FSB FINANCIAL STABILITY BOARD

Thematic Review on FSB Global Regulatory Framework for Crypto-asset Activities

Peer review report

16 October 2025

The Financial Stability Board (FSB) coordinates at the international level the work of national financial authorities and international standard-setting bodies in order to develop and promote the implementation of effective regulatory, supervisory and other financial sector policies. Its mandate is set out in the FSB Charter, which governs the policymaking and related activities of the FSB. These activities, including any decisions reached in their context, shall not be binding or give rise to any legal rights or obligations.

Contact the Financial Stability Board

Sign up for e-mail alerts: www.fsb.org/emailalert
Follow the FSB on X/Twitter: @FinStbBoard
E-mail the FSB at: fsb@fsb.org

Foreword

Financial Stability Board (FSB) member jurisdictions, under the FSB Charter and in the *FSB Framework for Strengthening Adherence to International Standards,*[1] have made commitments in relation to leading by example by implementing international financial standards, disclosing their level of adherence to those standards and undergoing periodic peer reviews to evaluate adherence to these standards. To fulfil this responsibility, the FSB has established a regular programme of country and thematic peer reviews of its member jurisdictions.

Thematic reviews focus on the implementation and effectiveness across the FSB membership of international financial standards developed by standard-setting bodies (SSBs) and policies agreed within the FSB in a particular area important for global financial stability. Thematic reviews may also analyse other areas important for global financial stability where international standards or policies do not yet exist. The objectives of the reviews are to encourage consistent cross-jurisdiction and cross-sector implementation; to evaluate (where possible) the extent to which standards and policies have had their intended results; and to identify gaps and weaknesses in reviewed areas and to make recommendations for potential follow-up (including through the development of new standards) by FSB members.

This report describes the findings of the peer review on implementation of the FSB's global regulatory framework for crypto-asset activities, including progress to implement comprehensive regulatory frameworks for crypto-asset service providers and stablecoin arrangements, data reporting and collection, and cross-border cooperation and coordination. This peer review focused on evaluating the progress of implementation rather than the effectiveness of the regulatory approaches undertaken by jurisdictions. The review is based on the objectives and guidelines for the conduct of peer reviews set forth in the *Handbook for FSB Peer Reviews.*[2] The analysis and conclusions of this peer review reflect information as of August 2025 unless otherwise noted and includes the key elements of the discussion of the FSB Standing Committee on Standards Implementation (SCSI) in September 2025.

The draft report for discussion by SCSI was prepared by a team chaired by Arthur Yuen (Hong Kong Monetary Authority). The team comprised Olivier Brochand (Autorité des Marchés Financiers, France), Manisha Sinha (Ministry of Finance, India), Taro Kimura (Financial Services Agency, Japan), Mohsen Al-Zahrani (Saudi Central Bank), Benjamin Zheng (Monetary Authority of Singapore), Diego Hernández (Banco de España), Jane Moore (Financial Conduct Authority, United Kingdom), John Levin (Federal Reserve Bank of Boston, United States), Nico Di Gabriele (European Central Bank), Parma Bains (International Monetary Fund), Dorothee Delort (World Bank Group) and a staff member from the Office of the Comptroller of the Currency, United States. Peter Goodrich, Michael Januska, Lara Douglas and Terence Choy (FSB Secretariat) provided support to the team and contributed to the preparation of the report.

---

1 FSB (2010), *FSB Framework for Strengthening Adherence to International Standards*, January.

2 FSB (2017), *Handbook for FSB Peer Reviews*, April.

Executive summary

The FSB published its global regulatory framework for crypto-asset activities in July 2023. This framework consists of high-level recommendations for the regulation, supervision and oversight of crypto-asset markets and activities (CA recommendations) and revised high-level recommendations for the regulation, supervision and oversight of global stablecoin arrangements (GSC recommendations). This report reviews implementation progress by FSB jurisdictions and some volunteering non-FSB jurisdictions.

Crypto-asset markets and regulation are changing rapidly and this point-in-time analysis of implementation of the CA and GSC recommendations is instructive as it demonstrates progress made by these jurisdictions in regulating crypto-asset activities and global stablecoin arrangements (GSCs) but reveals significant gaps and inconsistencies that could pose risks to financial stability and to the development of a resilient digital asset ecosystem. While jurisdictions have made notable advancements toward implementing the CA recommendations, few have finalised their regulatory frameworks for GSCs (see Table 1). Moreover, even where regulatory frameworks are finalised, full alignment with the FSB recommendations remains limited and jurisdictions may continue to update, modify, or refine their frameworks. Uneven implementation creates opportunities for regulatory arbitrage and complicates oversight of the inherently global and evolving crypto-asset market.

For crypto-asset activities, gaps remain in addressing financial stability risks, particularly in the regulation of crypto-asset service providers (CASPs). Comprehensive coverage of potentially higher risk activities, such as borrowing, lending, and margin trading, is often lacking. In addition, gaps or the lack of comprehensive reporting frameworks for CASPs hinder authorities' ability to monitor and address potential financial stability risks effectively. Moreover, supervision and enforcement efforts lag behind regulatory development, with many jurisdictions yet to implement the tools necessary for ensuring compliance and oversight.

The regulation of GSCs similarly reflects a fragmented and inconsistent landscape. Implementation progress has been slow, as relatively few jurisdictions have established comprehensive regulatory frameworks for GSCs. This is largely because jurisdictions' existing regulatory mandates and tools are unlikely to comprehensively address the risks of GSCs and align with the GSC recommendations. As a result, jurisdictions are recognising that they should develop tailored regulatory frameworks that treat stablecoins as distinct payment instruments. However, few of these tailored frameworks are fully aligned with the GSC recommendations, and critical gaps include insufficient requirements for robust risk management practices, capital buffers, and recovery and resolution planning (including insolvency frameworks). Variations across jurisdictions in redemption and custody requirements, the timing and details of disclosures, as well as reserve collateralisation frameworks pose particular regulatory and supervisory challenges for stablecoin arrangements that operate across multiple jurisdictions.

Finally, cross-border cooperation and coordination is fragmented, inconsistent, and insufficient to address the global nature of crypto-asset markets, due in part to the fact that implementation efforts are still ongoing. Authorities are leveraging existing mechanisms for enforcement and licensing purposes, but these mechanisms rarely extend to broader supervisory objectives or financial stability monitoring. Partly in reflection of the early-stage nature of regulatory

approaches to evolving crypto-asset markets, fragmented responsibilities among domestic authorities, divergent definitions of crypto-assets, and legal barriers such as secrecy or privacy laws threaten to impede effective information sharing. These shortcomings constrain effective and comprehensive oversight of cross-border crypto-asset activities and may delay coordinated responses to potential systemic risks.

