Policy Recommendations for Crypto and Digital Asset Markets

Consultation Report

THE BOARD
OF THE
INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS

CR01/2023	**MAY 2023**

Copies of publications are available from:
The International Organization of Securities Commissions website: www.iosco.org

Foreword

The International Organization of Securities Commissions (IOSCO) has published this Consultation Report with the aim of finalizing IOSCO's policy recommendations to address market integrity and investor protection issues[1] in crypto-asset markets in early-Q4 2023. In line with IOSCO's established approach for securities regulation, the Crypto and Digital Asset Recommendations (CDA Recommendations)[2] are addressed to relevant authorities and look to support jurisdictions seeking to establish compliant markets for the trading of crypto or 'digital' or 'virtual' assets (hereafter "crypto-assets" and read to include all relevant tokens) in the most effective way possible.

Feedback to the Consultation Process

IOSCO welcomes input from all stakeholders as part of this consultation process.

Please submit consultation responses to cryptoassetsconsultation@iosco.org by 31 July 2023.

Your comment letter should indicate prominently that it is a *'Public Comment on IOSCO's Consultation Report on Policy Recommendations for Crypto and Digital Asset Markets'*.

All comments received will be made available publicly, unless anonymity is specifically requested. Comments will be converted to PDF format and posted on the IOSCO website.

[1] The general body of IOSCO's existing Principles and recommendations also cover prudential matters concerning asset managers, trading platforms and others involved in investment in, and the trading of securities. Those matters have not been covered in this report with respect to the crypto-asset sector. In parallel, the Financial Stability Board is considering the financial stability issues arising from crypto asset activities.

[2] The Recommendations in this Consultation Report are focussed on centralized crypto asset market activities. IOSCO will separately consult on issues related to Decentralized Finance (DeFi).

Table of Contents

EXECUTIVE SUMMARY

This consultation report proposes 18 policy recommendations that IOSCO plans to finalize in early Q4 this year to support greater consistency with respect to regulatory frameworks and oversight in its member jurisdictions, to address concerns related to market integrity and investor protection arising from crypto-asset activities. The recommendations have been developed under the stewardship of the IOSCO Board's Fintech Task Force (FTF) in accordance with IOSCO's Crypto-Asset Roadmap published in June 2022.[3]

The proposed recommendations are principles-based and outcomes-focused and are aimed at the activities performed by crypto-asset service providers (CASPs)[4]. They apply IOSCO's widely accepted global standards for securities markets regulation to address key issues and risks identified in crypto-asset markets. The proposed recommendations are activities-based and follow a 'lifecycle' approach in addressing the key risks identified in this report. They cover the range of activities in crypto-asset markets that involve CASPs from offering, admission to trading, ongoing trading, settlement, market surveillance and custody as well as marketing and distribution (covering advised and non-advised sales) to retail investors. The proposed recommendations do not cover activities, products or services provided in the so-called "decentralized finance" or "DeFi" area. The FTF DeFi workstream is considering issues in relation to DeFi and will publish a consultation report with proposed recommendations later this summer.

One of IOSCO's goals is to promote greater consistency with respect to how IOSCO members approach the regulation and oversight of crypto-asset activities, given the cross-border nature of the markets, the risks of regulatory arbitrage and the significant risk of harm to which retail investors continue to be exposed. IOSCO is also seeking to encourage optimal consistency in the way crypto-asset markets and securities markets are regulated within individual IOSCO jurisdictions, in accordance with the principle of 'same activities, same risks, same regulatory outcomes'.

The proposed recommendations also cover the need for enhanced cooperation among regulators. They aim to provide a critical benchmark for IOSCO members to cooperate, coordinate and respond

---

3 The FTF was established in March 2022 to develop recommendations to the Board of IOSCO and thereafter to oversee the implementation of IOSCO's regulatory agenda for Fintech and crypto-assets. The FTF is prioritising policy-focused work on crypto-asset markets and activities in its initial 12 to 24 months of operation, while continuing to monitor market developments associated with broader Fintech-related trends and innovation.

4 CASPs are 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 ancillary activities such as lending / staking of crypto-assets and the promotion and distribution of crypto-assets on behalf of others.

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.

While the proposed recommendations are not directly addressed to markets participants, CASPs and all participants in crypto-asset markets are strongly encouraged to carefully consider the expectations and outcomes articulated through the proposed recommendations and the respective supporting guidance in the conduct of registered/licensed, and cross-border activities.

INTRODUCTION

IOSCO is issuing 18 Recommendations for public consultation to help IOSCO members apply IOSCO's Objectives and Principles for Securities Regulation and relevant supporting IOSCO standards, recommendations, and good practices (hereafter "IOSCO Standards"), as appropriate, to crypto-asset[5] activities within their jurisdictions and, in particular, to respond to widespread concerns regarding market integrity and investor protection within the crypto-asset markets.

The proposed 18 Recommendations cover six key areas, consistent with IOSCO Standards:

1. Conflicts of interest arising from vertical integration of activities and functions,
2. Market manipulation, insider trading and fraud,
3. Cross-border risks and regulatory cooperation,
4. Custody and client asset protection,
5. Operational and technological risk, and
6. Retail access, suitability, and distribution.

Acknowledging the definitional and interpretive jurisdictional differences that currently exist, IOSCO has developed the proposed Recommendations by developing a functional, economic approach to mitigate against the risks, rather than attempting to develop a one-size fits all prescriptive taxonomy.

Accordingly, IOSCO is developing an outcomes-focused, principles-based approach across each key area noted above. This approach is informed by a mapping of IOSCO standards, principles and relevant sectoral recommendations and guidance to relevant elements of the infrastructure, and to the services provided by, and the activities of participants.

By doing this, we have been able to examine and assess how IOSCO's existing policy framework maps to key identified risks in crypto-asset markets, which IOSCO and its members understand from their expertise as securities markets and conduct regulators.

5 The term "crypto asset," also sometimes called a "digital asset," refers to an asset that is issued and/or transferred using distributed ledger or blockchain technology ("distributed ledger technology"), including, but not limited to, so-called "virtual currencies," "coins," and "tokens." To the extent digital assets rely on cryptographic protocols, these types of assets are commonly referred to as "crypto assets."

OVERVIEW OF KEY CONTENTS OF THE REPORT

This consultation report, and the 18 Recommendations contained within, are structured thematically as follows:

- ***Introduction***

  This provides an overview of the key content and structure of the report, along with the broader international regulatory and market context for the development of the proposed recommendations.

- ***Chapter 1 – Overarching Recommendation Addressed to All Regulators***

  This Chapter lays down an overarching Recommendation and supporting guidance calling upon all IOSCO members, collectively, to apply or adopt these recommendations in a consistent, outcomes-focused manner.

  As set out in Recommendation 1 *('Overarching Recommendation Addressed to All Regulators')*, the regulatory frameworks (existing or new) should seek to achieve regulatory outcomes for investor protection and market integrity that are the same as, or consistent with, those required in traditional financial markets in order to facilitate a level-playing field between crypto-assets and traditional financial markets and help reduce the risk of regulatory arbitrage.

  Regulators are therefore encouraged to analyze the applicability and adequacy of their regulatory frameworks, and the extent to which (1) crypto-assets are, or behave like substitutes for, regulated financial instruments, and (2) investors have substituted other financial instrument investment activities with crypto-asset investment activities.

  In adopting this approach, these Recommendations are designed to apply to all types of crypto-assets. This includes stablecoins, where further risks presented by such crypto-assets are explored by way of supplementary guidance with two additional recommendations in the box text in Chapter 10.[6]

  Through its preamble *('Preamble: Intent of the Recommendations')*, Chapter 1 further clarifies the intent of the proposed 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

[6] The targeted commentary on stablecoins builds on the findings of the March 2020 IOSCO Report on Global Stablecoin Initiatives.

outcomes-based flexibility in their domestic implementation.[7]

- ***Chapter 2 – Recommendations on Governance and Disclosure of Conflicts***

  This Chapter includes the proposed recommendations and supporting guidance to address risks arising, in particular, from vertically integrated crypto-asset trading platform business models. Many CASPs typically engage in multiple functions and activities under 'one roof' – including exchange trading, brokerage, market-making and other proprietary trading, offering margin trading, custody, settlement, and re-use of assets – whether through a single legal entity or an affiliated group of entities that are part of a wider group structure. Recommendation 2 *('Organizational Governance')* states that CASPs should have effective governance and organisational requirements in place to effectively address and mitigate issues on conflicts of interests arising from vertical integration, including the possible need for measures such as legal disaggregation and separate registration. Where a CASP engages 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 the capacity in which it is acting, in relation to its clients. Accordingly, Recommendation 3 *('Disclosure of Role, Capacity and Trading Conflicts')* states that a CASP should accurately disclose each role and capacity in which it is acting at all times.

- ***Chapter 3 – Recommendations on Order Handling and Trade Disclosures (Trading Intermediaries vs Market Operators)***

  This Chapter includes proposed recommendations and supporting guidance in the areas of Order Handling and Trade Disclosures. Despite common market parlance of referring CASPs as "exchanges", a CASP may actually be operating as a trading intermediary (a broker or dealer or both) instead of a market operator (or trading venue). Recommendation 4 *('Client Order Handling')* addresses inherent conflicts of interests where CASPs may front-run clients' orders in favor of their own, or related party, transactions. CASPs are thus expected to implement systems, policies and procedures that provide for fair, orderly, timely execution and in the best

[7] The Recommendations recognize that some jurisdictions have existing regulatory frameworks that encompass crypto and digital assets, while other jurisdictions are in the process of developing regulatory frameworks. Each jurisdiction should implement the CDA Recommendations, as they deem appropriate, within their existing or developing frameworks.

interest of clients. In the context of a CASP acting as a market operator (or trading venue), it is expected to have resilient systems to effectively support its operation of a central limit order book in a fair, orderly and transparent manner. Recommendation 5 *('Market Operation Requirements')* sets out transparency requirements in trade disclosures to promote price discovery and competition, which applies to all CASPs and not just those acting as market operators. Transparency requirements and trade disclosure expectations apply to both on-chain and off-chain activity.

- ***Chapter 4 – Recommendations in Relation to the Listing of Crypto-Assets and Certain Primary Market Activities***.

  This Chapter relates to the management of conflicts of interest which may arise from the listing and trading of crypto-assets by CASPs. Many crypto-assets are sold without important disclosures about the crypto-asset and its issuer. There is a lack of accurate and sufficient disclosures to facilitate informed decision-making, a key tenet of traditional financial markets. There also tends to be little, if any, verifiable continuous information provided about or by the crypto-asset issuer. Recommendation 6 *('Admission to Trading')* states that CASPs should adopt and disclose substantive and procedural listing and delisting standards pertaining to crypto-assets. The recommendation also specifies the types of disclosures that regulators may consider requiring, including information which may be more relevant to stablecoins. Recommendation 7 *('Management of Primary Markets Conflicts')* is concerned specifically with the management of conflicts around crypto-assets issued by crypto-asset issuers in which the CASP has a material interest. Conflict mitigants could include prohibitions on the CASP listing/trading such assets.

