in varying degrees, in implementing this Recommendation. Among the 20 assessed jurisdictions 10[15] have put in place relevant requirements that are already operating. Notwithstanding, one of these jurisdictions[16] is still proposing to introduce different additional measures in their existing framework to further enhance CASPs' governance and organisational requirements.

For the 10 remaining jurisdictions, two of them[17] are in the process of consulting on their draft framework, and eight of them[18] have started looking at new measures that implement this Recommendation, but they have not published implementation measures yet or there are gaps.

[14] Market intermediaries should be required to establish an internal function that delivers compliance with standards for internal organisation and operational conduct, with the aim of protecting the interests of clients and their assets and ensuring proper management of risk, through which management of the intermediary accepts primary responsibility for these matters.

[15] Abu Dhabi, AIFC Astana, Bermuda, Canada, France, Hong Kong, Liechtenstein, Malta, Singapore, Thailand.

[16] Abu Dhabi.

[17] Australia and United Kingdom.

[18] Bahamas, Brazil, Gibraltar, Georgia, Japan, Republic of Korea, South Africa, Switzerland.

Regarding the eight Participating Jurisdictions that have thus been rated as not having published implementation measures, for five of them[19] this rating reflects the least progressed element, even though other elements of Recommendation 2 are met[20].

These governance and organisational arrangements generally include requirements related to firms' management board members to be of good repute and have appropriate knowledge, skills and experience, responsibilities and qualifications of senior management and functions of governing bodies, policies and procedures relating to protecting the interests of clients and their assets, and systems and control measures such as anti-money laundering, operational resilience, record-keeping.

Risk of conflicts of interest

Some Participating Jurisdictions consider the following situations where risks of conflicts of interest will increase:

- firms offering a wide range of both centralized and de-centralized crypto-asset services, where there are interactions between group entities when providing crypto-asset services;

- firms that handle token issuance, trading, and settlement are also involved in certain activities (such as lending, borrowing and staking) that give rise to conflicts of interest. The operational complexity of these activities and the potential misalignment of interests between service providers and customers entail risks. For example, crypto lending and borrowing can create conflicts between lenders, borrowers, and the platform itself - especially if the contractual terms are not transparent or if the platform engages in proprietary trading or rehypothecation of client assets.

Additional crypto-asset activity-measures to address conflicts of interest

Across various activities, Participating Jurisdictions[21] considered that staking (particularly delegated staking business models) could pose risks of conflicts of interest. For example, a service provider may both safeguard clients' assets and engage in the staking validation

[19] Bahamas, Gibraltar, Japan, South Africa, Switzerland.

[20] For example, the Bahamas Commission is currently in the process of amending the DARE Act for the purposes of addressing any legislative gaps, ambiguities and procedural concerns with the legislation. In particular, the DARE Bill will explicitly establish standards for addressing conflicts of interests and connected third party relationships. Japan does permit CASPs to operate under vertically integrated models. While the framework includes general obligations to manage conflicts of interest, including those between internal divisions and related entities, it does not explicitly assess risks linked to vertical integration. There is no mention of restrictions on combining functions such as custody, trading, issuance, and advisory services within the same entity.

[21] Brazil, France, Hong Kong, Republic of Korea, South Africa.

process[22]. In this situation, there is a risk that the CASP prioritizes its own interests in validator selection, reward distribution, or the handling of network penalties (e.g. slashing), which may not align with the best interests of clients and create conflicts of interest.

Some jurisdictions, to a lesser extent, also cited lending and borrowing as another area of increased risks of conflicts of interest. In particular, such business models could lead to increased risks such as misappropriation of customer assets, liquidity risks, and unfair practices stemming from information asymmetries, thereby requiring more investment protection measures. Some jurisdictions have put in place[23] or are considering the additional risks arising from [24] staking and lending (Conflicts of interest not being the sole reason for jurisdictions to have staking or lending-specific measures). A few jurisdictions have specific measures, such as requiring staking-CASPs to comply with additional requirements related to internal controls, information disclosure, and operational risk, selection of blockchain protocol and third-party service providers.

Proprietary trading

Participating Jurisdictions have adopted a wide variety of approaches to mitigate and address conflicts caused by proprietary trading, generating a diversity of results. Specifically on proprietary trading, Participating Jurisdictions have different viewpoints as to whether such activity poses high risks and therefore require corresponding risk-based measures.

For those Participating Jurisdictions that have referenced and considered proprietary trading in traditional financial services and the crypto-asset sector, they tend to introduce measures such as restrictions to mitigate potential conflicts of interest. For example, one Participating Jurisdiction[25] is considering introducing rules to restrict crypto trading platforms from trading as principal against clients on its own platform, in a similar way to traditional financial services.

[22] For instance, in Brazil investment vehicle providers, particularly ETF providers, depend on qualified custodians for both safekeeping and staking operations. The same concentration pattern may develop in other jurisdictions. This creates a "walled garden" model where the custodian controls both the assets and validator operations, giving rise to conflicts of interest among others. In fact, validators can influence transaction ordering for additional profit (maximal extractable value, or MEV), and inconsistent MEV policies across custodians or validators could result in differing returns or exposure to non-compliant strategies. This introduces a new layer of potential conflicts, as ETF sponsors may not have full transparency or control over how MEV is managed.

[23] Bermuda, Hong Kong, Singapore, and Thailand. Georgia has addressed the additional risk by implementing a strict prohibition of staking. In the case of EU/EEA jurisdictions staking itself is not prohibited under the EU Regulation on crypto-assets MICAR and does not require specific licensing. However, when staking services are provided by intermediaries (staking-as-a-service), they are considered ancillary to custody services. This means that the service provider must be authorized under MICAR to provide custody and administration of crypto-assets on behalf of clients. Staking service providers must comply with MICAR's requirements for custody and administration, including asset segregation, risk minimization, and liability for loss of crypto-assets.

[24] Abu Dhabi, Republic of Korea, South Africa, and the United Kingdom.

[25] United Kingdom

In another group of jurisdictions[26], CASPs operating a trading platform for crypto-assets should not deal on own account on the trading platform for crypto-assets they operate, including where they provide the exchange of crypto-assets for funds or other crypto-assets. In addition, CASPs operating a trading platform for crypto-assets may only be allowed to engage in matched principal trading where the client has consented to that process. With respect to enforcement powers, administrative measures are foreseen against any member of the management body of a CASP or any other natural person who is held responsible for the infringement, from dealing on own account. Others[27] are monitoring the situation to determine whether and how to address such risks.

Different approaches have been identified to regulate proprietary trading. Some Participating Jurisdictions strictly prohibit CASPs, under the current or future framework, from engaging in proprietary trading on their own platform while other jurisdictions allow proprietary trading subject to policies and procedures effective enough to manage and mitigate conflicts of interest that may arise from various business activities, such as functional segregation.

The RT notes the different approaches adopted by Participating Jurisdictions in mitigating conflicts arising from proprietary trading. While some jurisdictions have introduced or are considering outright bans on CASPs engaging in proprietary trading on their own platforms, others permit the activity conditional upon stringent governance, disclosure, and conflict management requirements. A minority of jurisdictions have in place principle-based requirements and do not impose stricter measures for proprietary trading. Any such activity is subject to case-by-case risk assessment, and the entity's ability to demonstrate that conflicts of interest are appropriately managed should be enforced during both licensing and ongoing supervision[28].

The RT is aware that the CDA Recommendations explicitly highlight proprietary trading as an area where conflicts of interest may be unmanageable within the CASP. In this context, the RT carefully considered whether the jurisdictional approaches in place or under development reflect a sufficient regulatory response to this identified risk. After assessing the measures in each jurisdiction, the RT concluded that the diversity of approaches, ranging from prohibition, to a risk-based mitigation approach, reflects different regulatory judgments about proportionality and market structure. Therefore, the RT did not classify the absence of a full prohibition on proprietary trading as a universal implementation gap, but instead evaluated

[26] EU/EEA jurisdictions covered under MICAR

[27] For example, Bahamas, Gibraltar, Republic of Korea, South Africa. With regard to Republic of Korea, the Virtual Asset User Protection Act, which primarily emphasizes safeguarding users rather than regulating Virtual Asset Service Providers (VASPs), does not establish a comprehensive framework for managing conflicts of interest among VASPs. Nevertheless, the Act explicitly prohibits VASPs and their affiliated individuals from trading crypto-assets they have issued.

[28] Bahamas, Gibraltar, Japan, South Africa. The conflict-of-interest risks are dealt with in terms of the current framework e.g. through governance, disclosure, and internal systems. The regulatory framework does not adequately tackle the conflicts of interest inherent in crypto-asset activities. E.g. it does not prohibit or condition proprietary trading.

whether jurisdictions have adopted appropriate measures, whether through restriction, enhanced governance requirements, or other controls, that are intended to address the underlying conflicts of interest that proprietary trading presents. Conversely, in relation to the case-by-case risk assessment approach, the RT has identified shortcomings in implementation, attributable to the absence of tangible evidence of supervisory or enforcement actions in relation to unmitigated conflict of interests.

Other observations

When a CASP performs multiple activities and functions in a crypto-asset trading environment, it is important for investors and regulators to understand the precise activities and functions that the CASP performs and the capacity in which it acts in relation to its clients. Many jurisdictions that responded require or will require disclosure on the matter under their existing or draft frameworks.

In addition, the RT explored the extent to which jurisdictions allow CASPs to engage in multiple functions under a vertically integrated model. Consistently with the findings outlined above, Participating Jurisdictions have mixed practices, ranging from a case-by-case basis, risk-based approach, to outright restriction. Some jurisdictions allow such operational models, while others impose specific measures such as restricting the operation of certain activities such as proprietary trading.

Emerging practices

- Some jurisdictions have very detailed rules, providing clear, objective and enforceable criteria, to address potential conflicts of interest. One example of this are rules that reach to shared company relationships and identity of board and director members, which provide for explicit criteria to drive implementation. For example, one Participating Jurisdiction[29] prohibits digital asset custodians from providing custody services to other digital asset business operators if there is a shareholding relationship where either party holds more than a specified percentage of shares. This measure aims to prevent structural conflicts of interest arising from ownership ties between the custodian and the other digital asset business operator. When a custodian holds a significant shareholding interest in a client (or vice versa), there is a risk that decisions about safeguarding client assets could be influenced by the financial or commercial interests of the affiliated entity. This could undermine the custodian's independence, compromise the security of client assets, and create incentives for preferential treatment or riskier operational practices. By prohibiting such relationships, the jurisdiction promotes the independence of custodial functions and strengthens investor protection. This helps to preserve the integrity and impartiality of custody services.

[29] Thailand

- In order to prevent conflicts of interest for selling digital tokens through initial coin offering (ICO) portals, the jurisdiction has set a rule that ICO Portals are prohibited from having a control over token issuers, and issuers are likewise prohibited from holding shares in the ICO Portals [30]. Rather than focusing solely on functional independence, these rules primarily aim to prevent structural conflicts of interest arising from ownership or control ties between entities that could compromise neutrality in service provision and decision-making processes.

- Individuals responsible for screening token offerings must not also serve as directors or executives of the issuers. This requirement ensures impartiality and governance integrity in token offering processes, by preventing individuals responsible for screening token offerings from simultaneously serving as directors or executives of the issuers. It reduces the risk of conflicted approvals and strengthens investor protection.
- In one regulatory approach, where a regulated entity permits third-party providers to offer key services related to the digital enterprise, prohibition and/or deeper inquiry into conflict of interests (more criteria for participation and background on key individuals) among such vendors is appropriate.

Challenges and Gaps

Generally, the RT has not identified major gaps in the regulatory framework for governance across the Participating Jurisdictions. As in all other CDA Recommendations, the RT considers that the priority is for all jurisdictions to introduce and implement a framework.

Some Participating Jurisdictions consider that disclosure requirements alone may not be sufficient to enable regulators to identify and address all relevant conflicts of interest, particularly those that are structural or group-wide in nature. This challenge arises when CASPs operate within complex group structures, where affiliated entities may be engaged in different, and sometimes unregulated, crypto-asset activities across multiple jurisdictions. The regulatory status and activities of these group entities may not be transparent or readily known to all competent authorities involved. As a result, regulators may struggle to detect and supervise conflicts that arise from intra-group dealings, shared management, or common financial interests across entities. This creates a risk of “hidden” conflicts that remain outside the scope of regulatory oversight unless there is robust group-wide governance, reporting obligations, and information-sharing between relevant authorities. Addressing this challenge may require jurisdictions to adopt enhanced supervisory cooperation, broader conflict of interest rules that capture group relationships, or impose disclosure requirements that cover group-wide structures and activities.

[30] Rather than focusing solely on functional independence, these rules primarily aim to prevent structural conflicts of interest arising from ownership or control ties between entities that could compromise neutrality in service provision and decision-making processes.

Another challenge faced by jurisdictions is due to the difference and inconsistency of regulatory scopes. For example, while a CASP could provide multiple activities, with some covered in the regulatory regime (e.g. stablecoins) but not all (e.g. lending or staking, or DeFi activities), it is unclear whether conflicts of interest requirements would cover the potential conflicts for activities outside the regulatory regimes. If the requirements could not tailor for non-regulated activities, jurisdictions may find it difficult to supervise accordingly.