Table 1: Overall implementation status of CA and GSC recommendations

		CA Recommendations		GSC Recommendations	
Stages of progress*		Jurisdictions**	Count	Jurisdictions**	Count
1	*No framework in place*	**China^, India,** Kazakhstan, Lebanon, **Mexico, Saudi Arabia^**	**6**	**Argentina,** Chile, **China^, India, Indonesia**, Kazakhstan, Lebanon, **Mexico, Saudi Arabia^, South Africa, Türkiye**	**11**
2	*Partial regulations in place*	**Argentina, Canada, South Africa**	**3**	**Canada,** Philippines, Thailand	**3**
3	*Plans for framework under public discussion*	**Brazil, Korea***, Switzerland***,** Uruguay	**4**	**Australia***, Brazil, Korea,** Nigeria, **Switzerland***,** Uruguay	**6**
4	*Framework proposed but not finalised*	Armenia, **Australia***,** Philippines, **UK**	**4**	Armenia, **Singapore***, UK, US**	**4**
5	*Regulatory framework finalised*	The Bahamas, Bermuda, Chile, **EU, Hong Kong, Indonesia, Japan**, Nigeria, **Singapore,** Thailand, **Türkiye**	**11**	The Bahamas, Bermuda, **EU, Hong Kong, Japan**	**5**

*The stages of progress reflect a jurisdiction's overall implementation progress and are not an assessment of compliance with each CA or GSC recommendations nor of effectiveness. For definitions of each stage, see Annex 1.

FSB member jurisdictions are **bolded.

***Indicates a jurisdiction where partial regulations are also in place.

^ Indicates a jurisdiction where crypto-asset activities are prohibited.

Recommendations

Based on the findings described in this report, there are eight recommendations, which are addressed to jurisdictions as they develop their regulatory regimes, and to the FSB, SSBs, and international organisations as they consider further work on the subject.

Implementation Progress

1. Jurisdictions should review their current plans to ensure that, when implemented, they will amount to full implementation of the FSB Crypto Framework. They should also prioritise their implementation of the FSB Crypto Framework given the rapid pace of developments in the crypto-asset markets, drawing reference from the good practices identified in the peer review report to monitor and safeguard global financial stability.

2. The FSB, as well as the other SSBs and international organisations, should continue to promote comprehensive and aligned implementation of the FSB Crypto Framework, including by engaging with jurisdictions beyond the FSB membership, particularly those not covered in this review, in which implementation progress remains unknown.

Comprehensiveness of regulatory frameworks

3. Jurisdictions that have implemented or are currently developing a regulatory framework for CASPs should close any identified gaps, based on a comprehensive gap analysis or other appropriate assessment against the FSB's 2023 CA recommendations, in particular regarding CASP activities that give rise to financial stability risks and implement the supervisory reporting requirements that are relevant in their jurisdiction.

4. Jurisdictions that have implemented or are currently developing a regulatory framework for GSCs should close any identified gaps, based on a comprehensive gap analysis or other appropriate assessment against the 2023 GSC recommendations, in particular requirements for liquidity risk management, capital buffers, stress testing, user redemption, custody of and eligibility for the reserve of assets, and recovery and resolution planning (including insolvency frameworks).

5. Jurisdictions should improve their data capabilities and infrastructure to be able to monitor financial stability risks within the crypto-asset market and between the crypto-asset market and traditional financial markets, including by leveraging regulatory and supervisory reporting from CASPs, stablecoin issuers, and other market participants to close data gaps.

Consistency

6. In the course of its further work, and as appropriate, the FSB should work closely with the SSBs and international organisations to consider ways to promote further alignment of regulatory approaches and frameworks for stablecoin arrangements, including through information sharing to facilitate capacity building, as well as analysis of the vulnerabilities stemming from GSCs with multi-jurisdictional issuances.

Cross-border cooperation and coordination

7. At the appropriate time, jurisdictions should conduct an assessment of the scale and nature of cross-border crypto-asset activities into and out of their jurisdictions. Based on this assessment, jurisdictions should utilise existing tools available to engage in cross-border cooperation, develop (as needed) bilateral and multilateral arrangements to ensure pro-active cross-sectoral and cross-border cooperation, and consider if any additional tools for cooperation across borders might be needed to deal with the corresponding cross-border risks.

8. In the course of its further work, the FSB, as well as relevant SSBs, should consider potential best practices and solutions to fully implement CA and GSC recommendation 3 and to address the challenges identified in this report and promote the wider adoption of those best practices and solutions to achieve more effective cross-border cooperation and coordination.

1. Introduction

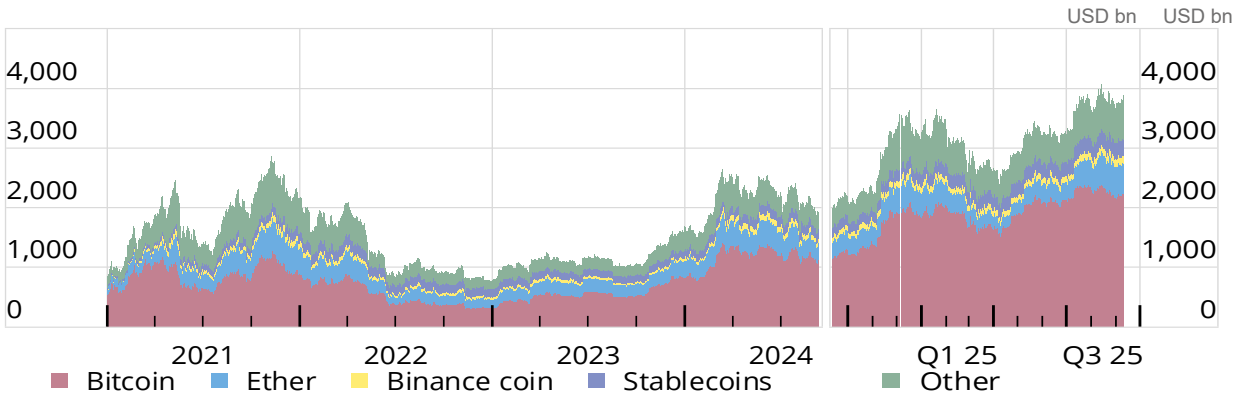
Recent developments in crypto-asset markets

The rapid evolution and growth of crypto-asset markets underscores the importance of implementing the FSB's recommendations for crypto-assets (CAs) and global stablecoins (GSCs). While financial stability risks from crypto-assets appear limited at present, growing interlinkages with the traditional financial system and the expanding use cases for stablecoins highlight the need for close monitoring of developments and activity and robust regulatory oversight. Recent developments in these markets reflect both their significant growth and their increasing integration into financial systems, which, if left unchecked, could amplify vulnerabilities and introduce new risks to financial stability.