- ***Chapter 5 – Recommendations to Address Abusive Behaviors***

  This Chapter provides recommendations and supporting guidance to address issues on market integrity risks which have been exacerbated by the fragmented, cross-border nature of the crypto-asset market, such as (1) the lack of effective market surveillance, (2) manipulative market practices (including pyramid and Ponzi schemes, 'pump and dump' schemes, wash-trading, front-running), (3) insider dealing and unlawful disclosure of inside information; and (4) fraudulent, misleading, or insufficient disclosure. To address such behaviors, Recommendations 8 to 10 *('Fraud and Market Abuse; Market Surveillance; Management of Non-Public Information')* set out the critical expectation that there should be effective systems and controls to identify and monitor for manipulative market practices and to prevent leakage

of inside information. Consideration is given to the availability of data ('on-chain' and 'off-chain'), consistent reporting standards and the existing tools available to regulatory authorities (e.g., intelligence and co-operation) and market participants (e.g., surveillance systems and controls).

- ***Chapter 6 – Recommendation on Cross-Border Cooperation***

  This Chapter and its supporting guidance responds to the cross-border character of crypto-asset trading by setting out a critical recommendation for how IOSCO members should adopt best practices in international cooperation in order to help ensure effective supervision and enforcement *(see Recommendation 11 'Enhanced Regulatory Cooperation'),* and to reduce the risk of money laundering. Experience has shown that CASPs often present themselves as operating in a borderless manner and tend to take an ambivalent approach to regulatory compliance. This – in tandem with the global reach of the crypto-asset market, its participants, activities, and some unique characteristics linked to the underlying distributed ledger technology ("DLT") and cryptography, as well as the scale and scope for cross-border regulatory arbitrage – means that investor protection and market integrity issues will persist without coordinated international regulatory action to address them. IOSCO's wide memberships in securities and derivatives markets, with market conduct regulatory expertise and existing information-sharing tools for authorization, supervision and enforcement are well positioned to achieve investor protection and market integrity objectives.

- ***Chapter 7 – Recommendations on Custody of Client Monies and Assets***

  This Chapter provides recommendations and supporting guidance to deal with custody-related risks and the safeguarding of Client Monies and Assets and to provide clients with clear, concise and non-technical disclosures of the associated risks. These risks relate to the asset segregation, re-use of assets, liability and ownership considerations. The Recommendations address, amongst other things, the controls that should be embedded within regulatory frameworks to help ensure that where Client Monies and Assets are held by CASPs they are held safely, and transferred securely, and that inappropriate mixing of assets and other potential abuses are avoided *(see Recommendations 12 to 16: 'Overarching Custody Recommendation'; 'Segregation and Handling of Client Monies and Assets'; 'Disclosure of Custody and Safekeeping Arrangements'; Client Asset Reconciliation and Independent Assurance; Securing Client Money and Assets').*

- ***Chapter 8 – Recommendation to Address Operational and Technological Risks***

  This Chapter provides the recommendations and supporting guidance to address the broad spectrum of operational risks that can arise because of lax controls at CASPs combined with the risks related to DLT and smart contracts. *(Recommendation 17 'Management and Disclosure of Operational and Technological Risks').*

- ***Chapter 9 – Recommendation for Retail Distribution***

  This Chapter provides the recommendation and supporting guidance to address the particular issues not covered elsewhere in this report that arise from CASPs' aggressive promotion to retail investors of the trading and holding of crypto-assets. Recommendation 18 *('Retail Client Appropriateness and Disclosure')* 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 inherent in this market, and use appropriate measures when promoting crypto-assets to this population. Indeed, retail investors often would not otherwise hold or trade their own investment portfolios but for the marketing efforts by CASPS to onboard them. Therefore, a particularly acute asymmetry of information arises between CASPs and the retail investor, the significance of which is intensified by the weak market discipline arising 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.

- ***Chapter 10 – Box Text on Stablecoins***

  These Recommendations apply to all types of crypto-assets, including stablecoins. In applying these Recommendations, regulators should consider any unique issues, risks, and conflicts that CASPs have with regard to stablecoins. Where possible idiosyncratic features or risks are presented by stablecoins, the box text on stablecoins in this Chapter supports the Recommendations and captures these features and risks. The box text provides an overview of stablecoins, their roles and uses in crypto-asset markets, before outlining specific features of stablecoins for consideration. Additional guidance in relation to stablecoin disclosures and the custody of reserve assets is included.

Next steps and potential future work

This consultation paper is based on currently available information as of the date of publication. The paper highlights the investor protection and market integrity issues that exist within crypto-asset markets. IOSCO welcomes input from the public, including crypto-asset market participants, academics, technology experts, data providers and from any other interested party, on the presentation of information and recommendations in this document, as well as on any other crypto-asset related issues.

The anticipated next steps involve publishing a final report in the coming months and, at the latest, by the end of the year. This final report will be informed by input from IOSCO members and continued extensive consultation with external stakeholders, as well as responses to the questions in this report. It will also complement IOSCO's ongoing work on Decentralized Finance. Further details can be found in the IOSCO Crypto-Asset Roadmap for 2022-2023.

In addition, IOSCO is currently considering what crypto-asset related issues might require further analysis as potential follow-up to this initial set of proposed policy recommendations.

IOSCO welcomes views from stakeholders on potential additional issues for consideration.

Pre-Consultation Stakeholder Engagement

The proposed recommendations and guidance are informed by extensive pre-consultation outreach with IOSCO members and external stakeholders. IOSCO has hosted six regional roundtables with Asian, European, Middle East and African, and North American stakeholder constituencies. These roundtables included CASPs, academics, data analytics firms, industry trade associations, professional service providers, researchers and technologists. The FTF also extensively surveyed its membership to identify key risks faced by regulators and policy measures needed to address the risks.[8] It has also consulted, and benefited from the advice, of its Affiliate Member Consultative Committee (AMCC).[9]

---

8 In terms of the structure of the stakeholder engagement, questions and discussions generally centered on the following key issues (i) conflicts of interest arising from the vertically integrated model of CASPs; (ii) abusive behaviors in crypto-asset markets; (ii) custody; and (iv) retail investor harms.

9 The AMCC is comprised of 68 IOSCO affiliate members, representing securities and derivatives markets and other market infrastructures, self-regulatory organizations (SROs), investor protection funds and compensation

IOSCO members were also extensively surveyed as part of the risk analysis and identification process which informed the FTF's subsequent stakeholder engagement and policy direction.

Interaction with the FSB and the other Standard Setting Bodies

At a global level, the International Monetary Fund (IMF) and the Financial Stability Board (FSB) are calling for more regulation of the crypto-asset market. Acting on IOSCO's investor protection and market integrity mandates, the proposed recommendations look to complement and support the work of the FSB and the sectoral initiatives of other international Standard Setting Bodies (SSBs). Risks to investors and markets arising from market integrity and investor protection concerns can also have a consequential systemic impact within crypto-asset markets, and potentially also on wider financial stability given the lack of transparency and possible growing linkages to the traditional financial sector.

IOSCO is also pursuing its systemic risk mandate for crypto-asset market activities through its engagement with the FSB's agenda on the financial stability implications of crypto-assets. On 11 October 2022, the FSB published two consultation papers on the international regulation, supervision and oversight of crypto-assets activities and markets from a financial stability perspective.[10] The FSB is now analyzing consultation feedback with the aim of finalizing both sets of recommendations by July 2023. The FSB will set-out high-level principles in each area that the proposed IOSCO Recommendations, as the relevant standard setting body, have addressed in greater depth to articulate governing expectations, notably to mitigate the relevant identified market and conduct risks. This helps to ensure alignment and complementarity in the respective regulatory agendas.

Through CPMI-IOSCO[11], IOSCO also published guidance on the application of the principles for financial market infrastructure (PFMIs) to systemically important stablecoin arrangements used for payments[12] and continues to monitor market developments.

The Basel Committee on Banking Supervision (BCBS) has endorsed its finalized standard on the

---

funds, as well as other bodies with appropriate interest in securities regulation. There are currently 32 jurisdictions represented in the AMCC which also includes ten regional or international associations.

10 See 'Recommendations that promote the consistency and comprehensiveness of regulatory, supervisory and oversight approaches to crypto-asset activities and markets and strengthen international cooperation, coordination and information sharing' and 'Revised high-level recommendations for the regulation, supervision and oversight of "global stablecoin" arrangements'.

11 Committee on Payments and Market Infrastructures

12 See Application of the Principles for Financial Market Infrastructures (PFMI) to stablecoin arrangements

prudential treatment of banks' exposure to crypto-assets. Following the publication of the crypto-asset standard, there are various elements of the standard that are subject to close monitoring and review.

Furthermore, the Financial Action Task Force (FATF) has issued guidance concerning how FATF Anti-Money Laundering (AML) and Counter Terrorist Financing (CTF) obligations apply to virtual assets and virtual asset service providers.[13] For example, the Travel Rule requires virtual asset service providers and other financial institutions to share relevant originator and beneficiary information alongside virtual asset transactions. This, combined with the other work being progressed by global SSBs, illustrates the concerted international effort taking place to develop a coordinated global framework of regulation and supervision for crypto-assets to address the risks associated with crypto-asset activities.

Market Backdrop informing the Need to Develop a Globally Consistent and Coordinated Approach to Crypto-Asset Regulation

Given the global nature and certain unique characteristics of the crypto-asset market, the application of robust regulatory standards alongside international regulatory cooperation will be pivotal to help ensure that any useful innovation can occur without the risk of regulatory arbitrage and lessening standards of investor protection and market integrity.

Global retail investor exposure to crypto-assets has grown exponentially in recent years, as have retail investor losses due, not only to market conditions, but also financial crime, fraud, money laundering and other illegal crypto-asset market practices. The fragility and interconnectedness of the crypto-asset market continues to leave entities and investors exposed to significant losses triggered by all too frequent shock events.[14]

Given the speculative nature driving the demand for many crypto-assets, the lack of intrinsic value in the vast majority of crypto-assets, and the potential for retail investors to suffer significant harm at the hands of market participants, retail access, and investor protection, measures are crucial. Data from the Bank for International Settlements (BIS) examining CASP activity, calculated on a sample of more than 200 crypto-asset trading apps operating in more

[13] See, e.g., Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers

[14] Examples in 2022 alone include Terra / Luna, Celsius, Voyager, Three Arrows Capital, and FTX.

than 95 countries, from August 2015 – December 2022, shows that a majority of crypto-asset trading app-users in nearly all economies experienced losses on their bitcoin holdings.[15]

Many retail investors conduct their trading activities through, and entrust custody of their crypto-assets to, centralised intermediaries, referred to as CASPs. Many CASPs, including those with the largest market share and highest trading volumes, have demonstrated a consistent lack of willingness to comply with applicable regulatory frameworks that seek to achieve investor protection and market integrity outcomes, and in many cases structured their operations in a way to evade such frameworks.[16] By not complying with such measures, CASPs profit off retail investors while seeking to avoid the crucial safeguards that come with adherence to regulatory requirements.

A number of recent crypto-asset market events are included below in Annex B that highlight a small portion of the severe misconduct witnessed in crypto-asset markets and issues evident within CASPs currently. Regulators have been bringing enforcement actions as they respond to the investor protection and market integrity risks in crypto-asset markets in accordance with their respective regulatory remits.

---

15 See BIS Bulletin No. 69: Crypto shocks and retail losses
More users trade when the bitcoin price increases…but a large share of users in nearly all economies probably lost money. In nearly all economies in the sample, a majority of investors probably lost money on their bitcoin investment. The median investor would have lost $431 by December 2022, corresponding to almost half of their total $900 in funds invested since downloading the app. Notably, this share is even higher in several emerging market economies like Brazil, India, Pakistan, Thailand and Turkey. If investors continued to invest at a monthly frequency, over four fifths of users would have lost money.