As observed from the responses by Participating Jurisdictions, some of the impediments to full implementation of this Recommendation include:

- Not having appropriate personnel and budget[31]
- Relying on the current framework in the absence of a specific crypto-assets regulation:
    - Insofar as the offering of the crypto-assets fall within the regulatory scope of banks or financial institutions, the rules of banking regulation or financial institution regulation apply[32].
    - Integrating crypto-assets into existing financial market regulatory frameworks falls short of addressing conflicts of interest specific to crypto-asset activities, such as those arising when CASPs operate multiple functions[33].
    - The current regime covers only VASP registration and AML/CFT requirements[34].
- Pending regulatory review or further regulatory is underway:
    - In one jurisdiction regulatory development to include requirements for CASPs to implement a clear and effective governance framework or organisational arrangements, to move away from the approach of self-regulation[35].

[31] Decree No. 11,563 of 13 June 2023 designates the Central Bank of Brazil as the authority responsible for regulating, authorising and supervising CASPs, while the Brazilian Securities and Exchange Commission (CVM) is responsible for regulating the issuance and offering of crypto-assets whenever they are considered securities, pursuant to Law No. 6,385 of 1976.

[32] Switzerland

[33] For example, there are no specific and explicit rules and requirements around crypto-asset/token issuance, trading and listing under the FAIS Act in South Africa.

[34] Georgia

[35] Republic of Korea

5.2 Recommendation 3: Disclosure of Role, Capacity and Trading Conflicts

Recommendation 3 (Disclosure of Role, Capacity and Trading conflicts): *Regulators should require a CASP to have accurately disclosed each role and capacity in which it is acting at all times. These disclosures should be made in plain, concise, nontechnical language, as relevant to the CASP's clients, prospective clients, the general public, and regulators in all jurisdictions where the CASP operates, and into which it provides services. Relevant disclosures should take place prior to entering into an agreement with a prospective client to provide services, and at any point thereafter when such position changes (e.g., if and when the CASP takes on a new, or different, role or capacity).*

If a CASP is engaging in different activities and functions in a crypto-asset trading environment, it is important for investors and regulators to understand the precise activities and functions that the CASP is providing, and in what capacity it is acting, in relation to its clients. The vertical integration and aggregation of different activities and roles of CASPs makes this issue more acute.

If permitted to perform multiple functions in a vertically integrated manner, a CASP should identify and disclose the conflicts encountered when acting in multiple capacities, the policies and procedures to prevent or mitigate such conflicts, and the risks to clients arising from the vertically integrated operations.

In view of the novel nature of crypto-assets, and especially when such activities may not necessarily have a direct equivalent activity in traditional financial markets, some regulators have adopted an approach of requiring more information from the sector.

For the purposes of this review, the RT considered the following three key elements when assessing the Participating Jurisdictions' frameworks, specifically whether jurisdictions require a CASP to: –

- Disclose information regarding conflicts of interest;
- Disclose information regarding role and capacity to the public and/or clients prior to entering into an agreement with prospective client, and at any point thereafter when such position changes;
- Notify regulators of information regarding role and capacity and make subsequent notification when such position changes.

To be rated Fully Implemented, the RT looked for affirmative and satisfactory responses to all of the above elements. Where the legal or regulatory framework in force covers only some of the above elements, the relevant rating of the least progressed element would be reflected.

Key Findings

Overall Progress

The majority of the Participating Jurisdictions have progressed in implementing this Recommendation. Among them, 11[36] have put in place various degrees of disclosure requirements relating to role, capacity and trading conflicts. Seven[37] jurisdictions have new regimes or developments underway to supplement their existing regulatory frameworks, of which three jurisdictions[38] have published draft implementation measures. Three jurisdictions[39] meet two key elements, of which two jurisdictions meet the elements using their existing regimes and will have regulatory developments underway but the draft measures are yet to be published.

Disclosure relating to Role, Capacity, and Conflicts

- Role and capacity: Many Participating Jurisdictions require CASPs to disclose their roles and capacity, including the specific legal entity with whom the client is contracting, the specific services and activities that are being provided by the CASP, and the role of the CASP when handling or executing clients' orders (e.g., whether as a principal or agent)[40].
- Conflicts of Interest: Whilst most[41] Participating Jurisdictions require CASPs to disclose conflicts of interest, the specifics of what needs to be disclosed and how it should be managed can vary. For example, one jurisdiction[42] requires CASPs to provide detailed written disclosures including measures taken to avoid or mitigate conflicts; another[43] requires CASPs to disclose information on fees, the nature of transactions, and risks associated with transactions. Another jurisdiction[44] requires CASPs to clearly disclose the

[36] Abu Dhabi, AIFC Astana, Bermuda, Canada, France, Hong Kong, Japan, Liechtenstein, Malta, Singapore, Thailand

[37] Australia, Brazil, Gibraltar, Republic of Korea, South Africa, Switzerland, United Kingdom

[38] Australia, Brazil, United Kingdom

[39] Bahamas, South Africa, Switzerland

[40] Abu Dhabi, AIFC Astana, Australia, Bermuda, Brazil, Canada, France, Hong Kong, Japan, Liechtenstein, Malta, Singapore, South Africa, Thailand.

[41] Abu Dhabi, AIFC Astana, Australia, Bahamas, Bermuda, Brazil, Canada, France, Hong Kong, Japan, Liechtenstein, Malta, Singapore, South Africa, Switzerland, Thailand, and the United Kingdom.

[42] South Africa

[43] Japan

[44] Abu Dhabi

nature and sources of potential conflicts of interest to their clients before undertaking business whenever CASPs' arrangements to address Recommendation 2 are not sufficient.

- Material Interest Disclosure: Some jurisdictions specifically require CASPs to disclose any material interests they have in the crypto-assets they offer. For instance, one jurisdiction[45] requires CASPs (trading platform) to disclose on its website if it is affiliated with the issuer, and the management or development team (or any of its known key members) of the crypto-assets it offers. Another[46] requires CASPs to disclose their material interest or venture investment in any crypto-assets they offer. One jurisdiction[47] has prohibited CASPs from selling, purchasing, or trading crypto-assets issued by themselves or related parties. Where such assets are acquired due to unavoidable circumstances, the CASP must disclose certain information on its website such as the type, quantity, and value of the acquired crypto-assets, the reason for acquisition, the relationship with the related party, and the disposal plan.

Disclosure to the public and clients

- Public Disclosure: A large group of jurisdictions[48] in various regions have imposed requirements on CASPs to disclose certain information on their websites. This may include information about the risks associated with crypto-assets, any conflicts of interest and the CASP's regulatory status. One jurisdiction[49] has also put in place specific advertising-related disclosure on paid relationships and affiliated group companies promoting the business.
- Disclosure to clients: A large group of jurisdictions[50] require CASPs to enter into written client agreements before providing services. These agreements may include detailed information about the services provided and any potential conflicts of interest. A number of jurisdictions[51] have put in place requirements for CASPs to provide their clients with clear and comprehensive explanations of the nature and key terms of any contract or transaction.

Ongoing disclosure to the public and clients

[45] Hong Kong

[46] France (specifically the PACTE regime, which governed digital asset service providers prior to the entry into force of MICAR on 30 December 2024. In France, market participants who can demonstrate that they provided crypto-asset services in accordance with national law prior to this date may continue to do so until 1 July 2026.)

[47] Republic of Korea

[48] Abu Dhabi, AIFC Astana, Australia, Bahamas (for providing custody service only), Bermuda, Brazil, Canada, France, Hong Kong, Japan, Liechtenstein, Malta, Singapore, Thailand.

[49] Thailand

[50] Abu Dhabi, AIFC Astana, Bermuda, France, Hong Kong, Liechtenstein, Malta, Singapore.

[51] Abu Dhabi, Australia, France, Hong Kong, Japan, Liechtenstein, Malta, South Africa.

- Some jurisdictions[52] explicitly requires CASPs to make ongoing disclosures to the public and clients when information regarding the CASP's role and capacity changes, while others[53] may rely on high-level principles where appropriate.

Disclosure or Notification to Regulators

- Many jurisdictions[54] also have measures in place for CASPs to notify their regulators of their role and capacity and any subsequent changes to such information. One jurisdiction[55] requires CASPs to provide detailed information about any third parties involved in the provision of CASP services during the registration process. Another jurisdiction[56] is considering requiring CASPs to identify entities operating market making strategies on the platform and disclose legal, contractual, or commercial relationships.

Emerging practices

As most jurisdictions have progressed to implement disclosure requirements, some practices have started to emerge. These include:

- Clear disclosure requirements tailored to consumers, thereby promoting transparency and allowing consumers to make informed decisions. Some of this information are not only related to fees or market models, but also potential conflicts of interests, material interests CASPs have in the crypto-assets they offer, or nature of their transactions[57]. Additional disclosure of information such as product or activity-related restrictions imposed by regulators on CASPs, referral arrangements[58], and participation of contracted entities in the services and operations[59], provides another avenue to facilitate consumers making informed investment decisions.
- Additional disclosure for higher risk financial products such as crypto derivatives being subject to the OTC trade reporting requirements[60].

[52] Bermuda, Canada, France, Hong Kong, Liechtenstein, Malta, South Africa (regular update), Thailand.

[53] For example, Abu Dhabi, AIFC Astana, Japan, Singapore.

[54] Abu Dhabi, AIFC Astana, Bahamas, Bermuda, Brazil, Canada, France, Georgia, Hong Kong, Japan, Liechtenstein, Malta, Singapore, Switzerland, and Thailand.

[55] Georgia

[56] United Kingdom

[57] Hong Kong

[58] Canada

[59] Brazil

[60] Australia

- Having explicit requirements on ongoing disclosure to the public and/or clients when a CASP's role and capacity changes[61], ensuring CASPs provide investors with up-to-date information.
- Displaying plain and concise non-technical risk-related information on prominent location on websites, or ensuring risk warnings to be statically fixed and visible at the top of the screen even when a user scrolls up or down the webpage, and on each linked webpage on the website[62]. All these obligations to CASPs help support consumers making informed decisions.

These approaches enhance the accessibility, clarity, and visibility of critical information for retail investors, reducing the risk of investor misunderstanding or information asymmetry (for example from opaque business models or undisclosed conflict). By providing clear, tailored, and prominent disclosures—such as fixed risk warnings or detailed explanations of conflicts of interest—regulators help ensuring that investors can easily identify and assess key risks before they engage with CASPs.

Challenges and Gaps

Notwithstanding the approaches set out above, some key gaps are observed. These include inadequate conflict of interest management systems, variability in disclosure requirements, and a lack of requirements for ongoing disclosures.

- **Inadequate conflict of interest management systems**: Some jurisdictions only require the disclosure of one specific conflict[63] instead of all relevant conflicts, or do not require disclosure to clients[64]. This inconsistency can result in inadequate protection for investors and a lack of transparency in the operations of CASPs who might engage in regulatory arbitrage to exploit regulatory gaps regarding conflict-of-interest disclosure requirements.
- **Variability in Disclosure Requirements**: A few jurisdictions[65] do not mandate disclosures of role and capacity to clients. While the information may be provided to clients in practice, these jurisdictions may not be able to ensure that CASPs have accurately disclosed their roles and capacity. For other jurisdictions, the scope of the disclosure varies. For example, some jurisdictions[66] do not require the disclosure of the specific legal entity with whom the client is contracting, while a number of jurisdictions mandate comprehensive disclosures. Jurisdictions will need to consider the extent of information that requires disclosure.

[61] Bermuda, Canada, France, Hong Kong, Liechtenstein, Malta, Singapore, South Africa (regular update), Thailand.

[62] AIFC Astana

[63] Republic of Korea

[64] Georgia

[65] Bahamas, Georgia, Republic of Korea

[66] Bahamas, Georgia, Republic of Korea, United Kingdom

- **Lack of requirements on ongoing disclosure**: A few jurisdictions[67] do not have requirements covering ongoing disclosure. Without such requirements, investors may be using information which is no longer accurate thus affecting ability to make informed investment decision.

5.3 Recommendation 8: Fraud and Market Abuse

Recommendation 8 (Fraud and Market Abuse): *Regulators should bring enforcement actions against offences involving fraud and market abuse in crypto-asset markets, taking into consideration the extent to which they are not already covered by existing regulatory frameworks. These offences should cover all relevant fraudulent and abusive practices such as market manipulation, insider dealing and unlawful disclosure of inside information; money laundering / terrorist financing; issuing false and misleading statements; and misappropriation of funds.*

Crypto-assets can be used for fraudulent and abusive transactions in the same way, or in different ways, as traditional finance assets. Crypto-asset markets should be regulated in a manner consistent with the aim of preventing the same (as well as any idiosyncratic) types of fraudulent and manipulative practices that exist in traditional financial markets. Regulation of traditional financial markets prohibits abusive practices that undermine market integrity, and in some cases this regulation may cover certain fraudulent and abusive practices in crypto-asset markets.