The total market value of crypto-assets has increased sharply in recent months, reaching approximately USD 4 trillion in early August, almost doubling that from a year ago (see Graph 1). Much of the growth reflects a more permissive regulatory environment for crypto-assets, as seen through an increase in the market value of Bitcoin and other unbacked crypto-assets, which accounted for over 90% of the total market value. While still small in comparison, stablecoins – particularly those backed by US dollar assets – have grown by almost three-quarters over the past year to just under USD 290 billion.

Developments in the crypto-assets and stablecoins market

Daily crypto-asset market value — **Graph 1**



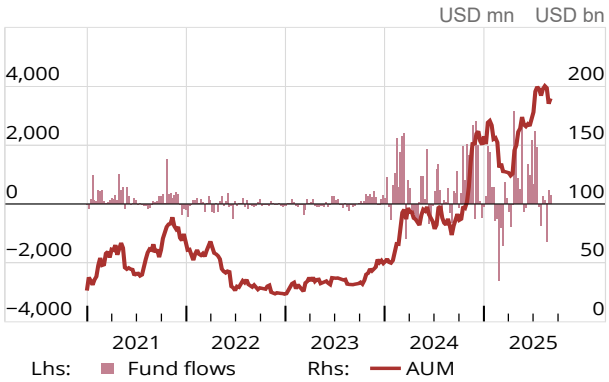
Source: CCData, FSB calculations.

Despite their strong growth, crypto-assets and stablecoins are still not widely used in critical financial functions and shared services supporting the real economy (such as payments), and decentralised finance (DeFi) remains a niche market segment. However, linkages between crypto-assets and the traditional financial system are growing. While this may reflect that financial institutions and retail investors expect benefits from increasing such linkages, they may also increase the risk that major shocks from the crypto-asset ecosystem spillover to the broader financial sector through various transmission channels. For instance, investors are increasingly gaining exposure to crypto-assets via traditional financial markets, such as via exchange-traded products (ETPs) or purchasing the equities of listed firms holding large quantities of crypto-

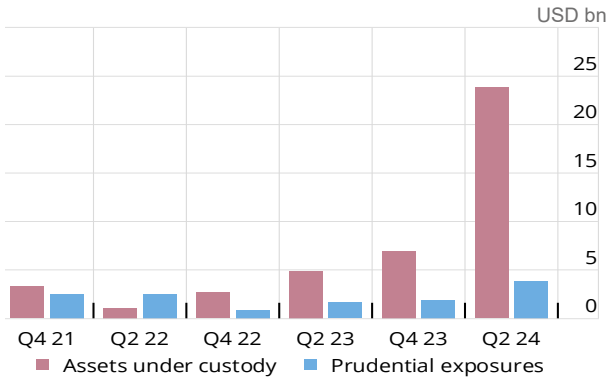
assets on their balance sheet, some of which are debt-funded (see Graph 2).[3] In addition, large global banks' prudential exposures to and custody of crypto-assets have increased significantly, albeit from a low base. An increasing number of major financial institutions have also announced products or partnerships to integrate stablecoins into payment and settlement services, issue proprietary stablecoins, or provide investment services for crypto-assets, thus increasing their exposure to the crypto-asset ecosystem further.

Growing interlinkages between crypto-assets and financial system **Graph 2**

A. Weekly fund flows and AUM of crypto-asset funds[1]



B. Prudential exposures and assets under custody by the largest global banks[2]



1 Include trusts, closed-end funds, derivative based funds, and ETPs. 2 Sample includes 29 large global banks as of Q2 2024.

Source: BCBS; Bloomberg.

While stablecoins are not yet widely used to facilitate real economic activities – such as payments – stablecoin issuers are becoming significant players in traditional financial markets via their substantial reserve holdings, which has become comparable to those from foreign governments or large money market funds.[4] This concentration of holdings among a few stablecoin issuers, particularly at the very short end of the yield curve, raises concerns about potential market disruptions during periods of stress. Stablecoin issuers may be forced to liquidate reserves rapidly to meet redemption requests. Continued growth in stablecoins requires close monitoring of developments and robust regulatory safeguards, especially given their growing use cases (particularly in emerging market and developing economies (EMDEs)), potential for bank disintermediation via deposit displacement, and risks that may arise from certain business models that issue stablecoins across multiple jurisdictions and therefore may need to manage reserves across jurisdictional borders.

Background and rationale of this report

The G20, during India's Presidency in 2023, charged the FSB with coordinating the delivery of an effective and comprehensive regulatory framework for crypto-assets. In consultation with standard-setting bodies (SSBs) and international organisations, the FSB finalised in 2023 a global regulatory framework for crypto-asset activities based on the principle of 'same activity, same risk,

3 Listed firms employing this strategy currently hold USD 117 billion worth of Bitcoin on their balance sheet and have raised or announced they will raise USD 100 billion in funding for this strategy in 2025 alone. See Financial Times (2025), *Why struggling companies are loading up on Bitcoin*, August; and BitcoinTreasuries.net.

4 See Circle Internet Financial (2025), Transparency & stability, July; Tether (2025), Transparency, July; and Department of US Treasury (2025), *US Treasury Monthly Statement of the Public Debt*, August.

same regulation.' This framework consists of high-level recommendations for the regulation, supervision and oversight of crypto-asset markets and activities (CA recommendations) and revised high-level recommendations for the regulation, supervision and oversight of GSCs (GSC recommendations).[5]

The FSB in 2023 committed to conducting, by end-2025, a review of the status of the review implementation of the CA and GSC recommendations. The FSB was subsequently asked by South Africa's 2025 G20 Presidency to deliver this review to the G20.

In line with the mandate of the FSB, the focus of the CA and GSC recommendations, and this peer review, is on regulatory, supervisory and oversight frameworks relating to crypto-assets activities, including stablecoins, that address financial stability concerns. The report therefore does not comprehensively address all specific risk categories related to crypto-asset activities, such as: money laundering/ terrorism financing (ML/TF); data privacy; cyber security; consumer and investor protection; market integrity; competition policy; taxation; monetary policy; monetary sovereignty; and other macroeconomic concerns.[6] Macro-financial policies, financial regulation, and additional policy and regulatory considerations to address legal risks, financial integrity, market integrity, and investor protection are all essential elements of an effective policy framework for crypto-assets, including stablecoins.