16 According to some data, the three largest CASPs purportedly account for almost three quarters of all trading volume.

CHAPTER 1: OVERARCHING RECOMMENDATION ADDRESSED TO ALL REGULATORS

Preamble: Intent of the Recommendations

The exposure of retail investors across the globe to crypto-assets has grown in recent years, as have retail investor losses amid financial crime, fraud, money laundering and other illegal crypto-asset market activity. Given the similar economic functions and activities of the crypto-asset market and the traditional financial markets, many existing international policies, standards, and jurisdictional regulatory frameworks are applicable to crypto-asset activities.

IOSCO is issuing these proposed Policy Recommendations to help IOSCO members apply relevant existing IOSCO objectives, principles, standards, recommendations and good practices, as appropriate, to crypto-asset activities within their jurisdictions. More specifically, the proposed Policy Recommendations respond to widespread concerns regarding investor protection and market integrity within the crypto-asset markets. The need to address these concerns is evident from recent market turmoil involving crypto-asset trading, lending and borrowing platforms and other market participants, resulting in significant losses and risks to retail investors due to inadequate protections and safeguards.

Many crypto-asset activities and markets currently operate in non-compliance with applicable regulatory frameworks or are unregulated. These Recommendations recognize that some jurisdictions have existing regulatory frameworks that encompass crypto and digital assets, while some jurisdictions are in the process of developing regulatory frameworks. In addition, in some jurisdictions, the regulatory framework may allocate responsibility for the regulation and oversight of crypto and digital assets to different Regulators that possess discrete and complementary mandates and objectives, to address investor protection and market integrity risks. 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.[17] These Recommendations should be considered by IOSCO members as they apply existing regulatory frameworks, or they are granted new powers and/or

[17] Given the diversity of operating landscapes across different jurisdictions, the application and/or implementation of the 18 Recommendations can take into account the context of specific legal structures prevailing in each jurisdiction, as well as the respective mandates of individual regulators where relevant. This can be met where a regulator, through its given mandate and the regulatory frameworks it applies, sets out clear principles-based expectations for a CASP to meet (which can be supported by regulatory guidance, as appropriate), so as to achieve the same regulatory outcomes articulated in this report.

develop new requirements (such new powers and/or new requirements, together "New Frameworks"), to crypto and digital assets and related activities in a manner that achieves outcomes across jurisdictions consistent with the IOSCO Objectives and Principles for Securities Regulation.

These Recommendations apply to all types of crypto-assets, including stablecoins. Where possible idiosyncratic features or risks are presented by stablecoins, box text is included in the explanatory guidance to the individual recommendations to capture these features and risks.

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 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.

IOSCO Principles supported: 1 – 7.

The IOSCO Standards apply generally to all crypto-assets, their issuers and the provision of services in relation to primary issuance, secondary trading and ancillary services and activities linked thereto.

As crypto-assets markets and market participants have grown significantly, with market participants often acting in non-compliance with existing laws or regulations, in consideration of the identified risks in the crypto-asset market and significant ongoing harm to investors, regulators are encouraged to analyze the applicability and adequacy of their regulatory frameworks, and the extent to which:

(1) crypto-assets are, or behave like substitutes for, regulated financial instruments,[18] and
(2) investors have substituted other financial instrument investment activities with crypto-

[18] For these purposes, financial instruments include securities, traded commodities and derivative instruments thereof.

asset trading activities.

In doing so, regulators are encouraged to evaluate whether specific requirements address or are needed to address the investor protection and market integrity risks associated with such activities or certain types of crypto-assets and use existing regulatory and/or New Frameworks to regulate the services and activities.[19]

Application of IOSCO Standards, supported by these targeted Policy Recommendations, will facilitate more effective supervision, enforcement and international cooperation regarding CASPs with the goal of promoting regulatory compliance. In addition, cooperation and coordination among international bodies such as the FSB and the BIS, and between the SSBs (such as IOSCO, CPMI-IOSCO and the BCBS) on crypto-assets and crypto-asset regulations are important to achieve greater regulatory harmonization and minimize regulatory arbitrage. This should help facilitate a level-playing field between crypto-assets and traditional financial markets and help reduce the risk of regulatory arbitrage arising from any differences in how rules apply to, and are enforced with respect to, crypto-assets and traditional financial markets.

IOSCO's wide membership with securities markets and conduct regulatory expertise is well positioned to achieve these objectives.

Chapter 1 Questions:

***Question 1:* – Are there other activities and/or services in the crypto-asset markets which Recommendation 1 should cover? If so, please explain.**

***Question 2:* – Do respondents agree that regulators should take an outcomes-focused approach (which may include economic outcomes and structures) when they consider applying existing regulatory frameworks to, or adopting new frameworks for, crypto-asset markets?**

[19] As stated in IOSCO Principle 7, the Regulator should have or contribute to a process to review the perimeter of regulation regularly.

CHAPTER 2: RECOMMENDATIONS ON GOVERNANCE AND DISCLOSURE OF CONFLICTS

Recommendation 2 – *(Organizational Governance)*

Regulators should require a CASP to have effective governance and organisational 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 disaggregation and separate registration and regulation of certain activities and functions to address this Recommendation.

IOSCO Principles supported: 8, 23, 31, 33, 34

Although often presenting themselves as "exchanges", 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, settlement, lending, and/or staking – whether through a single legal entity or a closely affiliated group of legal entities that are part of a wider group structure.

Conflicts arise from engaging in these activities and functions in a vertically integrated manner. For example, a CASP that operates an order-matching service has a conflict with its users if it is also making markets or otherwise trading as principal against other users in that market. A CASP that allows margin trading may have an incentive to offer margin to an affiliate on terms better than it offers to other users.

Regulators should evaluate whether permitting a CASP to continue to engage in multiple activities in a vertically integrated manner gives rise to conflicts of interest that are not capable of being mitigated and for which disclosure is ineffective to protect markets and investors.

A regulator that does not require disaggregation by function and/or activity should consider addressing certain conflicts by prohibiting a CASP from combining certain functions in a single

legal entity or group of affiliated entities. For example, this may involve splitting particular functions into separate legal entities, with separate board and management teams and practical separation when operating the separate legal entities (or otherwise restricting conflicting activities within the same legal entity).

In addition, if considering New Frameworks, regulators should further consider taking steps to require CASPs to establish effective conflicts of interest policies, procedures and controls and provide public disclosure and reporting, as well as annual effectiveness reviews in light of any new activities or services offered. Regulators may also consider imposing additional independence requirements or de-coupling of functions.

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).

IOSCO Principles Supported: 31, 34, 35 and 37

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. Recent events have shown that clients do not understand the differing conflicting activities and roles that CASPs are playing in a vertically integrated organization and operational structure. For example, it may not be clear to the client of a CASP the capacity in which the CASP is acting, particularly if the CASP combines multiple functions or works closely with a group of affiliated entities.

The type of disclosure by a CASP that may be important includes –

- The specific legal entity with whom the client is contracting;

- The specific services and activities that are being provided by the CASP and the relevant terms and conditions, and the role of the CASP when handling or executing clients' orders (e.g., whether as a principal or agent) and when holding in custody, moving, or making any use of Client Assets; and
- If the CASP is trading crypto-assets on behalf of its clients, the activities that the CASP engages in to effect the transactions, including whether the CASP, or its affiliates are engaging in market-making activities, whether any client trades will be made with the CASP or its affiliates on a principal basis, and how the CASP protects clients against front running trades;

If permitted to perform multiple functions in a vertically integrated manner (to the extent the regulator permits this combination of activities and functions), CASPs should identify and disclose the conflicts that the CASP has 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 (including a lack of protection from 'self-dealing' by the CASP, among others).

Chapter 2 Questions:

Question 3: ***– Does Chapter 2 adequately identify the potential conflicts of interest that may arise through a CASP's activities? What are other potential conflicts of interest which should be covered?***

Question 4: ***– Do respondents agree that conflicts of interest should be addressed, whether through mitigation, separation of activities in separate entities, or prohibition of conflicts? If not, please explain. Are there other ways to address conflicts of interest of CASPs that are not identified?***

Question 5: ***– Does Recommendation 3 sufficiently address the manner in which conflicts should be disclosed? If not, please explain.***

CHAPTER 3: RECOMMENDATIONS ON ORDER HANDLING AND TRADE DISCLOSURES (TRADING INTERMEDIARIES VS MARKET OPERATORS)

RECOMMENDATION FOR TRADING INTERMEDIARIES

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.

IOSCO Principles Supported: 29, 31

Despite common market parlance of collectively referring to CASPs as "exchanges" or "trading platforms", a CASP may not be an exchange (or commonly known as a market operator). It may operate as an intermediary such as a broker or dealer, or both. On the basis of "same activity, same risk and same regulatory outcome", specific recommendations should apply to CASPs based on the role that they undertake.

Information asymmetries and the lack of client disclosures arise due to a number of factors, including a lack of transparency by the CASP, and/or non-compliance with existing requirements concerning the role and capacity in which it is acting (particularly if it combines multiple activities and functions as described in the previous sections).

Clients may not understand that the CASP is trading against them and therefore is not acting in their best interests. Clients also may not understand that the CASP may be front-running client trades, or that it may not be providing the best price or execution for their trade. These inherent conflicts can give rise to significant investor harm.

To the extent not already addressed in regulation, regulators should require a CASP to implement systems, policies and procedures that provide for a fair, orderly and timely execution of client orders. Such systems, policies and procedures should be aligned with existing relevant securities and other regulations (e.g., requirements with respect to precedence of client orders and prohibition of front-running).

When requiring disclosure of such policies and procedures, to the extent not already addressed in regulation, regulators may consider requiring the CASP to perform the following in accordance with the regulators' authority:

- When entering an agreement to provide trade execution services to clients, disclose how the execution services will be done (e.g., executed on a principal or agency basis);
- Disclose to regulators and market participants, the order-routing procedures and how these are applied fairly (e.g., requirements with respect to precedence of client orders and prohibition of front-running);
- Disclose any arrangements in place with third parties for routing of client orders, including arrangements to disclose payment for order flow (PFOF), or any other forms of inducements;
- Take reasonable steps to deliver best execution for clients; and
- Disclose any significant differences from order handling rules applied to the trading of financial instruments on public markets in the jurisdiction of the client.

RECOMMENDATION FOR MARKET OPERATORS

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.

IOSCO Principles Supported: 33, 34, 35

In many jurisdictions, organized exchanges and trading venues are required to provide public trade transparency, for example, by displaying current bid and offer prices and the depth of trading interest.

Many CASPs are currently operating in non-compliance or in a manner inconsistent with existing regulations that apply to exchanges. This impedes critical trade transparency for transactions occurring on a CASP trading platform. This lack of information gives rise to a non-transparent market, not only with respect to pricing but also trading activities.

Regulators should require a CASP acting as a market operator to provide market participants/investors with access to an appropriate level of pre-trade and post-trade

information to promote transparency, price discovery, and competition. Regulators should consider how to provide investors with useful pre-trade information, including the bids and offers available on the CASP to enable crypto-asset investors to know, with a reasonable degree of certainty, whether and at what prices they can trade the crypto-assets.

Post-trade information on the prices, trade time and the volume of all individual transactions occurring on a CASP should be made publicly and freely available to the fullest extent practicable.

Chapter 3 Questions:

Question 6: ***– What effect would Recommendations 4 and 5 have on CASPs operating as trading intermediaries? Are there other alternatives that would address the issue of assuring that market participants and clients are treated fairly?***

Question 7: ***– Do respondents believe that CASPs should be able to engage in both roles (i.e. as a market operator and trading intermediary) without limitation? If yes, please explain how the conflicts can be effectively mitigated.***

Question 8: ***– Given many crypto-asset transactions occur "off-chain" how would respondents propose that CASPs identify and disclose all pre- and post-trade "off-chain" transactions?***

CHAPTER 4: RECOMMENDATIONS IN RELATION TO LISTING OF CRYPTO-ASSETS AND CERTAIN PRIMARY MARKET ACTIVITIES

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.