For the purpose of this Thematic Review, the RT considered the following three key elements in their assessment, specifically:

- Existence of legal framework that allows for enforcement against offences in crypto-asset markets;
- Offences covered include all relevant fraudulent and abusive practices (such as market manipulation, insider dealing and unlawful disclosure of inside information, money laundering / terrorist financing, issuing false and misleading statements and misappropriation of funds);
- Consistency in regulation between crypto-asset markets and traditional markets to prevent fraud and market abuse.

The RT considered that relevant enforcement powers include legal powers to take actions on fraudulent and abusive practices, such as market manipulation, insider dealing and unlawful

[67] Bahamas, Brazil, Georgia, Republic of Korea, Switzerland

disclosure of inside information, money laundering and terrorist financing, issuing false and misleading information, and misappropriation of funds.

To be rated Fully Implemented, the RT looked for affirmative and satisfactory responses, indicating that all of the above elements have been implemented. Where the legal or regulatory framework in force covers only some of the above elements, the relevant rating of the least progressed element would be reflected.

Key Findings

Overall Progress

Among the 20 Participating Jurisdictions, 12[68] of them reported a full implementation of fraud and market abuse measures. Five jurisdictions[69] are on the path towards full implementation, having published draft measures but have yet to finalise their policies. Three jurisdictions[70] have not published any draft measures for at least one of the key elements. However, ongoing regulatory reforms are being contemplated by one of these jurisdictions[71], including in the area of market abuse.

Coverage of Fraud and Market Abuse Offences

The scope of Recommendation 8 is broad, and in certain jurisdictions, may not always rest with a single regulator. As mentioned above, for this Review, 5 forms of fraud and market abuse were considered - market manipulation, insider dealing and unlawful disclosure of inside information, money laundering / terrorist financing, issuing false and misleading statements and misappropriation of funds. Jurisdictions' coverage of these offences may not always be comprehensive, as they may prioritise implementation of these elements differently.

Given the money-laundering risks posed by crypto-assets, some jurisdictions have implemented AML/CFT regimes and have in place regulations against fraud while further consulting on other regulatory reforms such as in the areas of market manipulation and unlawful disclosure[72].

[68] Abu Dhabi, AIFC Astana, Bahamas, Bermuda, Canada, France, Gibraltar, Hong Kong, Liechtenstein, Malta, Republic of Korea, Thailand.

[69] Australia, Brazil, Japan, Singapore, United Kingdom.

[70] Georgia, South Africa, Switzerland.

[71] Switzerland

[72] For example, Australia, Singapore, and the United Kingdom.

Enforcement Actions

There is not much evidence that enforcement actions in relation to fraud and market abuse have been taken in Participating Jurisdictions. This may be because legislative and regulatory frameworks are new (even if fully implemented), and perpetrators of such offences may also reside cross-border.

Emerging practices

- ***Cross Platform Information Sharing***: One jurisdiction[73] will introduce measures to allow CASPs having the ability to engage in cross platform information sharing in cases of suspected market abuse. To ensure that there are no barriers to the sharing, the legislative framework will also be updated correspondingly. This information sharing mechanism will support broader market abuse enforcement efforts.

- ***Close collaboration with the industry***: One jurisdiction[74] proactively arranged training sessions for CASPs and shares expertise in market surveillance with them, in light of their lack of experience and expertise regarding market surveillance. Another form of collaboration is active engagement with the industry[75], to understand changes and development in the crypto eco-system, any novel risks that may emerge and take them into consideration in designing robust risk management systems and controls.

- ***Systematic mechanism for escalation and investigation***: One jurisdiction[76] has established a mechanism (consisting of a 3-step process) to investigate unfair trading practices in the crypto-asset markets: (1) CASP identifying and reporting abnormal transactions to the regulators, (2) the authorities conducting investigations of unfair trading practices; and (3) the authorities notifying violations identified during investigations to investigative agency and imposing penalty surcharges. Furthermore, in high-risk sectors, the authorities may self-report abnormal transactions through market monitoring systems and conduct investigations.

Challenges and Gaps

- ***Limits in enforcement authority***: Authorities may not have powers in relation to fraud and market abuse offences, as perpetrators of fraudulent and market abuse practices are more likely to be unlicensed entities, or even individuals. While most of the Participating Jurisdictions that were assessed as green for this Recommendation are

[73] United Kingdom

[74] Thailand

[75] Singapore and United Kingdom

[76] Republic of Korea

able to undertake enforcement actions against non-CASPs, one authority[77] is limited in its powers to CASPs only. In such a case, the authority would bring disciplinary action against the authorised CASPs and their senior management, instead of the offending party.[78]

5.4 Recommendation 11: Enhanced Regulatory Cooperation

Recommendation 11 (Enhanced Regulatory Cooperation): *Regulators, in recognition of the cross-border nature of crypto-asset issuance, trading, and other activities, should have the ability to share information and cooperate with regulators and relevant authorities in other jurisdictions with respect to such activities. This includes having available co-operation arrangements and/or other mechanisms to engage with regulators and relevant authorities in other jurisdictions. These should accommodate the authorization and on-going supervision of regulated CASPs, and enable broad assistance in enforcement investigations and related proceedings.*

Crypto-assets is a sector with a global footprint. Many CASPs, regardless of the size and scale of businesses, operate in different countries and service a highly geographical mobile client-base with cross-border trading activities. As jurisdictions progress to incorporate this new sector into their regulatory remit, often at different paces and with different types and degrees of regulation, businesses can take advantage of this, choosing a jurisdiction with lighter or no regulation in which to structure their operations. With this backdrop, cross-border cooperation and information is key. Recommendation 11 aims to provide a critical benchmark for IOSCO members to cooperate, coordinate and respond to cross-border challenges in enforcement and supervision, including regulatory arbitrage concerns, that arise from global crypto-asset activities conducted by CASPs that offer their services, often remotely, into multiple jurisdictions.

In this assessment, the RT considered the two following key elements with respect to Recommendation 11 and evaluated whether Participating Jurisdictions have:

[77] Bermuda

[78] Under the Digital Asset Business Act 2018, unlicensed crypto-asset activity constitutes a criminal offence. While the Bermuda Market Authority does not have administrative sanctioning powers over non-CASPs, such cases are referred to law enforcement authorities.

- the ability to share information cross-border, through a framework in place that provides a legal basis to exchange information with regulators and relevant authorities in other jurisdictions;
- available cooperation arrangements and/or other mechanisms, which should accommodate information sharing throughout the life cycle of regulated CASPs, including authorisation, on-going supervision and enforcement proceedings.

For the avoidance of doubt, the scope of this Recommendation focuses on international cooperation between authorities from different jurisdictions; it does not cover domestic cooperation between authorities within a single jurisdiction.

To be assessed as having final implementation measures in force, the Participating Jurisdiction must have both of these two key elements in place. Where only one of the above elements is covered, the relevant rating of the least progressed element would be reflected.

The RT is aware that many Participating Jurisdictions are still in the process of introducing their regulatory frameworks and that these regulatory frameworks have different scopes and coverage of crypto-assets and related activities. These jurisdictions where regulatory regimes are in progress have therefore not yet had an opportunity to use cooperation arrangements extensively, as they may not yet regulate the relevant activities. The assessment (including rating) is therefore solely based on whether there is legal authority for information sharing and an available information sharing cooperation mechanism in place to facilitate assistance for the authorization, on-going supervision and enforcement related proceedings of CASPs, and not on a mechanism's effective or frequent use.

One of the key tools for information sharing is the IOSCO Multilateral Memorandum of Understanding (MMoU) and/or Enhanced Multilateral Memorandum of Understanding (EMMoU). Signatories to these arrangements are expected to provide the "fullest assistance permissible" when being requested information. As of August 2025, the IOSCO MMoU has 130 signatories. Being an MMoU/EMMoU signatory gives strong assurance on a Participating Jurisdiction's ability to share information with other jurisdictions for enforcement purposes. Based on the application of the MMoU/EMMoU to-date, a small number of Participating Jurisdictions have also used these frameworks to request information to facilitate fit and proper assessments during authorisation stage. Therefore, and although these arrangements do not explicitly preclude any jurisdictions from sharing information as part of on-going supervision, in practice they are mainly used for enforcement purposes and, to some extent, for authorisation purposes.

That is why Recommendation 11 encourages regulators to take proactive bilateral or multilateral steps, such as cooperation mechanisms beyond the enforcement context. including, as appropriate, "supervisory colleges or networks, regional arrangements, or other forms of cross-jurisdictional cooperation, to support rigorous and effective ongoing supervision of CASPs operating across multiple jurisdictions".

The RT considered views of Participating Jurisdictions on whether there are other potential ways for regulators to pursue closer cross-border cooperation, on a recurring basis, and not only on investigation-related matters or on an informal basis, in light of the fast-evolving nature

of crypto-asset activities, considering practical perspectives and legal constraints. In addition, the RT analysed qualitative feedback from Participating Jurisdictions, which pointed to some challenges and barriers further described below.

Key Findings

Overall Progress

The RT found that all the Participating Jurisdictions have a framework for sharing information and at least one information sharing mechanism in place to share crypto-asset information, relying mostly on the existing IOSCO MMoU and EMMoU. The IOSCO MMoU and EMMoU provide a mechanism for supporting members to engage in cross-border cooperation for enforcement purposes and to some extent authorisation, and cover both securities and derivatives markets.

Nineteen (19) Participating Jurisdictions[79] have also put in place regional or bilateral arrangements in addition to the IOSCO MMoU/EMMoU- covering either supervisory information sharing at large, or innovation and fintech topics, which allow for information sharing about crypto-assets to some extent.

That said, the use of all of the information sharing arrangements remains fairly limited to date, considering that the crypto-asset sector is still a relatively new sector. Some Participating Jurisdictions wishing to share information with others have found that the varying regulatory approaches, for example different categorisation in different jurisdictions of crypto-assets as securities or payment instruments, and the pace of implementation of regimes across jurisdictions have added hurdles in cross-border information sharing. However, it should be noted that information sharing is not restricted to when regulatory frameworks are in place, and capacity building and information sharing would be appropriate even as regulatory frameworks across jurisdictions are being developed. As such, with the ongoing developments in the crypto-asset market, sharing of emerging practices and risks would also be of use.

When used, the IOSCO MMoU and EMMoU mainly address information sharing requests for enforcement-related purposes such as market abuse, with more limited evidence of use for day-to-day supervision matters such as considering licensing applications. Although most of the Participating Jurisdictions said they experienced no barriers when cooperating across borders and sharing regulatory information on crypto-asset firms, some highlighted specific barriers to cross-border cooperation, notably legal barriers because of differences in legal or regulatory classifications of crypto-assets or differences in competences. This issue has also been highlighted by the FSB Report.

[79] Abu Dhabi, AIFC Astana, Australia, Bahamas, Bermuda, Brazil, Canada, France, Georgia, Gibraltar, Hong Kong, Japan, Republic of Korea, Liechtenstein, Malta, Singapore, Switzerland, Thailand, United Kingdom. The Republic of Korea has indicated that a change in law would be required to exchange information on virtual asset service providers.

Participating Jurisdictions support enhanced cross-border information sharing and many were supportive of the establishment of specific supervisory information sharing arrangements such as regulatory colleges in order to facilitate information sharing and supervisory coordination in relation to regulated global crypto-asset firms.

Jurisdictions have in place cross-border cooperation mechanisms that cover enforcement and authorisation purposes but less so supervisory purposes

The RT found that a majority of the Participating Jurisdictions have a range of information sharing mechanisms in place to share crypto-asset information, relying mostly on the existing MMoU and EMMoU. Among the 20 Participating Jurisdictions, all of them are signatories to the MMoU and 13 of them to the EMMoU. Most of these are of the view that the MMoU and EMMoU are sufficiently flexible to remain relevant and effective in the face of changes in traditional markets, including when new products such as crypto-assets or services are introduced to the market. These jurisdictions also expect signatories to provide the fullest assistance possible while being cognizant of existing challenges. In that respect, three Participating Jurisdictions consider that the use of the IOSCO MMoU and EMMoU may be limited for cross-border cooperation related to crypto-assets because other jurisdictions retain a restrictive interpretation of their application to new products.

For those Participating Jurisdictions that indicated relying on a mechanism in addition to the IOSCO MMoU or EMMoU, these mechanisms are mainly regional ones (e.g. IOSCO's Asia-Pacific Regional Committee or EU). Half of the Participating Jurisdictions have also leveraged on existing bilateral frameworks in place[80], often those already established for traditional financial services, rather than creating new, bespoke, and dedicated arrangements for crypto-asset information sharing. A few Participating Jurisdictions considered that the scope of those bilateral arrangements, covering for instance fintech, are broad enough to address requests for crypto-asset related information sharing. On the contrary, one Participating Jurisdiction indicated that the use of bilateral MoUs may be constrained as well when they do not cover crypto-assets specifically.