This peer review focuses particularly on jurisdictions' implementation of the following aspects of the FSB Crypto Framework:

- Regulatory frameworks and implementation status (powers, mandates, resources), e.g. CA and GSC recommendations 1 and 2;
- Data reporting (availability of data reporting requirements and granularity), e.g. CA recommendations 6-8 and GSC recommendations 6 and 8;
- Cross-border cooperation (applicable arrangements and their use), e.g. CA and GSC recommendations 1 and 3; and
- Stablecoins, which are included as part of the above topics in addition to more specific aspects of stablecoin regulations (e.g. GSC recommendation 9).

The primary source of information for the peer review was responses to a questionnaire by authorities in FSB jurisdictions, and by the European Commission and the European Central Bank (ECB). Given the concurrent passage of congressional legislation and the publication of the US President's Working Group report "Strengthening American Leadership in Digital Financial Technology" (US President's Working Group on Digital Asset Markets Report),[7] the US did not provide a response to the questionnaire. Instead, to accommodate policy changes in the US as they occurred, the primary source of information regarding the US is publicly available information, including the US President's Working Group on Digital Asset Markets Report and

---

5 FSB (2023), *FSB Global Regulatory Framework for Crypto-asset Activities*, July.

6 For a comprehensive overview of these risks and policies to address them, see IMF-FSB (2023), *IMF-FSB Synthesis Paper: Policies for Crypto-assets*, September.

7 President's Working Group on Digital Asset Markets (2025), *Strengthening American Leadership in Digital Financial Technology*, July

for payment stablecoins, the GENIUS Act.[8] Several non-FSB jurisdictions also responded to the questionnaire[9] or updated their responses to the high-level survey that was conducted as part of the 2024 G20 status report on the Crypto-asset Policy Implementation Roadmap.[10] Some jurisdictions with material crypto-asset activities did not participate in this peer review. In addition, the FSB issued a call for public feedback in February 2025.[11] The team held a virtual roundtable with FSB Regional Consultative Group members in June 2025 and a roundtable with stakeholders in London in July 2025 to discuss topics covered by the review.

The International Organization of Securities Commissions (IOSCO) has also undertaken a thematic peer review to examine a subset of the Crypto and Digital Asset Recommendations (CDA Recommendations) that are most directly relevant to IOSCO's investor protection and market integrity objectives within a group of its member jurisdictions with significant crypto-asset activities or with licensed crypto-asset activities (IOSCO Report). Together, this Peer Review and the IOSCO Report covers progress to implement crypto-asset and stablecoin recommendations covering financial stability risks, investor protection, and market integrity. The conclusions of the two reports are summarised in an information note.[12]

This report is structured as follows:

- Sections 2 and 3 describe the progress in implementing regulatory frameworks for crypto-asset activities and service providers, and stablecoins, respectively;
- Section 4 focuses on data reporting and disclosures frameworks in place, as well as financial stability risk monitoring approaches across jurisdictions;
- Section 5 describes the tools, progress, and challenges in cross-border cooperation and coordination.

Annex 1 describes the definitions used to measure implementation progress. Annex 2 summarises the coverage of CASP activities by jurisdictional regulatory frameworks. Annex 3 summarises the authorities responsible for licensing and overseeing CASPs and stablecoin issuers. Annex 4 summarises cross-border cooperation tools used by jurisdictions. Annex 5 provides a summary of the FSB high-level survey on implementation of the FSB crypto framework. Annex 6 provides a summary of the public feedback received.

2. Implementation of the CA recommendations

Many jurisdictions have implemented or are in the process of developing regulatory frameworks for crypto-asset activities that address financial stability risks, reflecting significant progress in this area. Most jurisdictions participating in this review have taken steps to regulate crypto-asset

---

8 12 USC 5901 (2025), Guiding and Establishing National Innovation for US Stablecoins Act, July.

9 Authorities in the following non-FSB member jurisdictions completed the questionnaire: Armenia, The Bahamas, Bermuda, Chile, Hungary, Ireland, Kazakhstan, Lebanon, Nigeria, Philippines, Poland, Thailand, Uruguay.

10 FSB and IMF (2024), *G20 Crypto-asset Policy Implementation Roadmap: Status report*, October.

11 FSB (2025), *Thematic Peer Review on FSB Global Regulatory Framework for Crypto-asset Activities*, February.

12 FSB and IOSCO (2025), *Progress towards implementing comprehensive regulatory frameworks for crypto-asset activities: Information note to accompany FSB and IOSCO reports*, October.

activities, with an increasing number prioritising financial stability alongside other risks such as financial integrity, consumer protection, and market integrity. To date, 11 jurisdictions (39%)[13] in the review have finalised a regulatory framework for crypto-assets that addresses financial stability, while eight jurisdictions (29%) are in process of consulting on or finalising frameworks. Three jurisdictions (11%) have a framework that partially addresses financial stability risks, while six jurisdictions (21%) remain at an early stage, with no comprehensive frameworks in place or publicly announced plans. Table 2 provides a summary of implementation status of the CA recommendations for each jurisdiction included in this peer review.

The approach and progress to implementing regulatory frameworks for crypto-asset markets and activities varies across jurisdictions, reflecting differing priorities, legal systems, and institutional capacities. Reflecting these differences, a sequential pattern can be observed across most jurisdictions' approach to implementation in terms of the breadth of frameworks: first, AML/CFT regulation is applied to crypto-asset activities; then consumer protection and market integrity; and risks to financial stability are addressed more thoroughly afterwards.

Table 2: Summary of CA implementation status by jurisdiction

Jurisdiction	Stage of progress[14]	Implementation summary
Argentina	2	Comisión Nacional de Valores (CNV) General Resolution No. 1058 (2025) establishes the regulatory framework for VASPs. The CNV regulatory framework primarily focuses on AML/CFT and market integrity requirements, with limited requirements related to financial stability.
Armenia	4	Central Bank of Armenia (CBA) has been empowered to regulate and oversee crypto-asset markets, including issuers and service providers. Detailed regulations remain under development.
Australia	4	Existing financial services laws apply to crypto-assets if they meet one of the definitions for 'financial product.' The Australian Government has proposed a regulatory framework that does not depend on the 'financial product' status of any particular digital asset.
The Bahamas	5	The Digital Assets and Registered Exchanges Act (2024) and related Guidelines on Digital Assets establishes a regulatory framework for crypto and other digital assets, including requirements for CASPs.
Bermuda	5	The Digital Business Act (2018) establishes a regulatory framework for digital asset businesses and related activities, while the Digital Asset Issuance Act (2020) established a bespoke framework for digital asset issuance, with the BMA empowered as supervisor for all digital asset business activities.