IOSCO Principles Supported: 16, 17

Substantive and procedural listing standards play a key role in investor and market protections in traditional markets. These standards for crypto-assets are just as important, as is the public availability of these standards.

As with traditional financial markets, the availability of ongoing information about the financial instrument (in this case, the crypto-asset) and about the issuer is key to informed decision-making and pricing in any trading market.

In the crypto-asset market today, many crypto-assets are sold without important disclosures about the crypto-asset and its issuer. Further, there tends to be little, if any, verifiable continuous information provided about or by the crypto-asset issuer. For those jurisdictions where existing rules apply already to crypto-asset issuers, including those relating to disclosures and protections against fraudulent statements, the crypto-assets are being sold in non-compliance with the law.

However, as crypto-asset trading activities implicate the same concerns as traditional financial markets, initial and ongoing information about crypto-assets and crypto-asset issuers is essential to avoid information asymmetries, to help protect against fraud, and to provide transparency to investors trading crypto-assets.

To address these issues from the trading platform standpoint, regulators should require a CASP to adopt substantive and procedural listing standards relating to crypto-assets and their issuers and describe the quantitative and/or qualitative standards that the CASP uses to assess a crypto-asset when approving the admission to trading, permitting it to continue to be admitted to trading, and standards for when its listing may be removed. The disclosures, as relevant, should

also include the procedures used to make those assessments.

In connection with the type of information that should be made available initially, and on an ongoing basis, about the crypto-asset, regulators may consider requiring the types of disclosures that apply when listing any financial instrument for trading on a traditional exchange.

This information would typically include, for example (but is not limited to), a comprehensive description of the crypto-asset, information about ownership and control of the crypto-asset, as well as full information about the issuer and its business, including audited financial statements, and information about the issuer's management team.

Regulators should require a CASP to also adequately disclose relevant information, including (but not limited to):

- Trading history of the crypto-asset, including volumes and prices;
- Operational description of the crypto-asset, including any incidents of manipulation or security failures;
- Token ownership concentration and any options and/or lock-ups for insiders and affiliates;
- Protocols for transfers; and
- The CASP's treatment of the client crypto-assets and their respective rights and entitlements when events such as, but not limited to, hard forks and airdrops occur.

These disclosures should apply and are important, even where there is no clearly identifiable entity issuing a crypto-asset.

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.

IOSCO Principles Supported: 29, 31, 33, 34

Currently, CASPs engage in a multitude of activities in a vertically integrated manner, many of which are being done in non-compliance with applicable law. Among the activities that CASPs

currently engage in are listing and trading crypto-assets that they issue or those of crypto- asset issuers in which they have, or acquire, a material interest. In these cases, CASPs have both a strong incentive and opportunity to influence the price discovery process, particularly when also acting as a market maker in the relevant crypto-asset. Such activities pose significant conflicts of interest and can give rise to significant investor harm.

The CASP engaging in these activities can have a significant economic interest in the success of the trading and related activities involving the crypto-asset. A CASP or an affiliate that has invested in a prospective enterprise and owns and trades the crypto-assets issued by that enterprise could have access to material non-public information and could have an incentive to use this information when engaging in trading activities. Even absent the misuse of any material inside information, the CASP may have an incentive to promote trading of the crypto-asset even if doing so might not be suitable for or in the best interests of its clients.

Regulators should consider requirements designed to mitigate these effects. The approach could include, for example, prohibitions on the CASP listing and/or trading such crypto-assets.[20]

Chapter 4 Questions:

<u>Question 9:</u> – Will the proposed listing/delisting recommendations in Chapter 4 enable robust public disclosure about traded crypto-assets? Are there other mechanisms that respondents would suggest to assure sufficient public disclosure and avoid information asymmetry among market participants?

<u>Question 10:</u> – Do respondents agree that there should be limitations, including prohibitions on CASPs listing and / or trading any crypto-assets in which they or their affiliates have a material interest? If not, please explain.

[20] in which the CASP has a material interest.

CHAPTER 5: RECOMMENDATIONS TO ADDRESS ABUSIVE BEHAVIORS

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.

IOSCO Principles Supported: 31, 33, 34, 35, 36

Regulation of traditional financial markets prohibits abusive practices that undermine market integrity. Three commonly observed types of abusive practices include (but are not necessarily limited to):

i. ***Unlawful disclosure of material, non-public information*** – Disclosing or 'tipping' inside information, except where strictly necessary and under appropriate conditions, allows those individuals to profit from this information and gives certain market participants an unfair advantage over others.

ii. ***Insider dealing*** – Trading based on 'inside' or material non-public information creates an unfair advantage due to the insiders privileged position at the expense of others.

iii. ***Market manipulation*** – Behaviors that create a false or misleading signal as to the supply, demand or price of a financial asset or otherwise impacts trading in the asset though any other form of deception or contrivance.

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. In some jurisdictions, these types of fraudulent and abusive practices in crypto-asset markets may already be covered by existing regulatory frameworks. New Frameworks should explore ways to impose such prohibitions, seeking alignment and consistency of outcomes when tackling market abuse in both traditional financial markets and crypto-asset markets.

Regulators should review their offence provisions and apply them as needed to deal with any potential gaps and new market developments.

Recommendation 9 *(Market Surveillance)*

Regulators should have market surveillance requirements applying to each CASP, so that market abuse risks are effectively mitigated.

IOSCO Principles Supported: 31, 33, 34, 36

Market surveillance is an important means to prevent or detect fraudulent or manipulative activity in traditional financial markets, and market surveillance for crypto-asset markets should provide a similar level of protection.

As with traditional financial markets, regulators should consider – to the extent that existing frameworks do not already apply – the following when evaluating market surveillance tools, systems and controls that should or already apply to CASPs:

- The timeliness of surveillance of transactions and orders to detect and prevent market abuse.
- Controls to take prompt remedial actions upon discovery of market abuse on their platform (e.g., suspension of trading).
- Systems for sharing information related to suspected market abuse between relevant crypto-asset markets.
- Systems to detect and report suspicious transactions and orders to the relevant body.
- Systems to identify malicious actors from a cyber and market integrity standpoint.
- Requirements, in line with FATF recommendations for AML-CTF, including (amongst other things) Customer Due Diligence Requirements.

Regulators should consider requiring proportionate additional systems and controls, based on the nature, scale and complexity of the CASP's business.

In evaluating whether market surveillance tools are effective, regulators should consider how to assure, amongst other things, oversight and verification of 'on-chain' and 'off-chain' transactions, including those transactions occurring directly on a crypto-asset trading platform

through the internal recordkeeping of ownership changes in omnibus accounts.[21] Regulators should evaluate different ways to engage in such oversight and verification, including requiring the detailed reporting of so-called 'off-chain activity' or settling of transactions on the internal books and records of the CASP, not reflected on the public ledger or blockchain.

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.

IOSCO Principles Supported: 31, 34, 36

As in traditional financial markets, a lack of controls on material non-public and market sensitive information, and a lack of restrictions on inappropriate use of such information, may result in manipulative market practices or insider trading.

This may be exacerbated by the cross-border nature of the crypto-asset market, for example, where a particular crypto-asset may be admitted on several trading platforms across jurisdictions, heightening the risk of regulatory arbitrage.

Regulators should thus require a CASP to put in place systems, policies and procedures around the management of material non-public information and to restrict inappropriate use of such information.

These could include the following:

- A process for the CASP to identify and classify information that is material non-public and market sensitive. Examples include, but are not limited to, information regarding the CASP's client orders and the planned listing of a particular crypto-asset;
- System and controls to restrict the access of material non-public and market sensitive information to a controlled list of persons on a 'need-to-know' basis, for example, via the use of ethical walls or information barriers;

[21] For the avoidance of doubt, this should apply to transactions arranged or executed by CASPs that provide custodial wallets as well as to those that do not.

- Periodic review of the list of persons who have access to material non-public and market sensitive information;
- Restrictions against the sharing and the use of material non-public and market sensitive information by the CASP and list of persons;
- Processes for monitoring for potential breach of the CASP's systems, policies and procedures policies regarding material non-public and market sensitive information, including, processes to facilitate whistleblowing and the reporting of potential breaches to the relevant authorities.

Chapter 5 Questions:

Question 11: *–*

In addition to the types of offences identified in Chapter 5, are there:

a) Other types of criminal or civil offences that should be specifically identified that are unique to crypto-asset markets, prevention of which would further limit market abuse behaviors and enhance integrity?

b) Any novel offences, or behaviors, specific to crypto-assets that are not present in traditional financial markets?

If so, please explain.

Question 12: *– Do the market surveillance requirements adequately address the identified market abuse risks? What additional measures may be needed to supplement Recommendation 9 to address any risks specific to crypto-asset market activities? Please consider both on- and off-chain transactions.*

CHAPTER 6: RECOMMENDATION ON CROSS-BORDER 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 cooperation arrangements and/or other mechanisms to engage with regulators and relevant authorities in other jurisdictions. These should accommodate the authorisation and on-going supervision of regulated CASPs, and enable broad assistance in enforcement investigations and related proceedings.

IOSCO Principles Supported: 13, 14, 15

Many CASPs offer services from offshore financial centers. CASPs often structure and present themselves as having little or no visible substantive presence within any jurisdiction, thus exacerbating supervisory and enforcement challenges that may arise. The provision of services into a jurisdiction by a CASP may nevertheless implicate that jurisdiction's laws.[22]

The differing approaches as well as the attempt by CASPs to avoid regulation or operate in non-compliance with existing regulation raise significant issues. This significantly increases the risk of regulatory arbitrage, reduces the ability of jurisdictions to enforce their laws, and depending on the laws of particular jurisdictions, potentially raises the prospect of jurisdictional borders hindering the effectiveness of the authorization and supervision process. This also enables money laundering risks and facilitates financial crime, and reduces the ability of regulators to effectively detect and enforce against these activities.

IOSCO is already active in tackling issues related to day-to-day cross-border cooperation between authorities. Crypto-asset related information requests are already captured by IOSCO's Multilateral Memorandum of Understanding (MMoU) and Enhanced Multilateral Memorandum of Understanding (EMMoU), premised on the underlying principle of same activity, same risk, same regulatory outcome. In tandem with the overarching MMoU and EMMoU, regulators should take proactive steps, bilateral or multilateral, to enable sharing of information for effective supervision and enforcement.

[22] It is recognized that the issues of international cooperation between regulators in view of the cross -border provision of crypto-asset services overlaps with issues being addressed in the separate proposal for a 20th anniversary review of the effectiveness of the IOSCO MMOU and the IOSCO Retail Market Conduct Task Force recommendations for further work on unauthorised provision of financial services.

Beyond the MMoU and EMMoU, regulators should also share information with one another and, where relevant, with law enforcement authorities, and work together to stop abusive and criminal behaviors, including financial crime and money laundering, and to mitigate risks to investors.

In addition, amongst wider measures to enhance cross border supervision of the market, regulators should consider bilateral and/or multilateral cooperation arrangements beyond the enforcement context, as appropriate, such as supervisory colleges[23] or networks,[24] or regional arrangements,[25] or other forms of cross-jurisdictional cooperation, to support rigorous and effective ongoing supervision of CASPs operating across multiple jurisdictions.