The use of cross-border cooperation mechanisms is developing

Considering that the crypto-assets sector is a relatively new sector and many Participating Jurisdictions are still in the phase of developing or early implementation of their crypto-asset regulatory regimes, the use of cross-border cooperation mechanisms remains fairly limited. Even when regimes are in place, the RT has not seen evidence of regular co-operation and information sharing, with only a small amount of information being shared across borders.

[80] AIFC Astana, Bermuda, Brazil, Canada, France, Gibraltar, Hong Kong, Liechtenstein, Malta, United Kingdom.

Notably, only a small group of Participating Jurisdictions[81] have used mechanisms to share crypto-asset information in the past two years. The application is mostly for the purposes of investigation relating to market abuse, and with limited use on authorisation-related matters. Based on the received responses, there was no indication suggesting that cooperation or information sharing has taken place for the purposes of day-to-day supervision, or on a regular basis.

Most of the jurisdictions reported that they do not encounter difficulties when using the IOSCO MMoU and EMMoU. However, in the past two years, Participating Jurisdictions, on average, have made one or two requests a year. Therefore, the use of the IOSCO MMoU/EMMoU as information sharing tools for crypto-asset information is in early days.

Challenges to effective information sharing

The Participating Jurisdictions who experienced barriers to cross-border cooperation[82] have highlighted the following challenges to information sharing: legal barriers, differences in legal or regulatory classifications of crypto-assets (e.g., as securities or commodities) or differences in competences (which resulted in some requested authorities to deny assistance because they had no oversight over CASPs, or aspects of the CASPs business, in their jurisdiction). They also identified specific challenges related to the sharing of personal data.

The RT found that while the IOSCO MMoU/EMMoU provides a broad mechanism for jurisdictions to share some information, there are questions as to whether they can cover matters relating to stablecoins, which may not be regulated by the securities regulators who are signatories to the IOSCO MMoU/EMMoU. Although the RT notes that domestic cooperation is not covered by the Recommendation, Participating Jurisdictions recognize that strong and cohesive domestic cooperation amongst the various different competent authorities at the domestic level would be helpful. However, confidentiality safeguards under domestic arrangements would need to be considered and may affect the ability to onward share data.

Types of regulators	**Which crypto aspects their regulation may cover**	**Likely to be a signatory to the IOSCO MMoU/EMMoU**
Securities regulators	CASPs/securities-related crypto-asset activities	✓
Central banks/banking regulator	Stablecoin issuance and use	×

[81] Abu Dhabi, AIFC Astana, Bermuda, France, Gibraltar, Hong Kong and the United Kingdom indicated having sent information requests under the IOSCO MMoU/EMMoU or bilaterally over the past two years.

[82] Australia, Bermuda, Canada, France, Hong Kong, Japan, Republic of Korea, United Kingdom.

Payments regulators	Stablecoin use within payment systems	×
Derivatives regulators	CASPs/derivatives-related crypto-asset activities	✓
AML/CTF regulators	AML/CTF aspects of all crypto activities and stablecoins	×
Law enforcement	Criminal aspects of all crypto activities and stablecoins including financial crime, money laundering, market abuse and other offences	×
Integrated regulators	Multiple aspects	✓

This table sets out general types of regulators who have crypto-assets within their remit, and generally indicates whether they are likely to be a signatory to the IOSCO MMoU/EMMoU. There are exceptions, and there may also be regulators who fulfil multiple functions and may be IOSCO MMoU/EMMoU signatories even where such regulators generally are not IOSCO MMoU/EMMoU signatories.

Similarly, it is unclear for those jurisdictions relying on cooperation mechanisms developed for anti-money laundering purposes, whether the scope of sharing supports sharing other information, especially financial conduct-related information, about crypto-assets.

Some Participating Jurisdictions underscored the importance of minimizing the risk of regulatory arbitrage and the importance of using the tools available to each jurisdiction to share information across jurisdictions, to achieve, so far as possible, market integrity and investor protection (in particular in relation to investors solicited by unregistered CASPs that are operating abroad), and to mitigate risks of financial misconduct.

Looking ahead: potential enhancements to existing cooperation mechanisms

In connection with Recommendation 11, the CDA Recommendations encourage regulators to consider cooperation mechanisms beyond the enforcement context, as appropriate, such as supervisory colleges or networks, regional arrangements, or other forms of cross-jurisdictional cooperation, to support ongoing supervision of CASPs operating across multiple jurisdictions.

Many Participating Jurisdictions [83] expressed support for the establishment of supervisory/regulatory colleges in order to facilitate information sharing and supervisory coordination in relation to global crypto firms, while showing openness to set up a similar arrangement for authorisation of these firms. They indicated that supervisory/regulatory colleges could be useful to exchange information about supervisory practices, promote consistent oversight, facilitate timely information sharing and coordinate actions among regulators to accommodate cross-border implications and could serve as a crisis management coordination cell when appropriate. These jurisdictions were of the view that such forums would help address regulatory and supervisory arbitrages and allow regulators to get a holistic overview of a CASP group's activities.

Some of these jurisdictions stressed the importance of designing appropriate governance arrangements to cater for confidentiality issues, amongst other considerations. Some also suggested organising workshops and capacity building sessions to discuss challenges and solutions in a fast-moving environment.

Emerging practices

One regional initiative of the IOSCO membership is addressing the challenges of information sharing for on-going supervision matters. The Asia-Pacific Regional Committee of IOSCO has set up a Supervisory MMoU (SMMoU) allowing, and encouraging, signatories to consult and exchange of information related to supervisory activities to the fullest extent permissible, in accordance with their domestic laws and regulations.

The scope of the SMMoU, covering securities and derivatives markets, is flexible enough for jurisdictions to opt-in and to engage in supervisory cooperation on CASPs in the following areas: assistance as part of initial applications for authorisation, licensing or registration; on-going oversight and supervisory actions; assistance to organise on-site visits, etc. Beyond individual supervisory information, the SMMoU offers a framework to exchange information on emerging or potential risks, and issues of common interest given the increasing cross-border activities of global market players.

The regional APRC SMMoU addresses the issues and challenges related to oversight of global entities such as CASPs and signatories may consider leveraging the SMMoU to promote further information sharing as this industry grows in size and footprint. The APRC SMMoU is a regional initiative that covers only a limited number of jurisdictions[84] - but IOSCO members may wish to consider whether there may be an opportunity to expand this initiative to the larger IOSCO membership.

[83] Abu Dhabi, AIFC Astana, Australia, Bahamas, Bermuda, Canada, France, Georgia, Gibraltar, Hong Kong, South Africa, Thailand, United Kingdom. Brazil, Japan and Singapore also expressed support stressing scope and governance considerations.

[84] Among the Participating Jurisdictions, signatories of the APRC SMMoU are Australia, Hong Kong, Japan, Republic of Korea, Singapore and Thailand.

In the EU, information sharing among securities markets regulators that are members of ESMA is conducted under the ESMA Multilateral Memorandum of Understanding (MMoU) on the exchange of information and cooperation. This framework enables the exchange of confidential information between European authorities in relation to authorisation, supervision, and enforcement matters.

Challenges and Gaps

While all Participating Jurisdictions have put in place at least one cross-border cooperation mechanism, the focus remains quite narrow given the global nature of crypto-asset operations and presence of market-related events. As set out in Recommendation 11, available cross-border cooperation mechanisms should accommodate all stages of the regulatory cycle, including authorisation, supervision and enforcement.

Participating Jurisdictions generally have not identified fundamental data gaps when requesting information via established multilateral, regional or bilateral arrangements – in the context of investigation and enforcement purposes. That said, a few Participating Jurisdictions highlighted that differences in regulatory pace or frameworks – such as token perimeter, activities' scope, involvement of different or additional competent authorities – could impede cooperation because of a lack of legal authority.

More generally, beyond ad hoc requests, a few Participating Jurisdictions highlighted the benefit of a broader mechanism for cooperation and discussion, to get a holistic overview of CASP activities in order to better manage cross-border spillovers and understand interlinkages with traditional finance as well as to link up with jurisdictions that do not have a regulatory regime in place yet.

The RT recognises that this is a pilot review and as jurisdictions are still in the process of developing and implementing their regulatory frameworks for crypto-assets, cross-border cooperation and coordination will continue to evolve as part of ongoing implementation efforts. The Review Team encourages IOSCO and other SSBs to monitor development in the space and ensure that jurisdictions remove any barriers to information sharing related to crypto-assets in the enforcement, supervision or other regulatory contexts.

Jurisdictions should explore additional information sharing enhancements, both in terms of types of information shared as well as throughout the entire regulatory cycle including authorisation and supervision stages. With most major CASPs having a global footprint, there is an increasing need for considering additional enhancements to facilitate cross-border cooperation. The Review Team recommends that IOSCO explore such potential enhancements with, where relevant, other global standard setting bodies, such as the FSB and FATF, as well as other international organizations providing technical assistance to promote understanding of crypto-asset activities and regulatory requirements (such as the International Monetary Fund and the World Bank).

Potential enhancements to be considered could include exploration of:

- establishing informational resources (e.g. regulator directory, firm directory);

- creating new mechanisms for information sharing (e.g. forums for information exchange, data gaps workstreams, a global network for crypto-asset information sharing, regulatory colleges to focus on thematic topics of common concern and/or exchange of information in relation to on-going supervision or enforcement issues of specific crypto-assets service providers operating in several IOSCO member jurisdictions);
- updating existing, or introducing new formal frameworks, (e.g. establishing a multilateral mechanism for cooperation, in the form of a Supervisory Cooperation MMoU or a crypto-specific MMoU, or updating the existing IOSCO MMoU to cover crypto-assets explicitly).

5.5 Recommendation 12: Overarching Custody Recommendation

Recommendation 12 (Overarching Custody Recommendation): *Regulators should apply the IOSCO Recommendations Regarding the Protection of Client Assets when considering the application of existing frameworks, or New Frameworks, covering CASPs that hold or safeguard Client Assets.*

The proper custody of Client Assets is reliant on the strength of a CASP's systems, policies and procedures as well as the legal arrangements governing the custody relationship. Regulators should require a CASP to ensure that client assets are adequately protected at all times, including when placed with a third party chosen by the CASP, specifically aiming to minimize the risk of loss or misuse.

Recommendation 12 sets out that Regulators should apply the IOSCO Recommendations regarding the Protection of Client Assets for CASPs that hold or safeguard Client Assets. These Recommendations cover eight areas including the maintenance of accurate and up-to-date records, the provision of regular statements to clients, the maintenance of appropriate arrangements to safeguard the clients' rights in client assets, compliance with foreign regimes where applicable, clarity and transparency in the disclosure of the relevant client asset protection regimes, safeguards in the case where waiver or modification of degree of protection is applicable, intermediaries' compliance, and consideration of foreign information sources where applicable.

For the purposes of this Review, the RT considered the following three aspects[85] when assessing the Participating Jurisdictions' frameworks:

1. Regulators should set out expectations that the CASP maintains accurate and up-to-date records and accounts of client assets that readily establish the precise nature, amount, location and ownership status of Client Assets and the clients for whom the assets are held;
2. Regulators should require a CASP to ensure that client assets are adequately protected at all times, including when placed with a third party chosen by the CASP, specifically aiming to minimize the risk of loss or misuse;
3. Requirements on methods and structures to hold client assets should take into account risk management, liquidity and efficiency considerations and trade-offs.

To be assessed as having final implementation measures in force, a Participating Jurisdiction must have all of these three key elements in place. Where the legal or regulatory framework in force covers only some of the above elements, the relevant rating of the least progressed element is reflected.

Key Findings

Overall Progress

Twelve (12) of the 20 Participating Jurisdictions have final implementation measures in force[86]. These jurisdictions rely on a combination of existing frameworks – extended and/or amended to cover CASPs that hold or safeguard digital assets – and new frameworks.

Three Participating Jurisdictions[87] have published consultative implementation measures.

[85] These are a subset of the areas covered in the IOSCO Recommendations regarding the Protection of Client Assets. These aspects have been selected from those explicitly mentioned in the text of Recommendation 12. Other relevant aspects – e.g., segregation and reconciliation of client assets, disclosure of client asset protection regimes – are covered under Recommendations 13-15. Further operational and technological considerations are set out under Recommendation 17.

[86] Abu Dhabi, AIFC Astana, Bermuda, Canada, France, Hong Kong, Japan, Republic of Korea, Liechtenstein, Malta, Singapore, Thailand.

[87] Australia, Brazil and United Kingdom. In May 2025, the Financial Conduct Authority issued a consultation paper on Stablecoin Issuance and Cryptoasset Custody (CP25/14) covering accurate books and records, adequate organisational arrangements and private key management and security, among others. The Government of Australia consulted on a proposal to regulate digital asset platforms (DAPs) whereby the general approach to custody of financial products would be extended to digital assets. A legislative framework that will focus on the operators of DAPs is currently under development. In Brazil, Decree No. 11,563 of June 13, 2023, designated the Central Bank of Brazil as the authority responsible for regulating, authorizing, and supervising CASPs. In

Five Participating Jurisdictions have not published implementation measures[88] or have gaps[89] in one or more elements the RT assessed. In the latter case, the rating reflects the least progressed element, even though other elements of Recommendation 12 are met. For example, one jurisdiction[90] currently applies general financial services regulation to digital assets, which falls short of addressing requirements on methods and structures to hold client assets.