[13] The EU and its member countries are counted as one jurisdiction in these totals.

[14] Stages of progress include: 1: No framework in place; 2: Partial regulations in place; 3: Plans for framework under public discussion 4: Framework proposed but not finalised; 5: Regulatory framework finalised. See Annex 1 for more detail.

Jurisdiction	Stage of progress[14]	Implementation summary
Brazil	3	Under Decree 11.563 (2023) provides BCB with the powers to regulate the provision of virtual asset services; and regulate, authorise, and supervise VASPs. In order to operationalise Decree 11.563, BCB in currently undergoing public consultation on more detailed rules.
Canada	2	Existing provincial securities regulation may apply where crypto-asset activities meet the definition of a security. Provincial securities regulators have published guidance to help entities understand how existing provincial securities laws may apply.
Chile	5	Law No. 21521 (Fintech Law) provides the legal framework for financial services providers (FSPs), and grants CMF the regulatory, supervision, and enforcement powers over FSPs that may operate with crypto-assets.
China	1	All crypto-asset activities are prohibited in China.
EU	5	MiCAR establishes EU-wide regulation and oversight requirements of crypto-asset activities. Supervision of CASPs is delegated to NCAs with ESMA providing EU-wide coordination.
Hong Kong	5	The Securities and Futures Commission (SFC) regulates, and oversees virtual asset trading platforms (VATPs) and virtual asset services provided by other intermediaries licensed by or registered with the SFC.
India	1	The government of India is examining policy approaches to implement the CA recommendations.
Indonesia	5	The Financial Services Commission (OJK) has the mandate to oversee crypto-asset regulation and supervision. Regulation on Digital Financial Asset Trading establishes oversight requirements for CASPs.
Japan	5	The Payment Services Act was amended in 2016 (effective 2017) to include requirements for crypto-asset exchange services and oversight provided by the Financial Services Agency (FSA).
Kazakhstan	1	The issuance, use, and operation of exchanges dealing with crypto-assets are prohibited in the Republic of Kazakhstan, except for activities within the territory of the Astana International Financial Centre.[15]
Korea	3	The Act on Reporting and Using Specified Financial Transaction Information (2021) and the Act on the Protection of Virtual Asset Users (2024) together establish a basic framework, while the FSS is empowered to supervise such activities. The Korean government plans to

[15] The regulatory framework of the Astana International Financial Centre was not in scope for this review.

Jurisdiction	Stage of progress[14]	Implementation summary
		propose a comprehensive regime covering issuers, service providers, and markets in the fourth quarter of 2025.
Lebanon	1	The Banque de Liban has issued public announcements warning against using crypto-assets while the regulatory framework for crypto-assets remains under development and therefore no CASPs have been licensed.
Mexico	1	The Fintech Law (2018) regulations the operations of crypto-asset activities and empowers the central bank to authorise financial technology institutions and credit institutions to operate with crypto-assets. Currently, Banco de Mexico has not designated any crypto-assets as legal assets and restricts the use of crypto-assets to internal transactions not involving the public.
Nigeria	5	The Investment Securities Act (2025) establishes a regulatory framework for crypto and other digital assets, providing the Nigeria SEC with a mandate to oversee these markets.
Philippines	4	The Philippines SEC has issued rules for CASPs. Meanwhile, the exchange and transfer of all virtual assets is regulated by the BSP. BSP Circular 1108 establishes oversight and prudential guidelines for VASPs.
Saudi Arabia	1	Crypto-asset activities are prohibited and no CASPs have been licensed while the regulatory framework for crypto-assets remains under development.
Singapore	5	Crypto-assets that are a digital representation of value and intended to be a medium of exchange are considered Digital Payment Tokens (“DPTs”). MAS currently regulates entities that provide regulated services in crypto-assets (including stablecoins) under the Payment Services Act (“PS Act”) as DPT service providers.
South Africa	2	The Financial Sector Conduct Authority (FSCA) declared crypto assets as financial products under the Financial Advisory and Intermediary Services Act (FAIS). This classification subjects CASPs to the same regulatory standards as traditional financial service providers in respect of providing financial services.
Switzerland	3	Existing financial regulations apply to crypto-asset activities. Activities with crypto-assets qualifying as securities are subject to the same rules as activities with traditional securities, including prudential supervision or market abuse regulations. Similarly, a crypto-asset activity may qualify as a banking or payment system activity under existing regulations and be subject to the related obligations. The Swiss authorities are currently drafting a bill to amend financial market legislation.

Jurisdiction	Stage of progress[14]	Implementation summary
Thailand	5	The Digital Asset Law (2018) establishes a regulatory framework for crypto and other digital assets, including requirements for CASPs.
Türkiye	5	Law No. 7518 (2024) places CASPs under the regulatory and supervisory authority of the Capital Markets Board. CASPs are subject to the requirements of Law no 6362 on Capital Markets.
UK	4	The FCA published a Crypto Roadmap in 2024 toward full oversight of CASPs, including a discussion paper on admission and disclosures, and in 2025 a discussion paper on regulating crypto-asset activities (with draft rules being consulted on custody and prudential requirements for CASPs). The UK has in place a crypto-asset regulatory regime for financial promotions and aspects of consumer protection.
Uruguay	3	The Virtual Asset Act (2024) clarifies the legal classification and licensing requirements of crypto-asset activities. The Banco Central Del Uruguay is developing more detailed regulations to implement the Virtual Asset Act.

2.1. Regulatory frameworks for crypto-asset activities

The FSB's CA recommendations seek to promote the comprehensiveness and greater international consistency of regulatory and supervisory approaches to crypto-asset activities and markets, including crypto-asset issuers and service providers (CASPs).[16]

Jurisdictions have broadly adopted two approaches to regulate financial stability risks of crypto-asset activities, reflecting the different legal frameworks, regulatory powers, and policy priorities. The first approach extends existing financial regulations to encompass crypto-assets (Argentina, Australia, Canada, Hong Kong, Japan, Nigeria, Singapore, South Africa, Switzerland, and Türkiye), aligning oversight of new entities (e.g., CASPs) and activities (e.g., crypto-assets) with traditional financial regulatory frameworks. On the other hand, the second approach introduces bespoke regulatory frameworks tailored to the unique characteristics of crypto-assets, addressing areas such as prudential safeguards, governance, and risk-based supervision (Armenia, Bermuda, The Bahamas, Chile, the EU, Indonesia, the Philippines, and Thailand,). Other jurisdictions are still developing their approaches or only partially regulate crypto-asset activities (Brazil, Korea, the UK, and Uruguay). Over time, jurisdictions may begin with one approach and transition to the other, or use a combination of approaches (such as Hong Kong), as the crypto-asset market develops. Finally, China, and Saudi Arabia have imposed a prohibition on crypto-asset activities. Temporary or targeted prohibitions on crypto-asset