Chapter 6 questions

<u>Question 13:</u> – Which measures, or combination of measures, would be the most effective in supporting cross-border cooperation amongst authorities? What other measures should be considered that can strengthen cross-border co-operation?

[23] For example, IOSCO has mentioned potential consideration of supervisory colleges in connection with crypto-asset platforms. See: Lessons Learned from the Use of Global Supervisory Colleges, Final Report, IOSCO (January 2022), pp. 28-30, available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD696.pdf.

[24] See: Principles Regarding Cross-Border Supervisory Cooperation, Final Report, IOSCO (May 2010), pp. 31, 36-37, available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD322.pdf.

[25] For example, IOSCO APRC (Asia-Pacific Regional Committee) established the APRC Supervisory MMoU, which is the first IOSCO framework undertaken as part of efforts to strengthen supervisory cooperation in the Asia-Pacific region. The APRC Supervisory MMoU enables signatories to exchange broader supervisory information than under the MMoU, that is enforcement-focussed.

CHAPTER 7: RECOMMENDATIONS ON CUSTODY OF CLIENT MONIES AND ASSETS

Recommendation 12 – *(Overarching Custody Recommendation)*

Regulators should apply the IOSCO Recommendations Regarding the Protection of Client Assets[7] when considering the application of existing frameworks, or New Frameworks, covering CASPs that hold or safeguard Client Assets.

The proper custody of a Client Assets[26] is reliant on the strength of a service provider's systems, policies and procedures. 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.

As is the case with traditional financial assets, regulators should set out expectations that the CASP maintain 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. The records should also be maintained in such a way that they may be used as an audit trail.

A number of different methods and structures can be used by a CASP to hold Client Assets taking into account risk management, liquidity and efficiency considerations and trade-offs.

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.[27] When considering the maintenance of private keys, safety of Client Assets should be prioritized.

Ultimately, sufficient, reliable and clear information should be made available to clients and any third parties (for example insolvency practitioners, regulators and the courts) to enable them to understand the rights to any Client Assets, including the ability for clients to receive their Client Assets back, or an equivalent value thereof, should they suffer losses, for instance, due to the CASP entering an insolvency process.[28]

---

[26] For these purpose, "Client Assets" cover both money and crypto-assets held for, and on behalf of, a client.

[27] Further operational and technological considerations are set out under Recommendation 17.

[28] The outcomes for clients' rights to their assets depend on jurisdictional application of custody and trust arrangements; a CASP should therefore provide its clients with appropriate and accurate disclosure on their respective rights upon the CASP entering into an insolvency process.

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.

IOSCO Principles Supported: 31, 32, 38

Taking into account the technological means by which crypto-assets are created and held, laws and court decisions in certain jurisdictions might not yet have evolved in ways that provide CASP clients with legal certainty regarding protection of their crypto-assets.

Regulators should nonetheless require a CASP to segregate Client Assets from their proprietary assets, and place Client Assets in trust or in segregated bankruptcy remote accounts (or provide equivalent protection through legal or accounting mechanisms recognized in the relevant jurisdiction), so that they are separate and distinct from the CASP's own assets / estate.

Regulators should require a CASP to specify how Client Assets are protected against loss or misuse and how such assets are segregated as Client Assets that are not subject to the claims of the CASP's creditors.

Where the CASP expressly takes legal and / or beneficial title to Client Assets (for purposes, e.g., of lending, re-use or re-hypothecation of the crypto-assets), the CASP will cease to hold those Client Assets in trust for the client. The CASP should obtain the client's explicit prior consent to such arrangements. The CASP should provide clear, concise and non-technical disclosure of these arrangements, sufficient for the client to understand that Client Assets are not held in custody and might not be returned should the CASP enter insolvency.

Regulators should impose specific measures in situations where the CASP takes legal and/or beneficial ownership of Client Assets. These requirements should include, for example:

- receiving prior explicit consent from the client for the assets, for example, to be lent out, re-used or re-hypothecated;
- providing clients with clear, concise and non-technical, prior disclosure about the risks of these types of activities, including the potential loss of their entire crypto-asset holdings;

In all cases, whether a CASP is acting as a custodian holding Client Assets in trust, or in another

segregated arrangement, regulators should consider requiring CASPs to:

- maintain accurate and up-to-date records and accounts of Client Assets at all times that readily establish the precise nature, amount, location and ownership status of the assets, and identify the clients for whom they are held; and
- maintain records and accounts that enable it, on a frequent and regular basis, to specify each client's rights and the CASP's obligations to each client with respect to Client Assets.

``**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:

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.**

IOSCO Principles Supported: 31, 32, 38

Where a CASP is providing custody services to a client, regulators should require the CASP 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.[29] Regulators also should require the CASP to identify how the

[29] With respect to this recommendation, regulators should carefully consider how to ensure that the disclosure requirements do not require a CASP to reveal technical information that exposes it to heightened cybersecurity risks.

CASP protects the Client Assets, including from the claims of the CASPs 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.

For example, the regulator should require the CASP to disclose to its clients whenever Client Assets are to be held or placed in a foreign jurisdiction and thus become subject to the client asset protection and/or insolvency regimes of that foreign jurisdiction.

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.

IOSCO Principles Supported: 31, 32, 38

To support Recommendation 13 on the segregation and handling of Client Assets, 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, which may include (but not be limited to):

- policies and procedures governing the process and controls for Client Asset reconciliation;
- conducting reconciliations on a regular and frequent basis;
- procedures to reconcile off-chain and on-chain records;
- providing clients with a statement of account, comprising information on their Client Assets and transactions;
- engaging an independent auditor, on an annual basis,[30] to:

[30] These engagements should be performed by an independent auditor to obtain reasonable assurance about whether the subject matter information is free from material misstatement (e.g., with respect to the audit), or whether the CASP complied with the specified requirements, in all material respects (e.g., with respect to

- conduct an independent audit of the CASP's Client Asset environment; and
- issue an internal control report, including an opinion as to whether the CASP's controls related to custodial services—including the systems, processes and procedures for safeguarding of Client Assets —are designed and operating effectively; and
- conduct an independent review of the adequacy of CASPs' policies and procedures.

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.

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.

IOSCO Principles Supported: 31, 32, 38

Where a CASP does not have appropriate arrangements to safeguard Client Assets, this can increase the risk of loss, misuse, and delay in returning Client Assets, particularly in the case of an insolvency.

CASPs ostensibly operating as custodians have been hacked in the past and / or have lost the means to access Client Assets they were responsible for safeguarding. In particular, loss of a private key or wallet would mean that the corresponding Client Asset is not recoverable.

Proper custody of a Client Assets is reliant on the strength of a CASP's policies, procedures and controls, including the means of access (such as private keys and wallets). However a CASP is holding Client Assets, it should maintain adequate policies, procedures and arrangements to minimize risk of loss, theft or inaccessibility to Client Assets.

These policies and procedures should recognize the risks associated with different wallet types (e.g. hot, warm and cold).

the internal control report).

Regulators should consider whether and how a CASP can compensate its clients under applicable law, in the event of theft or loss of Client Assets. Depending on the jurisdiction, this could include requiring a CASP to hold sufficient assets to compensate clients (e.g., additional own funds and/or guarantee).

Chapter 7 Questions:

Question 14: ***– Do the Recommendations in Chapter 7 provide for adequate protection of customer crypto-assets held in custody by a CASP? If not, what other measures should be considered?***

Question 15: **–**

(a) Should the Recommendations in Chapter 7 address the manner in which the customer crypto-assets should be held?

(b) How should the Recommendations in Chapter 7 address, in the context of custody of customer crypto-assets, new technological and other developments regarding safeguarding of customer crypto-assets?

(c) What safeguards should a CASP put in place to ensure that they maintain accurate books and records of clients' crypto-assets held in custody at all times, including information held both on and off-chain?

(d) Should the Recommendations in Chapter 7 include a requirement for CASPs to have procedures in place for fair and reliable valuation of crypto-assets held in custody? If so, please explain why.

Question 16: ***– Should the Recommendations address particular safeguards that a CASP should put in place? If so, please provide examples.***

CHAPTER 8: RECOMMENDATION TO ADDRESS OPERATIONAL AND TECHNOLOGICAL RISKS

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.

IOSCO Principles Supported: 31, 32, 33, 34, 38

A CASP faces operational and technological risks similar to those faced by traditional financial institutions.[31]

However, crypto-asset activities may introduce some unique operational and technological risks, including those arising from the underlying DLT used for the issuance, trading and provision of services related to crypto-assets and the deployment of smart contracts, forks and use of cross-chain bridges. The disclosures contemplated by this Recommendation should address these risks, which are idiosyncratic to CASPs.[32] Regulators should require a CASP to put in place sufficient measures to address cyber and system resiliency. These measures should be reviewed at least annually and updated to help ensure that they remain strong and robust. Such measures could include:

- identifying the relevant operational and technological risks which the CASP faces and requiring the CASP to adopt appropriate processes and procedures to address such risks.
- implementing operational and technology risk management framework and

[31] For example, see IOSCO (2019), Cyber Task Force Final Report and see CPMI-IOSCO (2016), Guidance on cyber resilience for financial market infrastructures (FMI).

[32] With respect to this recommendation, regulators should carefully consider how to ensure that the disclosure requirements do not require a CASP to reveal technical information that exposes it to heightened cybersecurity risks.

conducting at least an annual independent audit.

- implementing frequent, rigorous code audits to mitigate cyber security risks.

Chapter 8 Questions:

<u>Question 17:</u> – Are there additional or unique technology/cyber/operational risks related to crypto-assets and the use of DLT which CASPs should take into account? If so, please explain.

<u>Question 18</u>: – Are there particular ways that CASPs should evaluate these risks and communicate these risks to retail investors? If so, please explain.

CHAPTER 9: RETAIL DISTRIBUTION RECOMMENDATION

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 a CASP to implement adequate systems, policies and procedures, and disclosure 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.

IOSCO Principles Supported: 16, 17, 23

Crypto-asset markets differ significantly from traditional financial markets in having a high proportion of retail participants directly accessing CASP trading platforms. Many of these crypto-assets and CASPs are operating in non-compliance with applicable law in some jurisdictions, where important retail client protections already exist.

Notwithstanding the applicability of existing regulatory frameworks – considering the cross-border nature of these activities and direct access business models – there are significant additional risks of mis-selling and exposure to fraud in crypto-asset markets, including difficulty in seeking recourse against CASPs and other market participants.

In developing New Frameworks, regulators should consider imposing requirements related to suitability / appropriateness assessments.[33] Further, regulators should consider how to evaluate CASP marketing materials and advertising about crypto-asset trading generally or particular crypto-assets.

If suitability / appropriateness assessments are used by the CASP, regulators should require that the assessments are well constructed and robust and do not give clients the false impression that they sufficiently understand the operations of crypto-asset markets and the related risks, when this is not the case.

33 If a prospective client does not demonstrate sufficient knowledge, the CASP should not permit trading of crypto- assets.

Clear, concise, non-technical and accurate disclosures should be provided on the key features and risks related to the crypto-assets and services offered by the CASP, as well as any fee, commission or incentive it charged.

Regulators should require CASPs to have an efficient and effective mechanism to address client complaints.

Chapter 9 Questions:

<u>Question 19:</u> – What other point of sale / distribution safeguards should be adopted when services are offered to retail investors?

<u>Question 20:</u> – Should regulators take steps to restrict advertisements and endorsements promoting crypto-assets? If so, what limitations should be considered?

CHAPTER 10: BOX TEXT ON STABLECOINS

What is a Stablecoin?