Three Participating Jurisdictions [91] among those that have published consultative implementation measures or have not published implementation measures indicated that the existing regulation applies insofar as crypto-assets/crypto-asset services fall within the regulatory scope of financial instruments/financial services.

Requirements to maintain accurate and up-to-date records and accounts of Client Assets

These requirements are broadly covered in the regulations across most Participating Jurisdictions, though responses reflect different levels of granularity as to the extent and type of information to be maintained – from a detailed breakdown of the type of information[92] to a general principle of comprehensive and up-to-date records[93]. In the latter cases, it was not possible to validate that the minimum scope required under Recommendation 12 is covered.

Use of third-parties

For the most part, regulations address the use of third parties in the context of custody of client assets, preventing the circumvention of custody rules by way of delegation arrangements. For the purposes of this Review, different approaches have been considered to meet expectations for the implementation of Recommendation 12, including restrictions on using third parties (eg. that are not authorized as custodians) and the application of outsourcing rules, whereby the principal remains accountable for the outsourced activities. Only three jurisdictions' responses explicitly cover the use of third-parties located abroad.

Requirements on methods and structures to hold client assets

November 2024, the Central Bank of Brazil published a proposal for regulating the provision of crypto-asset services including, inter alia, custody services. However, the information submitted by this Participating Jurisdiction has been limited.

[88] Georgia, Switzerland.

[89] Bahamas, Gibraltar, South Africa.

[90] South Africa

[91] Australia, Brazil, Switzerland.

[92] E.g., Japan, Singapore, jurisdictions covered under MICAR.

[93] Bahamas, Gibraltar.

For the purposes of this Thematic Review, methods and structures to hold client assets focus on measures for safeguarding private keys or means of access to digital assets[94]. Other aspects, including segregation and account structure, will be covered under Recommendation 13-16. More than half of the jurisdictions have adopted these measures. To varying extents, jurisdictions have adopted practices for key management/storage, including key management protocols, the use of advanced cryptographic techniques, multi-signature authorization, and offline storage[95]. In their responses, some Participating Jurisdictions[96] have not prescribed specific methods or structures, but have covered means of access as part of broader risk management systems, policies, procedures to protect customer assets against fraud, cyber threats or negligence that emphasize appropriate organisational arrangements, access controls, and cyber security.

Emerging practices

Regulations in one Participating Jurisdiction[97] set out detailed requirements on CASP records of client assets. Records should include, among others, the details of each transaction, whether client assets are held in individual accounts or pooled accounts, and the name of the provider(s) with whom the CASP maintains client assets. The same requirements on safeguarding of client assets apply to all licensed CASPs, irrespective of whether they hold client assets directly or engage a third-party provider. Regulations outline criteria against which the CASP must assess and, satisfy itself of, the suitability of the third-party provider. Where a CASP engages a third-party provider located outside of the jurisdiction, it must provide additional client disclosures. The framework assigns responsibilities and accountability to senior management, including to control movements of customers' assets stored in devices located outside the jurisdiction. CASPs are also required to have systems and controls to manage the risks in relation to the safeguarding of client assets, including requirements on the use of cold wallets (see also Recommendation 16).

As regards requirements on methods and structures to hold client assets, another Participating Jurisdiction[98] outlines the standards and requirements for Digital Asset Businesses (DABs) regarding the custody of client assets in its DAB Custody Code of Practice, covering a suite of technical and operational measures to protect private keys.

[94] Cryptographic keys providing access to crypto-assets are stored in an application or device referred to as "wallets". A "hot" wallet is connected to the internet and usually takes the form of software for the user, while a "cold" wallet is a hardware that is not connected to the internet and stores the cryptographic keys.

[95] IOSCO is not prescribing specific expectations or thresholds regarding, for example, the holding of crypto-asset private keys in "hot" vs "cold" vs "warm" wallets. Furthermore, non-custodial wallets are not considered under Recommendation 12.

[96] E.g., jurisdictions covered under MICAR.

[97] Singapore

[98] Bermuda

Finally, two jurisdictions[99] have indicated that, in certain circumstances, regulations prescribe the use of independent custodians[100] for a specified portion of total client assets held in custody (80% and 90%, respectively).

Challenges and Gaps

Some gaps have been identified both in existing (adapted) frameworks and in new frameworks. Overall, existing (adapted) regulatory frameworks have provided a good basis for the implementation of Recommendation 12. However, in some cases[101], these frameworks may fall short of recognizing the nature of crypto custody, related to the service provider's control of the private keys for the digital assets, and the need to secure those private keys. At the same time, similar gaps were found in one jurisdiction with a bespoke framework for crypto-assets[102] that lacks granularity, and only states a general principle of safekeeping of means of access.

The use and treatment of providers of custody services located in a foreign jurisdiction is not consistently covered across country responses. While this may be in part the result of restrictions or limitations, it could raise additional supervision challenges.

5.6 Recommendation 13: Segregation and Handling of Client Monies and Assets

Recommendation 13 - *Regulators should require a CASP to place Client Assets in trust, or to otherwise segregate them from the CASP's proprietary assets.*

Recommendation 13 seeks to provide CASP clients with legal certainty regarding protection of their crypto-assets, and to protect client assets against loss or misuse. It also ensures that these assets segregated as client assets would not be subject to the claims of the CASP's creditors, should the firm enter an insolvency process. This is important as the technological means by which crypto-assets are created and held are vastly different from traditional finance.

The RT considered the following key aspects when assessing Participating Jurisdictions' frameworks for Recommendation 13:

[99] Canada, Thailand

[100] See *Emerging practices* under Recommendation 2.

[101] E.g., South Africa.

[102] Bahamas.

1. Client assets are protected against any loss or misuse;
2. Client assets are required to be segregated from the proprietary assets of a CASP and placed in a trust or in segregated bankruptcy remote accounts and enforceability of the segregation mechanism in the event of insolvency of the CASP;
3. Clients are protected from a CASP expressly taking legal and/or beneficial title to Client Assets without clients' explicit prior consent to such arrangements.

To be rated Fully Implemented, the RT looked for compliance with all of the above three aspects. Where the legal or regulatory framework in force covers only some of the above elements, the relevant rating of the least progressed element would be reflected.

Key Findings

14 Participating Jurisdictions have final implementation measures in force[103]. Two Participating Jurisdictions[104] have draft implementation measures published that address all key elements of the Recommendation.

Four Participating jurisdictions[105] have not published implementation measures. However, in certain cases, the respective jurisdictions already meet one or two key elements of the Recommendation. Other Participating Jurisdictions have reforms underway whereas two jurisdictions seem not to have taken any measures to implement the Recommendation.

Cases of Participating Jurisdictions have implemented at least one key element of Recommendation 13 include:

- In one Participating Jurisdiction[106], the regulatory regime requires a CASP to adopt systems, policies and procedures to mitigate the risk of loss, theft, diminution or inaccessibility of assets a CASP holds or safeguards for its clients. Segregation requirements and safeguards against taking legal and/or beneficial ownership of the crypto-assets are not implemented.
- In another Participating Jurisdiction[107], under the current law, CASPs are required to segregate client assets from their own assets, so that client assets are in no way affected by a possible bankruptcy of the CASP. The two other key elements of this Recommendation are not covered but the forthcoming CASP regulation may provide for more specific obligations.

[103] Abu Dhabi, AIFC Astana, Bahamas, Bermuda, Canada, France, Gibraltar, Hong Kong, Japan, Republic of Korea, Liechtenstein, Malta, Singapore, Thailand.

[104] Australia, United Kingdom.

[105] Brazil, Georgia, South Africa, and Switzerland.

[106] South Africa

[107] Switzerland

- One jurisdiction[108] has partially implemented the current Recommendation to the extent where a crypto-asset is a financial product. In fact, they would already meet the key elements of Recommendation 13 under their existing regulatory framework. They have highlighted the application of the existing financial services regime (including custody requirements) to CASPs providing services in relation to crypto and digital assets that are financial products (which applies more broadly than similar concepts in other jurisdictions, such as other jurisdictions' definitions of securities or financial instruments). However, in the absence of clarity as to the interpretation of the notion of financial services vis-à-vis crypto-assets/crypto-asset services, the current framework may not cover the full scope of crypto-assets and CASPs that hold or safeguard client crypto-assets. Therefore, the current proposal sets out some draft implementation measures to extend the existing financial services framework to cover digital asset platforms (i.e., CASPs that hold custody of digital assets, whether or not the digital assets are financial products).

Emerging practices

Most of the Participating Jurisdictions have made considerable progress and have now met some or all the requirements of this Recommendation. A summary of the approaches of some Participating Jurisdictions to implement Recommendation 13 is set out in paragraphs below.

- Specific requirements for CASPs to establish a custody policy with internal rules and procedures to ensure the safekeeping or the control of such crypto-assets, or the means of access to the crypto-assets – with the objective and specific requirement for the custody policy to minimise the risk of loss of clients' crypto-assets or the rights related to those crypto-assets or the means of access to the crypto-assets due to fraud, cyber threats or negligence[109].
- Requiring CASPs to arrange both operational and legal segregation of client assets held in custody from their own assets. CASPs also need to ensure that the means of access to crypto-assets of their clients is clearly identified as such and that the necessary procedures are in place to return crypto-assets held on behalf of their clients, or the means of access, as soon as possible to those clients[110].
- CASPs are required to have adequate arrangements in place to safeguard the ownership rights of clients and prevent the use of clients' funds for their own account in cases where CASPs expressly taking legal and/or beneficial title to Client Assets[111].
- A CASP is required to have appropriate and effective procedures in place to protect the client assets from theft, fraud and other acts of misappropriation. Additionally, there are also various safeguards imposed on a CASP to protect the client assets. For example, a CASP is required to store 98% of client crypto-assets in cold storage except under limited circumstances permitted by the regulator on a case-by-case

[108] Australia

[109] EU MICAR Article 75 (3)

[110] EU MICAR Article 75 (7)

[111] EU MICAR Article 70 (1) and (2)

basis to minimise exposure to losses arising from a compromise or hacking of the platform[112].

- CASPs are required to segregate client assets from their own assets and, specifically, to hold client assets on trust for its clients through its associated entity which is a wholly owned subsidiary of the CASP. Additionally, in terms of liability, a CASP is required to have in place insurance or compensation arrangements approved by the regulator to cover potential loss of 50% of client crypto-assets in cold storage and 100% of client crypto-assets in hot and other storages held by its associated entity[113].
- One Participating Jurisdiction[114] has a slightly different approach to how client assets are protected against any loss or misuse as it appears that client assets are protected by insurance, with CASPs required to insure against any loss through a variety of predefined scenarios. The insurance coverage obtained by the CASP shall be sufficient to cover the loss of crypto-assets, whether held directly or indirectly through the CASP's custodians.

Challenges and Gaps

Since Recommendation 13 addresses a variety of custody elements, it is not uncommon that Participating Jurisdictions are still in the progress of introducing reform measures to ensure full implementation. Notwithstanding, the RT has not identified any major challenges to implementation.

Gaps within regulatory frameworks applicable to CASPs have only been identified for three Participating Jurisdictions [115] and they are all due to individual circumstances in the corresponding Participating Jurisdictions. That being said, some jurisdictions do not have any regulation in place that applies to the custody of crypto-assets.

[112] Hong Kong

[113] Hong Kong

[114] Canada

[115] South Africa and Switzerland.

5.7 Recommendation 14: Disclosure of Custody and Safekeeping Arrangements

Where a CASP is providing custody services to a client, regulators should require the CASP

> **Recommendation 14**: *Regulators should require a CASP to disclose, as relevant, in clear, concise and non-technical language to clients:*
>
> *i. How Client Assets are held, and the arrangements for safeguarding these assets and/or their private keys;*
> *ii. the use (if any) of an independent custodian, sub-custodian or related party custodian;*
> *iii. the extent to which Client Assets are aggregated or pooled within omnibus client accounts, the rights of individual clients with respect to the aggregated or pooled assets, and the risks of loss arising from any pooling or aggregating activities;*
> *iv. Risks arising from the CASP's handling or moving of Client Assets, whether directly or indirectly, such as through a cross-chain bridge; and*
> *v. Full and accurate information on the obligations and responsibilities of a CASP with respect to the use of Client Assets, as well as private keys, including the terms for their restitution, and on the risks involved.*

to clearly disclose, as relevant, all terms and conditions attached to the custodial activity being provided, such as the safeguards in place to provide for adequate protection of Client Assets from losses or insolvency of the CASP. Regulators also should require the CASP to identify how the CASP protects the Client Assets, including from the claims of the CASP's creditors. Where the CASP enters into a sub-custody arrangement with a third party, the disclosure should also detail the terms of these contractual arrangements and any additional risks that these might create for the client, as relevant.

When assessing Recommendation 14, the RT considered the following five elements in the Recommendation. Specifically, the disclosure of:

1. how client assets are held;
2. use of custodian;
3. extent to which client assets are pooled;
4. risks arising from CASP's handling or moving client assets; and
5. disclosure of obligations of CASPs with respect to use of client assets.