[16] The terms referring to crypto-asset service providers may differ in various jurisdictional or international frameworks, including CASP, DASP, or VASP, etc.

activities may mitigate financial stability risks if they are effectively implemented and enforced, which can be particularly challenging given how crypto-assets are traded and held.[17]

Among those jurisdictions that extended existing financial regulations to encompass crypto-assets, some did so by expanding the definition of different types of financial instruments. For example, Singapore applies payment-based regulations to crypto-asset activities, ensuring that these activities are subject to the same rules as traditional payment service providers. Japan has established a dedicated framework for CASPs by defining crypto-asset activities within the Payment Services Act. On the other hand, Hong Kong, Nigeria, and Thailand apply regulatory standards modelled on securities market intermediaries, aligning the oversight of CASPs with established securities intermediary frameworks. Canada and Switzerland apply existing principles-based requirements to financial intermediaries involved in crypto-assets, tailoring these requirements proportionally to the risks posed by specific activities. Swiss authorities are currently examining whether its legal framework applicable to payment service providers and crypto-asset service providers has to be amended and drafting a bill to amend Swiss financial market legislation.

Among jurisdictions that have opted for bespoke regulatory frameworks tailored to the unique characteristics of crypto-assets, the EU's Markets in Crypto-Assets Regulation (MiCAR) is a notable example, providing a tailored regulatory framework that includes prudential requirements, governance standards, and conflicts of interest rules. MiCAR has been implemented directly in EU member states, however, some EU member states are still developing their domestic legislation to designate National Competent Authorities and establish supervisory frameworks, enforcement powers, and regulatory reporting requirements for CASPs,[18] and some areas, such as crypto-asset lending and borrowing, remain deliberately outside MiCAR's scope and are left to national authorities to address.[19] Bermuda has had a tailored framework in place since 2018, covering a wide range of activities, including digital asset exchanges, custodial wallet services, lending, and since 2020 the issuance of crypto-assets. The framework includes risk-based supervision, with higher-intensity oversight applied to entities deemed systemically important or interconnected with the broader financial system. Similarly, The Bahamas introduced legislation in 2024 that established a tailored regulatory framework for crypto-assets, including registration, capital, and disclosure requirements for CASPs and issuers. The Bahamas also established a Financial Stability Council to facilitate coordination among financial regulators and address risks arising from digital asset activities. Chile adopts a mixed approach with its Fintech Law, which is complemented by a General Rule, to regulate financial services and instruments, covering CASP among the financial service providers. The Fintech Law establishes different requirements for them, including collateral, capital, governance, risk management, supervision, and enforcement; however it does not cover crypto-asset issuance.

Most jurisdictions with developed regulatory frameworks for crypto-asset activities have focused their efforts on CASPs, addressing activities such as custody, trading, asset management and advisory services. In contrast, there has been less emphasis on regulating the issuance of crypto-assets other than stablecoins, with Armenia and the EU being the only jurisdictions with

---

17 See section 3.3.4 of IMF-FSB (2023), *IMF-FSB Synthesis Paper: Policies for Crypto-assets*, September.

18 For example, Poland is still developing its domestic legislation to formally designate its NCA(s).

19 While a report from the EU supervisory authorities analysed the risks of crypto-asset borrowing, lending and staking services and determined there is a limited engagement of EU consumers and financial institutions with such activities, they still remain outside the scope of regulation and are not consistent with CA recommendation 2 and 5 (see section 2.2 of this report).

direct regulation on such activity. In some other jurisdictions, such as Canada, the issuance of crypto-assets may be regulated where the crypto-asset meets the jurisdictions' definition of securities or derivatives.

Box 1: Recent policy developments in the US

To meet the current US administration's new approach towards the digital asset industry, which aims to reverse the prior US administration's regulatory approach, US authorities have recently sought to modernise and improve their digital asset regulatory framework and adopt a 'pro-innovation' mindset towards digital assets and blockchain technologies. [20] This Box summarises the US Presidents Working Group on Digital Asset Markets Report. The US President Working Group on Digital Asset Markets Report includes over 100 recommended regulatory and legislative actions on a broad range of issues, including: modernising banking and market structure regulation for digital assets; countering illicit finance; and ensuring fairness and predictability in crypto taxation.

The US President's Working Group on Digital Asset Markets Report observes that digital asset market participants need clearer guidance on registration requirements and on which authorities are responsible for regulating each type of digital asset. It recommends that the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) use their existing authorities to enable the trading of digital assets at the federal level by providing clarity to market participants on issues such as registration, custody, trading, and recordkeeping. The US President's Working Group on Digital Asset Markets Report further recommends legislation to clarify how the SEC would oversee digital asset securities, while providing the CFTC with new regulatory authority over certain activities involving non-security digital assets defined as "digital commodities." The Report also recommends that the US engage internationally on setting legal, regulatory, and technical standards—and advancing regulatory frameworks—for digital assets, including through international forums such as the FSB and the Basel Committee on Banking Supervision.

Licensing/Authorisation

Under existing US regulations, any platform that operates as an "exchange" for digital assets that are securities must register as a national securities exchange or operate pursuant to an exemption in conjunction with the SEC's relevant exemptive authority. Any intermediaries acting as a "broker" or "dealer" in interstate commerce in digital assets that are securities must register with the SEC and are subject to SEC oversight. Tokenised securities fall within the definition of "security" under the federal securities laws, and all offers and sales of such assets are subject to registration requirements (absent an exemption). Likewise, the US President's Working Group on Digital Asset Markets Report states that when a digital asset meets the statutory definition of a commodity, derivatives referencing the asset fall within the CFTC's regulatory licensing regime.

The US President's Working Group on Digital Asset Markets Report recommends that the SEC consider using its rulemaking, interpretive, and exemptive authorities to provide additional clarity and create fit-for-purpose exemptions from registration for certain digital asset-related activity. Similarly, it recommends that the CFTC provide clarity on the applicability of its various registration requirements to DeFi activities, smart contract protocols, or decentralised autonomous organisations, consistent with technology-neutral principles.

Permitted Activities

The US President's Working Group on Digital Asset Markets Report outlines a list of permitted activities that crypto-asset service providers may undertake, provided they are registered with the appropriate regulator. These activities include operating trading platforms, acting as brokers or dealers, providing custody and clearing services, facilitating settlement, and issuing or managing stablecoins. The US

[20] President's Working Group on Digital Asset Markets (2025.