As defined by the FSB[34], a stablecoin is "a crypto-asset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets".

Stablecoins represent a large portion of the total market value for crypto-assets, and as a result there is a renewed focus on stablecoin arrangements. While stablecoin arrangements seek to achieve a particular characteristic (i.e., a stable value, in most cases tied to a fiat currency (e.g. U.S. Dollar), they are not technologically different from other types of crypto-assets. Stablecoins generally purport to be pegged or linked to one or more assets, in many cases fiat currency ("reference assets").

Despite claims by some stablecoin[35] issuers that the arrangements are "backed" or "collateralized" by reserve assets, it should be noted that several currently traded stablecoins are not in fact fully "backed" or "collateralized" by reserve assets. Therefore, stablecoin holders may not be entitled to any redemption right (at face value or otherwise) from the issuer of the stablecoin.

Stablecoin arrangements can take many forms and can reference one or more of the following asset types, or a combination of these asset types:

- Fiat currencies: stablecoins can reference one or more fiat currencies. The fiat currencies, or assets with equivalent fair value, may or may not be safeguarded by a custodian.
- Other real-world assets: stablecoins can reference other real-world assets, for example, securities, commodities, derivatives, real-estate, and/or other financial instruments and assets.

Finally, some stablecoins can also be pegged to and supported by other crypto-assets and/or market themselves as algorithmically controlled. An algorithmically controlled stablecoin is one that typically uses an algorithm to maintain price stability relative to the identified

34 See FSB (2020) Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements, available at https://www.fsb.org/2020/10/regulation-supervision-and-oversight-of-global-stablecoin-arrangements/

35 Generally, the issuer of a stablecoin is the entity responsible for designing the stablecoin, and managing the minting, issuance, redemption and supply of tokens. The stablecoin issuer also manages the reserve assets. The trading price, and therefore maintenance of the peg, occurs with respect to fiat stablecoins through trading activities and the ability of certain market participants to acquire newly minted stablecoins in exchange for fiat currency and to put stablecoins to issuers for redemption. Algorithmically controlled stablecoins use a different mechanism to maintain the peg.

reference asset by adjusting the supply of tokens as needed. These types of arrangements are not covered in this Chapter.

Uses of Stablecoins

Stablecoins are predominantly used to facilitate trading, lending and borrowing of crypto-assets, and are used as a perceived stable leg of a crypto-asset trading pair and as collateral in lending and borrowing arrangements, both on crypto-asset platforms and in DeFi applications and protocols. As such, stablecoins can play an important role in a CASP's operations.

Some have said that stablecoins may have the potential to be used for payments, outside of trading, lending and borrowing activities. At the same time, stablecoins may constitute a security. Issues involving stablecoins have been considered by a number of global organizations and standard setting bodies, including the FSB, IOSCO and CPMI-IOSCO because of the potential systemic impact they could have if used globally as a means of payment in commerce and because of their potential impact on investors and markets.

Risks of Stablecoins

Risks presented by crypto-assets are also relevant to stablecoins. In particular, there are risks addressed by these Recommendations, such as conflicts of interest, abusive behaviors, lack of operational resilience, information asymmetry, poor governance, lack of financial resilience and increased concentration risk.

However, stablecoins also present specific risks that differ from other crypto-assets due to their purported "stability" in relation to reference assets. These risks include those that flow from a lack of transparency, lack of verification of underlying reserve assets and potential for a "bank run" on the stablecoin.

Reserve Assets

There are risks that the reserve assets supporting a stablecoin might either be insufficient, or unavailable, to fund redemption requests, either when the issuer is a going concern, or when it is insolvent. The particular risks relating to reserve assets is enhanced in stablecoin arrangements in which the reserve assets are not held in a segregated manner and investors and other holders of stablecoins do not have a direct right of redemption from the issuer from dedicated and segregated reserve assets. The credit risk of the issuer in this scenario, which is the most common currently is significant given the lack of segregation of reserve assets from

other creditors of the stablecoin issuer. The particular risks relating to the sufficiency and/or viability of the reserve assets themselves could arise as a result of mismanagement of the reserve assets by the stablecoin issuer or due to market conditions. Even where the reserve assets are segregated, liquidity is a key risk in relation to the reserve assets as the reserve assets must be sufficiently liquid to enable issuers to use the reserve to fund redemption requests. A failure to fund such requests or loss of confidence could result in a "run" on the stablecoin. If the stablecoin issuer becomes insolvent, even stablecoin holders that have a direct right of redemption from an issuer may not be able to redeem their stablecoins, thus facing loss of their entire value. Stablecoin holders are subject to the credit risk of the stablecoin issuer if the reserve assets are not segregated and held for the crypto-asset holders in a way that protects the assets from other creditors of the stablecoin issuer. In this case, there may be no legal claim by the stablecoin holder as against the issuer or reserve.

Reserve assets of a financial nature, including deposits with banks or assets held with custodians, create an interdependence channel with traditional finance. This poses two-way risks – a run on a stablecoin may threaten the viability of an institution that holds the reserve assets as, for example, deposits. Similarly, the failure of a bank or custodian will mean that those reserve issues may become either illiquid or diminished for a period – and there is a risk of destabilizing the stablecoin, the stablecoin issuer and the wider crypto-asset market.

Rights of Holders

The use of stablecoins is dependent upon a holder having a direct right against the stablecoin issuer to obtain the fiat value of the stablecoin. However, many issuers of stablecoins place restrictions on the types of persons that can request redemptions or place a minimum value for redemptions. In many stablecoin structures, the stablecoin issuer will allow only larger institutions and crypto-asset trading platforms to interact directly with the stablecoin issuer to create and to redeem stablecoins. Other persons interested in holding stablecoins must acquire them in trading or similar activities from these third parties and may only look to these third parties, including crypto-asset trading platforms for repurchase or redemption of the stablecoins. As a result, stablecoin holders are subject to counterparty risk of the crypto-asset trading platforms in order to redeem their stablecoins. The rights of holders may not be clearly disclosed, whether by the issuer of the stablecoin or other parties, and holders of stablecoins do not have any rights relating to the operation of the stablecoin arrangement.

The majority of stablecoin distributions and trading occurs on secondary markets through CASPs and clients may not be aware of what rights they have and do not have against a stablecoin issuer. Further, a holder of a stablecoin may not understand that they are dependent on the continued viability and desire of CASPs to purchase stablecoins from them in order for them to sell or otherwise dispose of their stablecoin. Related to this issue is the fact that the pricing and, therefore, value of the stablecoin in the hands of the stablecoin holder is determined by secondary market trading and market sentiment. For example, the secondary market price of a stablecoin can "de-peg" due to market conditions, including sentiment, even if the issuer is fulfilling redemptions of certain market participants at par.

Money Laundering / Fraud / Scams

As with other crypto-assets, stablecoins may appeal to money launderers and criminals who do not wish to subject the proceeds of crime to traditional financial system oversight. Stablecoins are also likely to be perceived as more stable than other crypto-assets, so are more attractive to money launderers and criminals who do not wish to be as exposed to crypto-asset market volatility.

In light of the price instability of crypto-assets, because of their relatively more stable nature scammers have turned to stablecoins, and are soliciting stablecoins from their victims.

Applicable policy recommendations

Each of the Recommendations in this Consultation Report apply to stablecoins.[36] There are additional policy recommendations regarding stablecoins of which regulators should be cognizant. These include the forthcoming FSB Recommendations on the Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements[37] and CPMI-IOSCO's report on stablecoin arrangements, noting potential use cases of stablecoins as a payment instrument.

In applying these Recommendations, regulators should consider any unique issues, risks, and conflicts that CASPs have with regard to stablecoins.

The Recommendations regarding conflicts of interest, speculation, and disclosure are

[36] As noted in the preamble to Recommendation 1, particular jurisdictions may allocate responsibility for the regulation and oversight of certain kinds of stablecoins to different Regulators that possess discrete and complementary mandates and objectives, to address investor protection and market integrity risks.

[37] The FSB will publish finalized High-Level Recommendations in July 2023.

particularly important (Recommendations 2, 3, 7). For example, a CASP may be directly involved with a stablecoin issuer in creating and redeeming stablecoins, giving rise to potential misuse of inside information (Recommendation 8) and other conflicts. In addition, risks to crypto-asset trading markets and CASPs are directly affected by the credit risk of the stablecoin issuer. In addition, due to the central role of CASPs in keeping the stablecoin price at or near the applicable peg, Recommendation 8 is important.

Stablecoins may be used in market manipulation schemes, including involving other crypto-assets, because the price of stablecoins is determined through trading markets, where arbitrage trading keeps the price at or near the peg. The critical role of stablecoins in crypto-asset markets, and their potential to be used in cross-border activities, highlight the importance of cross border cooperation (Recommendation 11).

Additional Recommendation – Disclosure Concerning Stablecoins by CASPs

These issues point to the significance of the role of CASPs in deciding which stablecoins they list for trading and the disclosure recommendations regarding stablecoins listed for trading by CASPs. **Recommendation 6** should be read with the following guidance in relation to stablecoins. Regulators should consider requiring a CASP to disclose, as relevant:

1. The terms of the stablecoin including:

(a) what the stablecoin represents, including, the reserve assets, how the stablecoin is pegged and the reference asset for the peg (e.g., to a single fiat, a basket of currencies, etc.);

(b) the mechanism to support the peg, including whether the stablecoin is fully backed or supported by specific types of assets;

(c) the mechanisms for creating and redeeming the stablecoin;

(d) the rights of any and all stablecoin holders to present the stablecoin for redemption to the issuer, to the CASP or to other third parties, and any claims against the stablecoin issuer and/or against the reserve assets;

(e) whether a stablecoin holder has an enforceable direct claim against the issuer of the stablecoin; and

(f) whether and how the stablecoin holder can exchange their stablecoin, in a timely manner,

for underlying fiat currency, and any fees that may be levied in respect of this.

2. Risks relating to the stablecoin and stablecoin issuer including:

(a) whether there is segregation of reserve assets from the stablecoin issuer's own assets, protecting the stablecoin holder in event of the issuer's insolvency or bankruptcy;

(b) how the reserve assets are safeguarded and if known, who is holding the reserve assets and in what capacity, whether reserve assets are invested in other assets and the investment policy, along with other disclosures set out in Recommendation 14;

(c) what potential or actual conflicts of interest exist between the CASP and the stablecoin issuer and how those conflicts of interest are addressed;

(d) the regulatory status of the stablecoin in jurisdictions in which it is used;

(e) public transparency about the stablecoin issuer's reserve; and

(f) whether the issuer has provided an independently audited and complete set of financial statements that includes the reserve assets.

Additional Recommendation of custody for reserve assets of stablecoins

How reserve assets are held by the stablecoin issuer or others is of paramount importance, as is the fact that they remain sufficient to cover redemption of all outstanding stablecoins. The custody and client asset recommendations (Recommendations 12 – 16) should therefore be read, as relevant, as referring to reserve assets backing stablecoins as well as client assets. Given that a large part of the market for stablecoins is through stablecoins being purchased and sold through CASPs, rather than directly from and to a stablecoin issuer, the disclosures set out in **Recommendation 14**, as relevant, should be included in any disclosures to clients by CASPs as set out above.

Question 21: Are there additional features of stablecoins which should be considered under Chapter 10? If so, please explain.