To be rated Fully Implemented, the RT looked for satisfactory responses with respect to all five elements. Where the legal or regulatory framework in force covers only some of the above elements, the relevant rating of the least progressed element would be reflected.

Key Findings

Overall Progress

Eleven Participating Jurisdictions[116] have final implementation measures in force, covering the five areas mentioned above while one jurisdiction[117] has published draft implementation measures covering all key elements.

Eight Participating Jurisdictions[118] have been rated as draft implementation measures not published, with five Participating Jurisdictions[119] being partially in line with this Recommendation since their framework meets at least one of the five elements described further above. The remaining three Participating Jurisdictions[120] of this group currently do not meet any elements of this Recommendation.

Further, four Participating Jurisdictions[121] have further reforms underway to be in line with this Recommendation.

Five Participating Jurisdictions have met at least one of the five elements described further above:

- The regulatory regime meets only points ii, iv and v of the elements under the disclosure requirements of Recommendation 14. The RT noted that the disclosure requirements remain quite high-level and do not specifically address custody of crypto-assets. However, they are currently undertaking legislative efforts to enact a comprehensive crypto-asset act, as detailed further below[122];
- The regulatory regime meets all elements of the disclosure requirements of Recommendation 14, except for point iii[123];

[116] Abu Dhabi, AIFC Astana, Bahamas, Bermuda, Canada, France, Hong Kong, Japan, Liechtenstein, Malta, Singapore.

[117] United Kingdom

[118] Australia, Brazil, Georgia, Gibraltar, Republic of Korea, South Africa, Switzerland, Thailand

[119] Australia, Gibraltar, Republic of Korea, South Africa, Thailand

[120] Brazil, Georgia, Switzerland

[121] Australia, Switzerland, Republic of Korea, United Kingdom

[122] Republic of Korea

[123] South Africa

- The regulatory regime only meets element iv of the disclosure requirements of Recommendation 14[124];
- The regulatory regime meets all elements of the disclosure requirements of Recommendation 14, except for point i. Even though there are quite extensive requirements on how those assets shall be held by CASPs (segregation, cold storage, etc.), there are no specific rules requiring CASPs to disclose to clients how those assets are held. Concerning key element iii, the RT understands that client assets can never be pooled or aggregated since client assets need to held separately for each client[125];
- One jurisdiction[126] has currently partially implemented elements i – iv of Recommendation 14. As explained under Recommendation 13, they have highlighted the application of the existing financial services regime (including custody requirements) to CASPs providing services in relation to crypto-assets that are financial products (which applies more broadly than similar concepts in other jurisdictions, such as other jurisdictions' definitions of securities or financial instruments).

There are some Participating Jurisdictions are currently working towards implementing a new/additional regulatory framework. This includes:

- The forthcoming regulatory regime of one Participating Jurisdiction[127] will extend the existing financial services framework to cover digital asset platforms. It will fully address points i – iv of the disclosure requirements of Recommendation 14. The RT understands that point v will not specifically be addressed but it would be for the individual service provider to assess if that information would be generally required to be disclosed to meet the requirements of the Participating Jurisdiction's Financial Services Guide.
- In another Participating Jurisdiction[128], as a general principle, the elements are governed by legislation if institutions provide financial services to investors. Financial market regulation is currently in the process of being revised[129], inter alia with respect to the offering of crypto-assets. A legislative proposal is expected in 2025. The points are expected to be addressed and regulated within the scope of this process. However, the results are not yet available.
- One Participating Jurisdiction[130] sets out its intentions and initial proposals in discussion and consultation papers. Whilst the detail of disclosures will be contained within subsequent papers, the intentions and what the disclosures will cover are contained within published discussion and consultation papers.

[124] Gibraltar

[125] Thailand

[126] Australia

[127] Australia

[128] Switzerland

[129] By the State Secretariat for International Finance

[130] United Kingdom

- One Participating Jurisdiction[131] is currently undertaking legislative efforts to enact a comprehensive crypto-asset act. This legislative process is being guided by the intention to align regulations with international standards, including the IOSCO CDA Recommendations, particularly concerning areas such as customer disclosure. It is anticipated that the finalised legislation will incorporate provisions designed to enhance transparency and investor protection.

Emerging practices

Most of the Participating Jurisdictions have made considerable progress and have now met some or all the requirements of this Recommendation. The Review Team has identified several approaches to implementing this Recommendation.

Below are some examples on how the regulatory frameworks address certain specific elements of custody related disclosure:

- Legislation provides for specific custody related disclosure requirements, such as (i) specific disclosure in writing to the customer before depositing any assets in the trust account; and (ii) disclosure of the terms and conditions that would apply to the safeguarding of the assets and the consequences for the customer in respect of the assets if the CASP becomes insolvent[132].
- Legislation provides for specific disclosure requirements for CASPs providing custody services, requiring CASPs providing custody and administration of crypto-assets on behalf of clients to conclude an agreement with their clients to specify their duties and their responsibilities. It is also defined what such agreement shall include at minimum (for instance a description of the security systems used by the crypto-asset service provider). Also, legislative or regulatory requirement includes requiring CASPs to establish a custody policy which shall be made available to clients (upon request)[133].

Challenges and Gaps

Recommendation 14 addresses disclosure requirements for CASPs providing crypto custody services. Those disclosure requirements as outlined in the box further above (points i-v) are precise and specific. As a result, not every local regulation will provide for the same level of granularity when it comes to disclosure requirements. However, general principles on disclosure might also include some of the more specific requirements set out above, subject to interpretation.

[131] Republic of Korea

[132] Singapore. Article 18D(e) and 18E of Payment Services Regulations 2019

[133] EU MICAR 75(1) and (3) or Hong Kong via paragraph 10.19 of Guidelines for Virtual Asset Trading Platform Operators

The RT has identified various gaps within regulatory frameworks applicable to CASPs for some Participating Jurisdictions [134], meaning that their regulatory framework addressed some disclosure requirements whereas other elements were missing. However, the RT could not identify any common gaps as the gaps were generally unique to specific jurisdictions.

Some jurisdictions do not have any regulation in place that require disclosure on the custody of crypto-assets.

5.8 Recommendation 15: Client Asset Reconciliation and Independent Assurance

> **Recommendation 15 (Client Asset Reconciliation and Independent Assurance)**: *Regulators should require a CASP to have systems, policies, and procedures to conduct regular and frequent reconciliations of Client Assets subject to appropriate independent assurance.*

To support Recommendation 15 on the Client Asset Reconciliation and Independent Assurance, a CASP should maintain appropriate books and records to track and record transactions and ownership of Client Assets. The CASP should conduct regular and frequent reconciliation of Client Assets on a client-by-client basis, to identify and resolve any discrepancies in a timely manner. In doing so, CASPs should also take into account both relevant off-chain and on-chain records. Regulators should require that each CASP implement measures to support reconciliations of Client Assets. Additionally, Regulators should have procedures to evaluate audits and independent reviews, investigate instances where these reviews contain qualifications and/or adverse findings, and take such action as they deem appropriate.

For the purposes of this Thematic Review, the RT focused on three aspects of implementation:

1. CASPs are required to implement measures to support frequent reconciliations of their client positions. Such reconciliations may be performed by the CASP itself or by a specialised third party appointed by the CASP.

2. The regulator has procedures to evaluate audits and independent reviews, investigate instances where these reviews contain qualifications and/or adverse findings, and take such action as they deem appropriate.

[134] Australia, Gibraltar, Republic of Korea, South Africa, Thailand.

3. CASPs are required to obtain independent assurance of their books and records at least on an annual basis.

Participating Jurisdictions were rated based on their responses to the above three elements. To be rated as fully implementing this Recommendation, the RT expected jurisdictions to have fully adopted enforceable rules or policies covering all of the three elements. Where the legal or regulatory framework in force covers only some of the above elements, the relevant rating of the least progressed element would be reflected.

Key Findings

Overall Progress

14 Participating Jurisdictions[135] reported having final implementation measures in force addressing both client asset reconciliation and independent assurance obligations under Recommendation 15.

Three Participating Jurisdictions[136] have partially implemented requirements of Recommendation 15 through legislation and three Jurisdictions[137] do not have any legislation into force or finalized implementation measures related to Recommendation 15. Three Participating Jurisdictions[138] are currently in the drafting process of a legislation. One Participating Jurisdiction[139] has already published the draft of the regulation in a consultation paper.

One jurisdiction[140] does have legislation requiring CASPs to have systems, policies, and procedures to conduct regular and frequent reconciliation, if the crypto-asset is considered a financial product under their Corporations Act. It also has procedures in place that enable authorities to obtain and evaluate audits/independent reviews but do not have a regulation for CASPs to obtain appropriate independent assurance on their books and records by an independent auditor as long as the crypto-asset is qualified as a financial product. There is no regulation in place if the crypto-asset does not classify as a financial product but the Participating Jurisdiction is proposing more regulation and already published a consultation paper on a framework for digital asset platforms. The situation is similar in another

[135] Abu Dhabi, AIFC Astana, Bahamas, Bermuda, Canada, France, Gibraltar, Hong Kong, Japan, Liechtenstein, Malta, Singapore, South Africa, Thailand.

[136] Australia, Republic of Korea, Switzerland.

[137] Brazil, Georgia, United Kingdom.

[138] Brazil, Switzerland, United Kingdom.

[139] United Kingdom

[140] Australia

jurisdiction[141]. Only crypto-asset services provided by banks are already regulated; stand-alone CASPs operate under AML-supervision only.

Client Asset Reconciliation

Fifteen Participating jurisdictions[142] have implemented measures which require CASPs to have systems, policies, and procedures to conduct regular and frequent reconciliation of Client Assets on a client-by-client basis in order to ensure the accuracy of its books and records at all times.

In one jurisdiction[143] digital asset businesses are required, generally, to conduct and provide reconciliation of assets held or safeguarded for their clients. While the legislation does not explicitly refer to systems, policies and procedures to conduct regular and frequent reconciliations, it does require that a digital asset business demonstrates that it has appropriate and sufficient systems and controls to perform its functions and manage its risks, and has implemented a framework design that addresses, inter alia, technology, security and governance.

One Participating Jurisdiction[144] proposed in its consultation paper that custodians carry out a qualifying crypto-asset reconciliation each business day. Firms will be required to check the total amount of each qualifying crypto-asset recorded in their client specific qualifying crypto-asset records against the content of the wallet addresses controlled by the firm and (where relevant) against any qualifying crypto-assets held by third parties. For the qualifying crypto-asset reconciliation to achieve this, the client specific qualifying crypto-asset records used in the reconciliation process must be maintained independently of any other information source used in the qualifying crypto-asset reconciliation. The qualifying crypto-asset custodians will be required to notify the regulator where they are unable to meet proposed reconciliation requirements or maintain accurate records.

Another Participating Jurisdiction[145] does not have any regulation in force covering client asset reconciliation. Another[146] has regulation in force on client asset reconciliation only for banks, which includes crypto services if the bank is offering those services. This jurisdiction is currently drafting a regulation for crypto custody business but does not have that a regulation

[141] Switzerland

[142] Abu Dhabi, AIFC Astana, Bahamas, Bermuda, Canada, France, Gibraltar, Hong Kong, Japan, Republic of Korea, Liechtenstein, Malta, Singapore, South Africa, Thailand.

[143] Bahamas

[144] United Kingdom

[145] Georgia

[146] Switzerland

in force now. Another jurisdiction[147] has client asset reconciliation for crypto-assets classified as financial instruments but beyond that there is no regulation in force.

There is no information about the client asset reconciliation in another jurisdiction[148], which although setting out that they have a regulatory framework have not provided further information.

Independent Assurance

Fourteen Participating jurisdictions[149] have procedures for their authorities to obtain and evaluate audits/independent reviews, and to take action as appropriate. In addition, those jurisdictions have a regulation for CASPs to obtain appropriate independent assurance on their books and records by an independent auditor. One Participating Jurisdiction[150] requires independent audits but provides no further information on how these audits are structured. The other six Participating Jurisdictions[151] assessed do not have (clear) regulation related to independent audits and procedures for their authorities.

- In one Participating Jurisdiction[152] CASPs do not have to mandate independent audits. Nevertheless, financial authorities may request information and conduct supervision and inspections to verify whether CASP complies with the law. If a CASP violates this Act or any dispositions under it, financial authorities may take corrective orders, suspend operations, notify investigative agencies, take enforcement against executives and employees, and impose fines. They have proposed specific regulation on independent audits in the next phase of crypto regulation, which is currently being developed.
- In another Participating Jurisdiction[153], CASPs should, only where the relevant crypto-assets are classified as a financial product, take the necessary steps to obtain a copy and consider an independent audit of the effectiveness of the controls of a third-party service organisation responsible for custody of assets.
- Another Participating Jurisdiction[154] has regulation for independent audits specifically in relation to anti-money laundering and is currently drafting regulation for custody services. Besides that, this Participating Jurisdiction has Recommendation 15 fulfilling

[147] Australia

[148] Brazil

[149] Abu Dhabi, AIFC Astana, Bahamas, Bermuda, Canada, France, Gibraltar, Hong Kong, Japan, Liechtenstein, Malta, Singapore, South Africa, Thailand.