President's Working Group on Digital Asset Markets Report notes that SEC and CFTC registrants should be permitted to engage in multiple business lines under the most efficient licensing structure possible, ensuring a clear and simple regulatory framework for digital asset market activities.

Reporting and Disclosure Requirements

The US President's Working Group on Digital Asset Markets Report also makes recommendations relating to disclosures and safeguarding of customer assets. Specifically, it recommends that the SEC and CFTC should adopt rules ensuring customer asset segregation for digital assets. Further, issuers of digital asset securities, and of securities involving digital assets, should be subject to disclosure requirements that are appropriately tailored to address the novel characteristics of digital assets and blockchain technology. Any ongoing disclosures should be fit-for-purpose and guided by publicly available information, such as open-source code, whenever possible. Digital asset trading platforms, brokers, dealers, and other CFTC-registered intermediaries that make available non-security digital assets should be required to disclose any such information that the CFTC determines to be appropriate for such assets. Under current US law, many crypto-asset service providers are registered on the state level as money services business and may hold additional registrations with the SEC and/or CFTC as applicable.

Facilitating Innovation

The US President's Working Group on Digital Asset Markets Report observes that existing US regulation – if strictly enforced – could restrict business model innovations and new activities enabled by digital asset technologies. To address this, it recommends that the SEC and the CFTC consider adopting certain safe harbours to enable innovative financial products.

Recent Accomplishments

US regulators have also recently taken steps to clarify and improve the US framework for regulating digital assets by rescinding past statements, publishing new statements, engaging with stakeholders, launching initiatives inviting public comment on the advancement of the recommendations contained in the US President's Working Group on Digital Asset Markets Report through the use of existing laws, and announcing efforts to draft new rules relating to digital assets.

The CFTC launched a "Crypto Sprint" to start implementation of the US President's Working Group on Digital Asset Markets Report's recommendations. The SEC has launched a dedicated Crypto Task Force, which aims to draw clear regulatory lines, craft tailored disclosure frameworks, provide realistic paths to registration for both crypto assets and market intermediaries, and make sure that enforcement resources are deployed judiciously.[21] In August 2025, the SEC announced the launch of Project Crypto, a Commission-wide initiative that will develop proposals to implement the Report's recommendations.[22]

Pending Legislation

Following passage of the GENIUS Act (see section 3), the US Congress is considering draft legislation on crypto-assets more broadly.[23] In July 2025, the House of Representatives passed the Digital Asset Market Clarity Act ("CLARITY"), which proposes a division of digital asset market jurisdiction between the SEC and the CFTC. CLARITY also calls for a study by the OCC on the extent to which DeFi has integrated with the traditional financial markets and any potential risks or improvements to the stability of the markets. The US Senate is also considering alternative market structure legislation.

---

21 SEC (2025), *SEC Crypto 2.0: Acting Chairman Uyeda Announces Formation of New Crypto Task Force*, January.

22 Atkins, Paul S. (2025), *American Leadership in the Digital Finance Revolution*, July.

23 The details and status of pending legislation remains subject to change.

2.2. Authorisation and licensing

As set out in CA Recommendation 1, authorities should have the powers and capabilities to enforce applicable regulatory, supervisory and oversight requirements, including authorisation and licensing requirements. Authorisation and licensing requirements are a critical tool to ensure CASPs meet all applicable regulatory, supervisory and oversight requirements before commencing any operations in that jurisdiction.

In line with the principle of "same activity, same risk, same regulation," most jurisdictions are adopting rigorous authorisation and licensing frameworks to ensure CASPs are subject to the same regulatory and supervisory oversight as traditional financial services firms providing similar services. Many jurisdictions have established comprehensive authorisation and licensing frameworks that go beyond registration or disclosure frameworks to include governance standards, financial and operational resilience measures, prudential requirements, and client asset protection rules.[24] These rigorous authorisation and licensing frameworks are a critical element of the CA recommendations.

However, the scope and maturity of licensing and authorisation frameworks for crypto-asset markets and activities vary widely across jurisdictions, reflecting both progress and challenges in regulating the sector (see box 2). While many jurisdictions[25] have implemented CASP licensing and regulatory frameworks that go beyond registration frameworks (e.g., AML/CFT compliance) to address financial stability risks, others[26] remain focused primarily on AML/CFT registration or are still developing their regulatory structures. Meanwhile, China, Saudi Arabia, and Mexico (partially)[27] maintain outright prohibitions on crypto-asset activities, although Saudi Arabia has indicated plans to develop a framework.

Box 2: Challenges in the authorisation and licensing process

A range of challenges has been identified by authorities in the authorisation and licensing of CASPs, reflecting the complexity and evolving nature of the sector. One prominent issue is the frequent lack of familiarity or experience with regulatory frameworks among applicants. Many entities, particularly start-ups and technology companies, are unfamiliar with financial regulations and fail to meet the required standards to obtain a license or authorisation. This often results in incomplete or poor-quality applications, with missing documentation, unclear descriptions of services, or inconsistencies in submissions. Authorities have noted the need for extensive pre-application consultations and enhanced guidance to address these deficiencies.

The global and borderless nature of crypto-asset businesses poses additional challenges. Domiciliation uncertainty complicates the determination of where certain activities require licensing. Furthermore, the borderless structure of crypto-assets creates difficulties in monitoring related developments and activities, especially in the absence of robust mechanisms to track transactions or identify unlicensed

24 These are Armenia, The Bahamas, Bermuda, Chile, the EU, Hong Kong, Indonesia, Japan, Nigeria, Philippines, Singapore, Thailand and Türkiye.

25 These are Argentina, Armenia, The Bahamas, Bermuda, Canada, Chile, the EU, Hong Kong, Indonesia, Japan, Nigeria, Philippines, Singapore, Thailand and Türkiye.

26 These are India, Korea and South Africa.

27 Financial and Credit Institutions are the only ones allowed to operate with virtual assets and may only carry out operations that correspond to internal operations, subject to authorisation granted by Banco de México. Thus, CASPs, do not fall within the regulatory framework.

or unauthorised players. This issue is compounded by the lack of resources and advanced technology to support effective oversight, particularly in jurisdictions with limited capacity.

Cybersecurity and adequacy of IT infrastructure are recurring concerns in the licensing process. Jurisdictions report that many applicants lack adequate cybersecurity measures, such as external audits or secure management of cryptographic keys. Weak IT systems and reliance on third-party providers further exacerbate such risks, particularly in business models involving un-hosted wallets or omnibus custodial accounts. Authorities have emphasised the importance of detailed risk assessments and the implementation of strong internal controls to address these vulnerabilities.