Annex A: Questions for Consultation

Chapter	Question
Chapter 1 – Overarching Recommendation Addressed to All Regulators	***Question 1:** – Are there other activities and/or services in the crypto-asset markets which Recommendation 1 should cover? If so, please explain.* ***Question 2:** – Do respondents agree that regulators should take an outcomes-focused approach (which may include economic outcomes and structures) when they consider applying existing regulatory frameworks to, or adopting new frameworks for, crypto-asset markets?*
Chapter 2: Recommendations on Governance and Disclosure of Conflicts	***Question 3:** – Does Chapter 2 adequately identify the potential conflicts of interest that may arise through a CASP's activities? What are other potential conflicts of interest which should be covered?* ***Question 4:** – Do respondents agree that conflicts of interest should be addressed, whether through mitigation, separation of activities in separate entities, or prohibition of conflicts? If not, please explain. Are there other ways to address conflicts of interest of CASPs that are not identified?* ***Question 5:** – Does Recommendation 3 sufficiently address the manner in which conflicts should be disclosed? If not, please explain.*

Chapter 3 – Recommendations on Order Handling and Trade Disclosures ***(Trading Intermediaries vs Market Operators)***	***<u>Question 6:</u> – What effect would Recommendations 4 and 5 have on CASPs operating as trading intermediaries? Are there other alternatives that would address the issue of assuring that market participants and clients are treated fairly?*** ***<u>Question 7:</u> – Do respondents believe that CASPs should be able to engage in both roles (i.e. as a market operator and trading intermediary) without limitation? If yes, please explain how the conflicts can be effectively mitigated.*** ***<u>Question 8:</u> – Given many crypto-asset transactions occur "off-chain" how would respondents propose for CASPs to identify and disclose all pre- and post-trade "off-chain" transactions?***
Chapter 4 – Recommendations in Relation to Listing of Crypto-Assets and Certain Primary Market Activities	***<u>Question 9:</u> – Will the proposed listing/delisting disclosures in Chapter 4 enable robust public disclosure about traded crypto-assets? Are there other mechanisms that respondents would suggest to assure sufficient public disclosure and avoid information asymmetry among market participants?*** ***<u>Question 10:</u> – Do respondents agree that there should be limitations, including prohibitions on CASPs listing and / or trading any crypto-assets in which they or their affiliates have a material interest? If not, please explain.***
Chapter 5 – Recommendations	***<u>Question 11</u>: –***

to Address Abusive Behaviors	***In addition to the types of offences identified in Chapter 5, are there:*** ***c) other types of criminal or civil offences that should be specifically identified that are unique to crypto-asset markets, prevention of which would further limit market abuse behaviors and enhance integrity?*** ***d) any novel offences, or behaviors, specific to crypto-assets that are not present in traditional financial markets?*** ***If so, please explain.*** ***<u>Question 12:</u> – Do the market surveillance requirements adequately address the identified market abuse risks? What additional measures may be needed to supplement Recommendation 9 to address any risks specific to crypto-asset market activities? Please consider both on- and off-chain transactions.***
Chapter 6 – Recommendation on Cross-Border Cooperation	***<u>Question 13:</u> – Which measures, or combination of measures, would be the most effective in supporting cross-border cooperation amongst authorities? What other measures should be considered that can strengthen cross-border co-operation?***
Chapter 7 – Recommendations on Custody of	***<u>Question 14:</u> – Do the Recommendations in Chapter 7 provide for adequate protection of customer crypto-assets held in custody by a CASP? If not, what other measures should be considered?***

Client Monies and Assets	***<u>Question 15:</u> –*** ***<u>(a)</u> Should the Recommendations in Chapter 7 address the manner in which the customer crypto-assets should be held?*** ***<u>(b)</u> How should the Recommendations in Chapter 7 address, in the context of custody of customer crypto-assets, new technological and other developments regarding safeguarding of customer crypto-assets?*** ***<u>(c)</u> What safeguards should a CASP put in place to ensure that they maintain accurate books and records of clients' crypto-asset held in custody at all times, including information held both on and off-chain?*** ***<u>(d)</u> Should the Recommendations in Chapter 7 include a requirement for CASPs to have procedures in place for fair and reliable valuation of crypto-assets held in custody? If so, please explain why.*** ***<u>Question 16:</u> – Should the Recommendations address particular safeguards that a CASP should put in place? If so, please provide examples.***
Chapter 8 – Recommendation to Address Operational and	***<u>Question 17:</u> – Are there additional or unique technology/cyber/operational risks related to crypto-assets and the use of DLT which CASPs should take into account? If so, please explain.***

Technological Risks	***<u>Question 18</u>: – Are there particular ways that CASPs should evaluate these risks and communicate these risks to retail investors? If so, please explain.***
Chapter 9 – Recommendation for Retail Distribution	***<u>Question 19:</u> – What other point of sale / distribution safeguards should be adopted when services are offered to retail investors?*** ***<u>Question 20:</u> – Should regulators take steps to restrict advertisements and endorsements promoting crypto-assets? If so, what limitations should be considered?***
Chapter 10 – Box Text on Stablecoins	***<u>Question 21:</u> – Are there additional features of stablecoins which should be considered under Chapter 10? If so, please explain.***
Additional issues	***<u>Question 22:</u> – IOSCO also welcomes views from stakeholders on potential additional issues for consideration.***

Annex B: Recent Crypto Asset Market Events

The following are examples of recent events that highlight the types of issues that the Recommendations are intended to address.

1. **Stablecoins**

There have been a number of recent events involving stablecoins that highlight many risks for holders and for CASPs engaging with stablecoins. While in some cases, the events were as a result of actions of stablecoin issuers directly, others involved external events that affected stablecoin trading and pricing.

Below are two examples relating to fiat stablecoins.

Paxos and Binance USD (BUSD): In 2023, Paxos was ordered by the New York Department of Financial Services to stop new creations of BUSD. This event affected the continued ability of BUSD traders to engage in arbitrage activities that kept the BUSD price pegged to the US dollar.

Circle: Following adverse actions involving certain U.S.-regulated banks who held reserve assets backing Circle's USDC stablecoin. USDC issued by Circle suffered a "de-pegging event", where the traded value of the USDC was lower than its peg of $1 despite USDC still being redeemable from the issuer for $1. Public reporting indicated that this was due to concerns about Circle's access to a portion of its reserve assets. Circle subsequently issued public statements about their reserve assets.

These events, and others, demonstrate the importance of stablecoin disclosures. In the case of stablecoins, CASP clients may not be aware of their rights and risks when trading such assets.

2. **Vertically Integrated CASP Activities**

FTX: FTX operated a vertically integrated crypto-asset trading platform, and as noted in public reports engaged in allegedly fraudulent activities, including with respect to their customers' assets. FTX stated that it was operating a digital assets trading and exchange platform where users could enter into both spot transactions of cryptocurrency assets and also derivative products including 'perpetual futures', 'options', 'move contracts' and 'leveraged tokens'. FTX also was engaging in numerous other CASP activities, including broker dealer, custodian, clearing agent, and market making. FTX collapsed in November 2022 and filed for bankruptcy and insolvency in the U.S. and

in the Bahamas. The FTX failure, and the public reports about the types of activities that FTX and its affiliates engaged in, including with regarding to their customers assets, affiliated transactions, and trading activities, highlights the importance of the Recommendations.

Among other things, Samuel Bankman-Fried, the CEO and co-founder of FTX, along with other FTX executives, is alleged to have orchestrated a years-long fraud to conceal from FTX's investors (1) the undisclosed diversion of FTX customers' funds to Alameda Research LLC, Bankman-Fried's privately-held crypto hedge fund; (2) the undisclosed special treatment afforded to Alameda on the FTX platform, including providing Alameda with a virtually unlimited "line of credit" funded by the platform's customers and exempting Alameda from certain key FTX risk mitigation measures; and (3) undisclosed risk stemming from FTX's exposure to Alameda's significant holdings of overvalued, illiquid assets such as FTX-affiliated tokens. Bankman-Fried allegedly used commingled FTX customers' funds at Alameda to make undisclosed venture investments, lavish real estate purchases, and large political donations.

To highlight some of the potential operating issues within FTX, the provisional liquidators of one of the FTX entities, FTX Digital Markets Ltd (FTX Digital), which is in provisional liquidation in the Bahamas, have identified various activities of that firm which they consider warrant further review[38]. These include: (i) cash management to determine the basis on which customers deposits were placed with FTX Digital; (ii) antecedent transactions to determine whether any transactors were entered into by the company prior to the commencement of the liquidation which dissipated the value of the estate at the expense of the creditors; (iii) customer migration – whether customers of other FTX companies were migrated to FTX Digital; (iv) customer assets – the provisional liquidators have indicated that they will go to the Supreme Court of the Bahamas to determine whether the digital assets are owned by the customers, FTX Digital or another FTX Group entity; and (v) Platform IP ownership – to determine which parties hold ownership (or other) rights to the software code and/or various developments over time.

FTX and its principals have been charged with fraud, both civilly and criminally.

The alleged issues at FTX highlight the need for CASPs to comply with existing applicable regulations or be subjected to New Frameworks, as appropriate, and the importance of the Recommendations.

[38] Contained within the First Interim Report and Accounts of the Provisional Liquidators to the Supreme Court of the Bahamas.

Outcome for FTX Japan

Japanese customers held assets with FTX through a subsidiary, FTX Japan. These assets were frozen when FTX Trading entered into Chapter 11 in the US.

In February 2023, FTX Japan became the first FTX affiliate to allow customers to withdraw crypto assets and cash. This is because the Client Assets were properly held in accordance with Japanese regulations.

This outcome shows the importance of Recommendations 12 – 16 in provision of custody services.

Overall Regulatory Framework in Japan

The Japanese Regulator, the Financial Services Agency, had previously introduced requirements for crypto-asset markets including following custody requirements for CASPs:

- Segregation of customers' assets from those of CAESPs[39]
- Storage of the private key in a 'cold wallet' (for at least 95% of the entire customer's crypto-assets);
- Custody obligation of customers' cash held on trust;
- Publication of audited financial statements; and
- Preferential treatment of customers' crypto-assets over other creditors at the insolvency procedure.

3. Money laundering of dark web funds

Bitzlato: Bitzlato, a crypto-asset trading platform allegedly, knowingly conducted a significant part of its money transmitting business in the US, ignoring anti-money laundering (AML) laws and facilitating illicit fund transfers. In January 2023, the U.S. arrested Anatoly Legkodymov, the founder and owner of Bitzlato Limited on charges of facilitating money laundering of more than USD 700 million in dark web funds through the exchange. This was followed by an operation led by French and US authorities, supported by Europol, which so far has resulted in 5 individuals arrested (1 in Cyprus, 3 in Spain and 1 in the US).

39 'Crypto Assets Exchange Services Providers,' under the Japanese regulations.

The US Department of Justice[40] accuses the company and Legkodymov of failing to implement appropriate AML safeguards required by US law, such as know-your-customer (KYC) procedures and allowed "straw man" registrant information where the submission of identifying information was required. By only requiring a user's email, Bitzlato allegedly became an attractive option for "darknet" marketplaces such as Hydra, facilitating more than USD 700 million in cryptocurrency fund transfers for users of the Hydra marketplace.

These events highlight the value of various of the Recommendations in this report, such as the requirement for all crypto-asset firms to perform adequate levels of KYC and customer due diligence procedures to prevent the use of crypto-assets by criminals to launder funds (Recommendation 9), as well as cross-border cooperation (Recommendation 11). The implementation by countries of FATF Recommendation 15, including among other things the "Travel Rule," which requires virtual asset service providers and other financial institutions to share relevant originator and beneficiary information alongside virtual asset transactions, helping to mitigate AML/CTF risks posed by crypto-assets and CASPs.