[150] Gibraltar

[151] Australia, Brazil, Georgia, Republic of Korea, Switzerland, United Kingdom.

[152] Republic of Korea

[153] Australia

[154] Switzerland

regulation for banks into force, which include crypto services if the bank is offering those services.

- Another Participating Jurisdiction[155] is proposing for their regulatory regime to require completing an independent annual audit on their compliance with client asset rules.
- Another Participating Jurisdiction[156] does not have any independent assurance regulation into force.
- There is no information about independent assurance regulation in one Participating Jurisdiction[157].

Emerging practices

Most of the Participating Jurisdictions have made considerable progress and have now met all the requirements of Recommendation 15. Some jurisdictions have provided responses with detailed examples of a regulatory approach consistent with Recommendation 15[158]. The answers of these jurisdictions explained in detail the implemented regulations and how these regulations fulfil Recommendation 15.

Client Asset Reconciliation

One Participating Jurisdiction[159] provided detailed answers about their regulation on client asset reconciliation. A CASP must maintain adequate systems and controls to ensure accurate reconciliations of clients' crypto-assets are carried out at least every week. The CASP must ensure that the process of reconciliation does not give rise to a conflict of interest. The CASP must maintain a clear separation of duties to ensure that an employee with responsibility for operating client accounts must not perform the reconciliations. A reconciliation performed must be reviewed by a member of the CASP who has adequate seniority. The CASP must notify the regulator without undue delay where there have been material discrepancies with the reconciliation. The CASP must arrange for a third-party auditor's report on the CASP's compliance with the applicable safe custody rules, to be submitted to the Regulator on an annual basis[160].

In another Participating Jurisdiction[161], a CASP must conduct daily reconciliation of each crypto-asset balance it maintains for issuers and holders. A CASP providing custody must have appropriate rules, procedures, and controls, including robust accounting practices, to

[155] United Kingdom

[156] Georgia

[157] Brazil. Brazil has a regulatory framework, but the CVM cannot provide any information, as they are not responsible for regulation and legislation on the topics of Recommendation 15.

[158] Abu Dhabi, AIFC Astana

[159] Abu Dhabi

[160] Rules 14.11 and 15.9, read in conjunction with 17.8 of the Conduct of Business Rulebook

[161] AIFC Astana

safeguard the rights of crypto-assets issuers and holders, prevent the unauthorised creation or deletion of crypto-assets. CASPs providing custody must at least every 25 business days perform an internal custody record reconciliation in respect of each individual Client's ledger balances. Issuers of stablecoins related to fiat currencies must mandate an independent third-party audit of the reserve assets annually but not later than 4 months after the close of its financial year.

Independent Assurance

In one Participating Jurisdiction[162], CASPs are required to put in place technology governance and risk management systems, controls and plans to assess and ensure the adequacy of the internal control environment in respect to crypto-asset wallet and key management, including independent audits[163]. On a supervisory basis, CASPs are required to put in place and carry out third party audits on compliance with the rules on technology governance and controls. The regulator has supervisory powers to require the production of information and documents[164]. The regulator can either impose the requirement on the person concerned to provide the report by the skilled person or can itself appoint to skilled person to provide the required report. In any event, the skilled person must have the skills necessary to provide the report and be either nominated or approved by the regulator. Auditors are provided[165] with protection in respect of information or opinions they provide to the regulator where they provide those in good faith and in the discharge of their Auditor's duties and functions.

Within another Participating Jurisdiction[166], the regulatory regime requires a CASP to undergo regular internal and external audits to assess their compliance with regulatory requirements. The supervisory powers of the regulator provides it with wide powers including without limitations to gather information, including results of audits, including independent audits[167]. The regulator may specifically require CASPs to produce a report by approving or nominating a person, which will prepare a report.

Challenges and Gaps

[162] Abu Dhabi

[163] COBS Rule 17.5 and Guidelines for Financial Institutions adopting Enabling Technologies

[164] Set out in section 201 FSMR and sections 203 & 204 FSMR

[165] By Section 191 FSMR

[166] AIFC Astana

[167] Sections 95 -101 of the AIFC Financial Services Framework Regulations (FSFR)

The RT has not identified major gaps in the regulatory framework on client asset reconciliation and independent assurance. However, three jurisdictions[168] do not have any regulation in place. One of them[169] has already published draft regulations covering this.

Two Participating Jurisdictions[170] have regulation regarding client asset reconciliation and independent assurance only for entities that fall within existing regulatory frameworks and do not extend to broader crypto markets (e.g. banks).

5.9 Recommendation 16: Securing client money and assets

Recommendation 16 (Securing client money and assets)*: Regulators should require a CASP to adopt appropriate systems, policies and procedures to mitigate the risk of loss, theft or inaccessibility of Client Assets.*

For the purposes of this Thematic Review, the RT focused on two aspects of implementation:

1. Whether jurisdictions have a regulatory framework in place that requires CASPs to adopt appropriate IT systems, policies and procedures that are proportional to their business model with the aim of minimising any loss or theft of client assets (to avoid hacking or any loss of the means to access Client Assets). Such policies and procedures should take into account and shall be based on the risks associated with their business model and the different wallet types.
2. Whether the regulatory framework provides clarity on the liability of CASPs for losing client assets. It shall be clear when and to what extent clients need to be compensated for the assets that have been lost or stolen.

To be rated Fully Implemented, the RT looked for affirmative and satisfactory responses to both elements. Where the legal or regulatory framework in force covers only one of the above elements, the relevant rating of the least progressed element would be reflected.

Key Findings

[168] Brazil, Georgia, United Kingdom

[169] United Kingdom

[170] Australia, Switzerland

12 Participating Jurisdictions [171] have final implementation measures in force across the two elements underpinning Recommendation 16: having systems, policies, and procedures in place to mitigate the risk of loss, theft and inaccessibility, and having clarity on liability and compensation rules in the event of a loss. Two Participating Jurisdictions met element 2 but not element 1[172] and one Participating Jurisdiction[173] met element 1 but not element 2.

13 Participating Jurisdictions [174] have in place requirements for policies, procedures, and appropriate IT systems to minimize any loss or theft of client assets. Most of these jurisdictions require relevant systems and controls to be in place ranging from fund safekeeping and segregation to the use of hot and cold wallets, and requirements for clear governance frameworks.

15 Participating Jurisdictions[175] have requirements on clarity of liability of CASPs losing client assets. In the remaining responses, jurisdictions either do not mention, or specifically carve out, liabilities for CASPs to compensate clients in the event of a loss of client assets. Some[176] require CASPs to be liable to their clients for the loss of any client assets including compensation[177].

Emerging practices

Procedures and Controls: For element 1, the importance of strong procedures and controls for controlling client money and assets is integral. One Participating Jurisdiction[178] provided a detailed response that requires CASPs to have multi-signature wallets, senior management oversight of client asset transfers, and ensuring prevention of unauthorized access of client assets. It also mandates these senior managers to be resident within the territory of the jurisdiction. Furthermore, the response emphasises that client assets should be subject to periodic reviews that assess the risk management framework.

[171] Abu Dhabi, AIFC Astana, Bermuda, Canada, France, Gibraltar, Hong Kong, Japan, Liechtenstein, Malta, Singapore, Thailand.

[172] Bahamas and Republic of Korea

[173] South Africa

[174] Abu Dhabi, AIFC Astana, Bermuda, Canada, France, Gibraltar, Hong Kong, Japan, Liechtenstein, Malta, Singapore, South Africa, Thailand.

[175] Abu Dhabi, AIFC Astana, Australia, Bahamas, Bermuda, Canada, France, Gibraltar, Hong Kong, Japan, Republic of Korea, Liechtenstein, Malta, Singapore, Thailand.

[176] Abu Dhabi, AIFC Astana, Australia, Bermuda, Hong Kong, Japan, Republic of Korea, Malta, Singapore

[177] Abu Dhabi, AIFC Astana, Australia, Bermuda, Hong Kong, Japan, Republic of Korea, Liechtenstein, Malta, Singapore

[178] Singapore

Compensation for Clients: For element 2, the ability to compensate clients in certain scenarios can provide investor protection. One Participating Jurisdiction's response[179] set out three options for ensuring clients are compensated in the event of a loss or inaccessibility of funds where crypto-asset entities must either have third-party insurance, funds or crypto-assets set aside and designated for compensation, or a bank guarantee provided by an authorized financial institution.

Hot and Cold Wallets, and other risk mitigants: The use of hot and cold wallets can help mitigate some of the risks that can arise in securing client assets, but authorities should recognize the risks associated with different wallet types. Seven jurisdictions mentioned requirements around the use of cold wallets[180] , with five of those setting out requirements around proportion of assets to be kept in such wallets[181] . The response by one Participating Jurisdiction[182] mentioned the need for systems and controls to be in place to manage the risk of employee collusions, while the response by another jurisdiction[183] highlighted that the transfer of assets from cold wallets must require the approval of at least two authorized individuals with no conflicts of interest. In their response, another jurisdiction[184] stated that they require CASPs to restrict any individual from being able to solely authorise and effect the movement, transfer or withdrawal of customers' asset, control the movement or transfer of customers' assets between the CASP's storage systems and devices and, are capable of preventing unauthorised access to or loss of the crypto-asset instruments associated with the customers' assets that are held or managed by the CASP.

Challenges and Gaps

No regulation in place: Gaps for Recommendation 16 exist largely where jurisdictions have limited or no frameworks that secure client money and assets in relation to crypto-asset markets and activities. Two jurisdictions specifically noted that their framework toward custody extends only to crypto-assets that fall within existing regulatory frameworks and do not extend to broader crypto markets[185] although in one of them[186] client assets held by CASPs are protected in case of bankruptcy of the CASP under general Bankruptcy Law. Three others do

[179] Hong Kong

[180] Bermuda, Gibraltar, Hong Kong, Japan, Republic of Korea, Singapore, Thailand.

[181] 98% in Hong Kong, 95% in Japan, 90% in Singapore, 90% in Thailand, 80% in the Republic of Korea.

[182] Hong Kong

[183] Thailand

[184] Singapore

[185] Australia, Switzerland

[186] Switzerland

not currently have specific custody requirements in place for crypto-asset markets and activities that ensures client money and assets are secured[187].

Regulation is not comprehensive: In some instance, regulation is in place but does not provide authorities with the powers to meet Recommendation 16 in full. One response[188] suggested that at least some elements of securing client money and assets are delivered through self-regulatory guidelines. One jurisdiction[189] does not have clear provisions within their framework for IT systems, policies, and procedures to mitigate the loss or theft of client assets, while another[190] does not have specific requirements to compensate clients in the event of losses.

5.10 Recommendation 18: Retail Client Appropriateness and Disclosure

Recommendation 18 (Retail Client Appropriateness and Disclosure): *Regulators should require a CASP to operate in a manner consistent with IOSCO's Standards regarding interactions and dealings with retail clients. Regulators should require, or work with other relevant authorities to require, that all promotions and marketing of crypto-assets to retail clients accurately and sufficiently disclose the product and service provided as well as the associated risks in a manner that is fair, clear, and not misleading. Regulators should require a CASP to implement adequate systems, policies and procedures, including for providing disclosures, in relation to onboarding new clients, and as part of its ongoing services to existing clients. This should include assessing the appropriateness and/or suitability of particular crypto-asset products and services offered to each retail client.*

Particularly acute asymmetry of information arises between CASPs and the retail investor, the significance of which is intensified by the weak market discipline arising in part from the relatively low level of participation of institutional and professional investors, and the unregulated or non-compliant distribution channels that are used to distribute crypto-assets to retail investors, often on a cross-border basis. In this context, Recommendation 18 sets out to help ensure that existing or new regulations require CASPs to diligently assess and onboard retail investors who are aware of, and deemed suitable to take on, the greater speculative risks

[187] Brazil, Georgia, United Kingdom

[188] Republic of Korea

[189] Bahamas

[190] South Africa

inherent in this market, and to use appropriate measures when promoting crypto-assets to this population, including if crypto-assets are promoted on social media.

For the purposes of this Review, the RT considered the following three aspects when assessing the Participating Jurisdictions' frameworks:

i. Regulations should require that all promotions and marketing to retail clients clearly disclose the product, service, associated risks, and any fee, commission or incentive, directly or indirectly charged to the client.
ii. Regulations should require a CASP to implement adequate systems, policies and procedures, including for providing disclosures, in relation to onboarding new clients, and as part of its ongoing services to existing clients. This should include assessing the appropriateness and/or suitability of particular crypto-asset products and services offered to each retail client, which should entail an assessment of retail investors knowledge and experience.
iii. Regulators should require CASPs to have an efficient and effective mechanism to address client complaints.

To be rated "Final implementation measures in force", the RT looked for affirmative and satisfactory responses to the above three questions. Where the legal or regulatory framework in force covers only some of the above elements, the relevant rating of the least progressed element would be reflected.

Key Findings

Eight Participating jurisdictions [191] have fully implemented Recommendation 18. Three jurisdictions[192] have not implemented any elements of Recommendation 18. Two jurisdictions[193] have reforms underway that cover Recommendation 18.

The elements of Recommendation 18 that were the most implemented across jurisdictions related to systems, policies and procedures for providing disclosures, particularly ongoing disclosures as opposed to onboarding new clients.

Disclosures to retail investors generally cover product/service key features and associated risks as well as fees, when retail investor promotions/marketing disclosures and general conduct rules on disclosures are taken together. Commercial arrangements with persons providing investment advice are not consistently captured in disclosures.

A divergence emerges on the scope of suitability assessments that regulations generally require CASPs to conduct, with some requirements at the level of client onboarding and

[191] AIFC Astana, Bermuda, Canada, Gibraltar, Hong Kong, Japan, Singapore, Thailand.

[192] Brazil, Georgia, Republic of Korea.

[193] Switzerland, United Kingdom.

service provision, and other restricted to specific types of services (advice or managing investments). Besides, regulations are often either lacking requirements or are not sufficiently clear on the application of appropriateness tests when CASPs execute client orders.

Fourteen (14) Participating Jurisdictions[194] require CASPs to have arrangements in place for the handling of complaints. While the assessment of efficiency and effectiveness fall outside the scope of this exercise, it is worth noting that countries have different approaches to ensuring timeliness of dispute resolutions – from binding deadlines, to guidance and general principles.[195]

Emerging practices

In one Participating Jurisdiction[196], the regulatory framework outlines clear requirements on CASPs to assess both suitability – when advising on investments or managing investments for a client – and appropriateness – when (a) dealing in investments as principal (dealer services); (b) dealing in investments as agent (brokerage service), or (c) receiving and transmitting orders for a client, and is not advising on investments or managing investments.[197]

Another jurisdiction[198] has implemented targeted enhancements to its regulatory framework to improve retail investor protection in crypto-asset services. Instead of appropriateness or suitability assessments relied upon in the traditional capital market, CASPs must perform a risk awareness assessment before offering services to retail customers. This assessment determines whether clients possess adequate knowledge of the risks associated with crypto-asset activities. The assessment must be both fair and robust, underpinned by CASP policies ensuring relevance to the specific services provided. Additionally, the assessment must avoid trivializing risks or promoting particular products, and should use a sufficiently diversified set of question to ensure the integrity of the assessment. Crypto-asset services cannot be provided to retail customers who have not been assessed to be aware of the risks.

Challenges and Gaps

[194] Abu Dhabi, AIFC Astana, Australia, Bermuda, Canada, France, Gibraltar, Hong Kong, Japan, Liechtenstein, Malta, Singapore, South Africa, Thailand.

[195] The United Kingdom has partially incorporated this key element in its draft implementation measures. FCA Discussion Paper DP23/4 "Regulating cryptoassets. Phase 1: Stablecoins" sets out conduct of business and consumer redress standards applicable to stablecoins and custodians. Complaints handling for CASPs more broadly will be addressed as part of the Consultation Paper on conduct and firm standards for all Regulated Activities Order (RAO) activities planned for Q3 2025, based on the FCA Roadmap

[196] AIFC Astana

[197] See AIFC Conduct of Business Rules AIFC Rules No. FR0005 of 2017, 5.1.2 in conjunction with AIFC Rules on Digital Asset Activities (DAA) AIFC Rules NO. FR00062 of 2023

[198] Singapore

Regulations often lack requirements or are not sufficiently clear on the application of suitability or appropriateness tests when CASPs execute client orders. In some jurisdictions[199] suitability assessments are required in the case where CASPs provide portfolio advice, but not if the CASP is simply executing a client order. Very few jurisdictions included details on ongoing disclosures to clients.

[199] E.g., Abu Dhabi, EU/EEA jurisdictions covered by MICAR

Appendix 1 –List of Policy Recommendations for Crypto and Digital Assets Markets

Recommendations *(Recommendations marked with * are assessed in the present report)*	
Recommendation 1 (Common Standards of Regulatory Outcomes):	Regulators should use existing frameworks or New Frameworks to regulate and oversee crypto-asset trading, other crypto-asset services, and the issuing, marketing and selling of crypto-assets (including as investments), in a manner consistent with IOSCO Objectives and Principles for Securities Regulation and relevant supporting IOSCO principles, standards, recommendations, and good practices (hereafter "IOSCO Standards"). The regulatory approach should seek to achieve regulatory outcomes for investor protection and market integrity that are the same as, or consistent with, those that are required in traditional financial markets.
*** Recommendation 2 (Organizational Governance):**	Regulators should require a CASP to have effective governance and organizational arrangements, commensurate to its activities, including systems, policies and procedures that would, amongst other things, address conflicts of interest, including those arising from different activities conducted, and services provided by a CASP or its affiliated entities. These conflicts should be effectively identified, managed and mitigated. A regulator should consider whether certain conflicts are sufficiently acute that they cannot be effectively mitigated, including through effective systems and controls, disclosure, or prohibited actions, and may require more robust measures such as legal segregation of functions and activities, as well as separate registration and regulation of certain activities and functions to address this Recommendation.
*** Recommendation 3 (Disclosure of Role, Capacity and Trading Conflicts):**	Regulators should require a CASP to have accurately disclosed each role and capacity in which it is acting at all times. These disclosures should be made, in plain, concise, non-technical language, as relevant to the CASP's clients, prospective clients, the general public, and regulators in all jurisdictions where the CASP operates, and into which it provides services. Relevant disclosures should take place prior to entering into an agreement with a prospective client to provide services, and at any point thereafter when such position changes (e.g., if and when the CASP takes on a new, or different, role or capacity).

Recommendations *(Recommendations marked with * are assessed in the present report)*	
Recommendation 4 (Client Order Handling):	Regulators should require a CASP, when acting as an agent, to handle all client orders fairly and equitably. Regulators should require a CASP to have systems, policies and procedures to provide for fair and expeditious execution of client orders, and restrictions on front-running client orders. Regulators should require that a CASP discloses these systems, policies and procedures to clients and prospective clients, as relevant. Orders should be handled promptly and accurately recorded.
Recommendation 5 (Market Operation Requirements):	Regulators should require a CASP that operates a market or acts as an intermediary (directly or indirectly on behalf of a client) to provide pre- and post-trade disclosures in a form and manner that are the same as, or that achieve similar regulatory outcomes consistent with, those that are required in traditional financial markets.
Recommendation 6 (Admission to Trading):	Regulators should require a CASP to establish, maintain and appropriately disclose to the public their standards— including systems, policies and procedures— for listing / admitting crypto assets to trading on its market, as well as those for removing crypto-assets from trading. These standards should include the substantive and procedural standards for making such determinations.
Recommendation 7 (Management of Primary Markets Conflicts)	Regulators should require a CASP to manage and mitigate conflicts of interest surrounding the issuance, trading and listing of crypto-assets. This should include appropriate disclosure requirements and may necessitate a prohibition on a CASP listing and / or facilitating trading in, its own proprietary crypto-assets, or any crypto-assets in which the CASP, or an affiliated entity, may have a material interest.
*** Recommendation 8 (Fraud and Market Abuse):**	Regulators should bring enforcement actions against offences involving fraud and market abuse in crypto-asset markets, taking into consideration the extent to which they are not already covered by existing regulatory frameworks. These offences should cover all relevant fraudulent and abusive practices such as market manipulation, insider dealing and unlawful disclosure of inside information; money laundering/terrorist financing; issuing false and misleading statements; and misappropriation of funds.
Recommendation 9 (Market Surveillance):	Regulators should have market surveillance requirements applying to each CASP, so that market abuse risks are effectively mitigated.

Recommendations *(Recommendations marked with * are assessed in the present report)*	
Recommendation 10 (Management of Material Non-Public Information):	Regulators should require a CASP to put in place systems, policies and procedures around the management of material non-public information, including, where relevant, information related to whether a crypto-asset will be admitted or listed for trading on its platform and information related to client orders, trade execution, and personally identifying information.
*** Recommendation 11 (Enhanced Regulatory Co-operation):**	Regulators, in recognition of the cross-border nature of crypto-asset issuance, trading, and other activities, should have the ability to share information and cooperate with regulators and relevant authorities in other jurisdictions with respect to such activities. This includes having available co-operation arrangements and/or other mechanisms to engage with regulators and relevant authorities in other jurisdictions. These should accommodate the authorization and on-going supervision of regulated CASPs and enable broad assistance in enforcement investigations and related proceedings.
*** Recommendation 12 (Overarching Custody Recommendation):**	Regulators should apply the IOSCO Recommendations Regarding the Protection of Client Assets when considering the application of existing frameworks, or New Frameworks, covering CASPs that hold or safeguard Client Assets.
*** Recommendation 13 (Segregation and Handling of Client Monies and Assets):**	Regulators should require a CASP to place Client Assets in trust, or to otherwise segregate them from the CASP's proprietary assets.

Recommendations *(Recommendations marked with * are assessed in the present report)*	
*** Recommendation 14 (Disclosure of Custody and Safekeeping Arrangements):**	Regulators should require a CASP to disclose, as relevant, in clear, concise and non-technical language to clients: 1. How Client Assets are held, and the arrangements for safeguarding these assets and/or their private keys; 2. The use (if any) of an independent custodian, sub-custodian or related party custodian; 3. The extent to which Client Assets are aggregated or pooled within omnibus client accounts, the rights of individual clients with respect to the aggregated or pooled assets, and the risks of loss arising from any pooling or aggregating activities; 4. Risks arising from the CASP's handling or moving of Client Assets, whether directly or indirectly, such as through a cross-chain bridge; and 5. Full and accurate information on the obligations and responsibilities of a CASP with respect to the use of Client Assets, as well as private keys, including the terms for their restitution, and on the risks involved.
*** Recommendation 15 (Client Asset Reconciliation and Independent Assurance):**	Regulators should require a CASP to have systems, policies, and procedures to conduct regular and frequent reconciliations of Client Assets subject to appropriate independent assurance.
*** Recommendation 16 (Securing client money and assets):**	Regulators should require a CASP to adopt appropriate systems, policies and procedures to mitigate the risk of loss, theft or inaccessibility of Client Assets.
Recommendation 17 (Management and disclosure of Operational and Technological Risks):	Regulators should require a CASP to comply with requirements pertaining to operational and technology risk and resilience in accordance with IOSCO's Recommendations and Standards. Regulators should require a CASP to disclose in a clear, concise and non-technical manner, all material sources of operational and technological risks and have appropriate risk management frameworks (e.g., people, processes, systems and controls) in place to manage and mitigate such risks.

Recommendations *(Recommendations marked with * are assessed in the present report)*	
*** Recommendation 18 (Retail Client Appropriateness and Disclosure):**	Regulators should require a CASP to operate in a manner consistent with IOSCO's Standards regarding interactions and dealings with retail clients. Regulators should require, or work with other relevant authorities to require, that all promotions and marketing of crypto-assets to retail clients accurately and sufficiently disclose the product and service provided as well as the associated risks in a manner that is fair, clear, and not misleading. Regulators should require a CASP to implement adequate systems, policies and procedures, including for providing disclosures in relation to onboarding new clients, and as part of its ongoing services to existing clients. This should include assessing the appropriateness and/or suitability of particular crypto-asset products and services offered to each retail client.

Appendix 2 – List of Participating Jurisdictions

1. Abu Dhabi (UAE)
2. AIFC Astana
3. Australia
4. Bahamas
5. Bermuda
6. Brazil
7. Canada (Quebec and Ontario)
8. France
9. Georgia
10. Gibraltar
11. Hong Kong
12. Japan
13. Liechtenstein
14. Korea (Republic of)
15. Malta
16. Singapore
17. South Africa
18. Switzerland
19. Thailand
20. United Kingdom

Appendix 3 – Composition of the Review Team

The RT is led by:

- Laurent Van Burik, CSSF Luxembourg & AC Chair, and
- Matthew Long (FCA UK)

The RT is composed of:

- Australia ASIC (Gerard Fitzpatrick and Edward Wong)
- Brazil CVM (Florisvaldo Justino Machado, Maria Eduarda Lacerda Daniel until July 2025)
- AMF France (Estelle de Beaucé and Jules Triolaire)
- BaFin Germany (Beatrice van Trill)
- Hong Kong SFC (Bonnie Tang)
- CBI Ireland (Cameron Carr and Renata Blaszczyk)
- Consob Italy (Daniela Gariboldi and Emanuela Ciucci)
- CSSF Luxembourg (Patrick Hoffman)
- AMMC Morocco (Tarik Malki until May 2025)
- MAS Singapore (Kelvin Tan and Estee Pang)
- UK FCA (Jane Moore and Janet Ho)
- U.S. SEC (Batkhuu Dashnyam and Magda Camillo)
- U.S. CFTC (Nancy Doyle until June 2025)
- International Monetary Fund (Parma Bains)
- World Bank (Maria Teresa Chimienti and Ana Carvajal)
- IOSCO Secretariat (Raluca Tircoci Craciun, Hemla Deenanath and Daniel Palacios)