4. Insider dealing and unlawful disclosure of inside information

Coinbase Employee: On 7 February 2023 Ishan Wahi, a former product manager at Coinbase who coordinated the platform's public crypto-asset listing announcements, pleaded guilty to two counts of conspiracy to commit wire fraud in connection with a scheme to commit insider trading in crypto-assets by using confidential Coinbase information about which crypto-assets were scheduled to be listed on Coinbase's exchanges[41]. The case was brought by the U.S. Department of Justice.

This case demonstrates how abusive behaviors seen in traditional financial markets, such as unlawful disclosure of inside information and insider dealing, can also occur in crypto-asset markets. It therefore highlights the importance of the Recommendations in having clear offences against these abusive behaviors, Recommendation 8 and the importance of CASP's having effective systems and controls to prevent and detect the abusive use of material non-public information.

---

40 https://www.justice.gov/usao-edny/pr/founder-and-majority-owner-bitzlato-cryptocurrency-exchange-charged-unlicensed-money

41 https://www.justice.gov/usao-sdny/pr/former-coinbase-insider-pleads-guilty-first-ever-cryptocurrency-insider-trading-case. Wahi and others were charged with insider trading by the U.S. SEC. https://www.sec.gov/news/press-release/2022-127.

5. CASP Non-compliance with Existing Securities Laws

Beaxy: In March 2023, the U.S. Securities and Exchange Commission (SEC) charged the crypto-asset trading platform beaxy.com (the Beaxy Platform) and its executives for failing to register as a national securities exchange, broker, and clearing agency under the U.S. federal securities laws. [42] The SEC also charged the founder of the platform, Artak Hamazaspyan, and a company he controlled, Beaxy Digital, Ltd., with raising $8 million in an unregistered offering of the Beaxy token (BXY) and alleged that Hamazaspyan misappropriated at least $900,000 for personal use, including gambling. Finally, the SEC charged market makers operating on the Beaxy Platform as unregistered dealers.

Bittrex: In April 2023, the SEC charged the crypto-asset trading platform Bittrex, Inc. and its co-founder and former CEO William Shihara for failing to register as a national securities exchange, broker, and clearing agency under the U.S. federal securities laws.[43] The SEC also charged Bittrex, Inc.'s foreign affiliate, Bittrex Global GmbH, for failing to register as a national securities exchange in connection with its operation of a single shared order book along with Bittrex. The complaint further alleges that Bittrex and Shihara, who was the company's CEO from 2014 to 2019, coordinated with issuers who sought to have their crypto-asset made available for trading on Bittrex's platform to first delete from public channels certain "problematic statements" that Shihara believed would lead a regulator, such as the SEC, to investigate the crypto-asset as the offering of a security.

As with FTX, the alleged Beaxy and Bittrex charges again highlight the need for CASPs to be regulated or comply with existing regulation, and the importance of the Recommendations contained in this report. All of the recommendations in this report are relevant and are intended to provide important investor and market protections.

---

42 https://www.sec.gov/news/press-release/2023-64

43 https://www.sec.gov/news/press-release/2023-78

Annex C: IOSCO Objectives and Principles for Securities Regulation

The 38 Principles of securities[44] regulation are based upon three objectives of securities regulation. These are:

- protecting clients[45];
- ensuring that markets are fair, efficient and transparent; and
- reducing systemic risk.

Application of IOSCO Principles

In pursuit of these core objectives, IOSCO members have resolved:

- to cooperate in developing, implementing and promoting adherence to internationally recognized and consistent standards of regulation, oversight and enforcement in order to protect investors, maintain fair, efficient and transparent markets, and seek to address systemic risks;
- to enhance investor protection and promote investor confidence in the integrity of securities markets, through strengthened information exchange and cooperation in enforcement against misconduct and in supervision of markets and market intermediaries; and
- to exchange information at both global and regional levels on their respective experiences in order to assist the development of markets, strengthen market infrastructure and implement appropriate regulation.

44 For convenience, the words 'securities markets' are used, where the context permits, to refer compendiously to the various market sectors. In particular, where the context permits, they should be understood to include reference to the derivatives markets. The same applies to the use of the words "securities regulation." (See IOSCO By-Laws, Explanatory Memorandum).

45 The term "client" is intended to cover all persons using the services of a CASP, including the term customer, whether retail or otherwise.

As part of the pre-consultation development process, IOSCO undertook an exercise to map the IOSCO Principles[46], Methodology[47] and underlying reports and outputs to activities and functions of crypto-asset markets.

This mapping exercise builds on the extensive range of outputs from IOSCO which bear relevance for crypto-asset market activities including, but not limited to –

- IOSCO Decentralized Finance (DeFi) Report
- IOSCO Report on Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms
- IOSCO Principles on Outsourcing
- IOSCO Cyber Task Force Final Report
- CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures (FMI)
- IOSCO Consultative Report on Principles for the Regulation and Supervision of Commodity Derivatives Markets
- IOSCO Recommendations Regarding the Protection of Client Assets
- IOSCO Risk Mitigation Standards for Noncentrally Cleared OTC Derivatives
- Mechanisms for Trading Venues to Effectively Manage Electronic Trading Risks and Plans for Business Continuity
- Market Intermediary Business Continuity and Recovery Planning.

The IOSCO Objectives and Principles of Securities Regulation ('The IOSCO Principles' / 'Principles') have been endorsed by both the G20 and the Financial Stability Board (FSB) as the relevant standards in this area.

The IOSCO Principles are IOSCO's main instrument to develop and implement internationally recognized and consistent standards of regulation, oversight and enforcement. Compliance with the Principles form the bedrock for our policy approach and enable effective supervision and enforcement in line with IOSCO's core objectives, set out

46 IOSCO Principles – https://www.iosco.org/library/pubdocs/pdf/IOSCOPD561.pdf

47 IOSCO Methodology – https://www.iosco.org/library/pubdocs/pdf/IOSCOPD562.pdf

above.

These principles are built into the domestic frameworks implemented by securities markets regulators across the globe. This is important as they form the basis for the evaluation of the securities sector for the Financial Sector Assessment Programs (FSAPs) of the International Monetary Fund (IMF) and the World Bank. The IOSCO Principles cover 10 core categories of securities markets as follows:

A. Principles Relating to the Regulator (1-8)
B. Principles for Self-Regulation (9)
C. Principles for the Enforcement of Securities Regulation (10-12)
D. Principles for Cooperation in Regulation (13-15)
E. Principles for Issuers (16-18)
F. Principles for Auditors, Credit Rating Agencies, and Other Information Service Providers (19-23)
G. Principles for Collective Investment Schemes (24-28)
H. Principles for Market Intermediaries (28-32)
I. Principles for Secondary and Other Market (33-37)
J. Principles Relating to Clearing and Settlement (38)

While the majority of the IOSCO Principles apply mutatis mutandis, there are certain issues at play in crypto-asset markets which may necessitate more targeted guidance and Policy Recommendations. See below for a more detailed overview of these principles.

A. Principles Relating to the Regulator

1	The responsibilities of the Regulator should be clear and objectively stated.
2	The Regulator should be operationally independent and accountable in the exercise of its functions and powers.
3	The Regulator should have adequate powers, proper resources and the capacity to perform its functions and exercise its powers.
4	The Regulator should adopt clear and consistent regulatory processes.
5	The staff of the Regulator should observe the highest professional standards, including appropriate standards of confidentiality.
6	The Regulator should have or contribute to a process to identify, monitor, mitigate and manage systemic risk, appropriate to its mandate.
7	The Regulator should have or contribute to a process to review the perimeter of regulation regularly.
8	The Regulator should seek to ensure that conflicts of interest and misalignment of incentives are avoided, eliminated, disclosed or otherwise managed.

B. Principles for Self-Regulation

9	Where the regulatory system makes use of Self-Regulatory Organizations (SROs) that exercise some direct oversight responsibility for their respective areas of competence, such SROs should be subject to the oversight of the Regulator and should observe standards of fairness and confidentiality when exercising powers and delegated responsibilities.

C. Principles for the Enforcement of Securities Regulation

10	The Regulator should have comprehensive inspection, investigation and surveillance powers.

11	The Regulator should have comprehensive enforcement powers.
12	The regulatory system should ensure an effective and credible use of inspection, investigation, surveillance and enforcement powers and implementation of an effective compliance program.

D. Principles for Cooperation in Regulation

13	The Regulator should have authority to share both public and non-public information with domestic and foreign counterparts.
14	Regulators should establish information sharing mechanisms that set out when and how they will share both public and non-public information with their domestic and foreign counterparts.
15	The regulatory system should allow for assistance to be provided to foreign Regulators who need to make inquiries in the discharge of their functions and exercise of their powers.

E. Principles for Issuers

16	There should be full, accurate and timely disclosure of financial results, risk and other information which is material to investors' decisions.
17	Holders of securities in a company should be treated in a fair and equitable manner.
18	Accounting standards used by issuers to prepare financial statements should be of a high and internationally acceptable standard.

F. Principles for Auditors, Credit Rating Agencies, and other information service providers

19	Auditors should be subject to adequate levels of oversight.
20	Auditors should be independent of the issuing entity that they audit.
21	Audit standards should be of a high and internationally acceptable quality.

22	Credit rating agencies should be subject to adequate levels of oversight. The regulatory system should ensure that credit rating agencies whose ratings are used for regulatory purposes are subject to registration and ongoing supervision.
23	Other entities that offer investors analytical or evaluative services should be subject to oversight and regulation appropriate to the impact their activities have on the market or the degree to which the regulatory system relies on them.

G. Principles for Collective Investment Schemes

24	The regulatory system should set standards for the eligibility, governance, organization and operational conduct of those who wish to market or operate a collective investment scheme.
25	The regulatory system should provide for rules governing the legal form and structure of collective investment schemes and the segregation and protection of client assets.
26	Regulation should require disclosure, as set forth under the principles for issuers, which is necessary to evaluate the suitability of a collective investment scheme for a particular investor and the value of the investor's interest in the scheme.
27	Regulation should ensure that there is a proper and disclosed basis for asset valuation and the pricing and the redemption of units in a collective investment scheme.
28	Regulation should ensure that hedge funds and/or hedge fund managers/advisers are subject to appropriate oversight.

H. Principles for Market Intermediaries

29	Regulation should provide for minimum entry standards for market intermediaries.
30	There should be initial and ongoing capital and other prudential requirements for market intermediaries that reflect the risks that the intermediaries undertake.
31	Market intermediaries should be required to establish an internal function that delivers compliance with standards for internal organization and operational conduct, with the aim of protecting interests of clients and their assets and ensuring proper management

	of risk, through which management of the intermediary accepts primary responsibility for these matters.
32	There should be procedures for dealing with the failure of a market intermediary in order to minimize damage and loss to investors and to contain systemic risk.

I. Principles for Secondary and Other Markets

33	The establishment of trading systems including securities exchanges should be subject to regulatory authorization and oversight.
34	There should be ongoing regulatory supervision of exchanges and trading systems which should aim to ensure that the integrity of trading is maintained through fair and equitable rules that strike an appropriate balance between the demands of different market participants.
35	Regulation should promote transparency of trading.
36	Regulation should be designed to detect and deter manipulation and other unfair trading practices.
37	Regulation should aim to ensure the proper management of large exposures, default risk and market disruption.

J. Principles Relating to Clearing and Settlement

38	Securities settlement systems, central securities depositories, trade repositories and central counterparties should be subject to regulatory and supervisory requirements that are designed to ensure that they are fair, effective and efficient and that they reduce systemic risk.