2.2.1. Role of competent authorities and coordination

The allocation of CASP licensing responsibilities varies significantly across jurisdictions. Market or securities supervisors most commonly play this role. For example, in the EU, NCAs and ESMA share intervention powers on matters of market integrity and financial stability. Most EU jurisdictions have appointed its market supervisor as NCA, such as Spain's CNMV and France's AMF to supervise CASPs, while others, such as the Netherlands, the AFM and DNB coordinate CASP supervision. In seven jurisdictions,[28] central banks act as the primary licensing authority, overseeing CASPs as part of their broader financial system responsibilities. For example, in Brazil, the Banco Central do Brasil will have oversight and supervisory responsibilities for CASPs once its regulatory framework is in place.

In some jurisdictions, licensing responsibilities are distributed across multiple authorities. For instance, in Australia, responsibilities are similarly divided between market and prudential supervisors. In other jurisdictions, ministries or executive branches play a direct role in licensing. For example, Thailand's Ministry of Finance oversee CASP licensing, while the Thailand SEC is responsible for oversight and supervision. Although shared supervisory responsibilities among various authorities in the same jurisdiction is not necessarily ineffective, it requires coordination effort and may impact the efficiency and even efficacy of supervision if it is not working well. See Annex 3 for a summary of the relevant authorities in licensing and/or authorisation of CASPs.

2.2.2. Scope of CASP activities within the regulatory framework

Consistent with CA Recommendation 2, authorities should apply comprehensive and effective regulation, supervision and oversight to CASPs on a functional basis and proportionate to the financial stability risks they pose (including their degree of financial intermediation). Furthermore, CA Recommendation 5 provides that authorities should require CASPs to effectively identify and manage potential risks arising from leverage, credit, liquidity, operational, and maturity transformation. Previous FSB work[29] has identified CASP activities that can give rise to financial stability implications including through the creation of leverage, liquidity mismatch and operational risks. Specific CASP activities that may give rise to these risks include custody, derivatives and margin trading, staking-as-a-service, yield and earn programs, borrowing and

---

28 These are Armenia, Brazil, Hungary, Ireland, Philippines, Singapore, and Uruguay. In Philippines, the BSP is responsible for the regulation and supervision of VASPs and the SEC is responsible for CASPs.

29 FSB (2022), *Assessment of Risks to Financial Stability from Crypto-assets*, February; and FSB (2023), *The Financial Stability Implications of Multifunction Crypto-asset Intermediaries*, November.

lending provision, and proprietary trading. In many cases, these activities and services are combined within a single CASP or group of affiliates entities.

The regulatory treatment of CASPs activities varies significantly across jurisdictions, with some activities being consistently addressed by most jurisdictions, other activities being regulated by only a smaller subset of jurisdictions, and certain activities largely omitted from regulatory frameworks. Notably, activities that could give rise to financial stability risks, such as crypto-asset borrowing and lending, are not addressed in many jurisdictions. Annex 2 provides more detail on the range of CASP activities covered by regulatory frameworks across jurisdictions.

Activities generating leverage risks

Leverage risks can arise when CASPs provide services that allow users to borrow against their exposures, potentially leading to margin calls and cascading failures during market stress. Borrowing and lending services, for example, involve CASPs facilitating loans of crypto-assets or fiat currencies, often collateralised by users' crypto-asset portfolios. CASPs can also increase their own leverage risk when they borrow funds from customers and other counterparties. Despite these risks, few jurisdictions have regulatory frameworks that address these activities.

Only two jurisdictions, Bermuda and The Bahamas, comprehensively regulate CASP borrowing and lending, requiring CASPs to manage counterparty risks and maintain capital and liquidity buffers. Other jurisdictions, such as Australia, Canada, and Switzerland, regulate CASP borrowing and lending in cases where the services meet the definition of existing financial products but otherwise the activities remain unregulated. Japan regulates CASP borrowing, with limits on excessive borrowings, but does not directly regulate CASP lending activities.[30] In contrast, Hong Kong, Korea, Türkiye and Thailand explicitly prohibit borrowing and lending by CASPs altogether, citing financial stability concerns.[31] Singapore, reflecting a cautious stance, prohibits these activities for retail customers but services for institutional clients are not considered a regulated activity. The Philippines SEC prohibits CASPs from providing margin to clients but otherwise CASP borrowing and lending is not covered by their regulatory framework. Most other jurisdictions, including Argentina, Armenia, Chile,[32] the EU, Korea, Indonesia, South Africa, do not explicitly address crypto-asset borrowing and lending in their regulatory frameworks. In many cases, borrowing and lending activities where the transaction does not involve a security or fiat currency (e.g., the CASP lends crypto-assets secured by a user's crypto-assets) is not covered by existing regulations. Frameworks not addressing CASP borrowing and lending activities leave a significant gap in oversight which is not aligned with CA recommendations 2 and 5.

Derivatives trading similarly enable users to take leveraged positions, further amplifying market risks. Poorly managed leverage can lead to rapid market contagion during stress events. Derivatives trading where the underlying reference asset is a crypto-asset is more commonly

---

30 In Japan, regulations under the Money Lending Business Act may apply for CASP lending activities.

31 While Hong Kong currently prohibits CASPs from providing crypto-asset borrowing and lending services, Hong Kong is considering allowing the provision of crypto-asset borrowing and lending services by imposing robust risk management measures.

32 In Chile, although borrowing and lending is not explicitly regulated, Alternative Trading Systems should have an internal regulation regarding trading and other aspects, and these entities, as well as intermediaries and custodians, should comply with prudential and conduct requirements which include custody safeguards when applicable.

addressed in jurisdictional regulatory frameworks, largely due to the broader definition of derivatives in existing frameworks that does not depend on specific underlying assets. Bermuda, The Bahamas, and Australia permit derivatives trading, subject to licensing requirements, leverage limits, and collateral rules. For instance, Bermuda and The Bahamas explicitly allow digital asset derivatives services under their regulatory frameworks. The EU regulates crypto-asset derivatives by requiring CASPs offering these services to obtain a license under applicable frameworks, such as MIFID II. Similarly, in Armenia, Japan, Singapore and South Africa, these activities are generally regulated under existing derivatives regulations. On the other hand, Hong Kong and Türkiye explicitly prohibit leveraged trading and derivatives transactions involving crypto-assets, reflecting a conservative regulatory stance.[33] Other jurisdictions, such as Argentina, Indonesia, and Thailand do not explicitly address these activities, leaving their regulatory treatment ambiguous pending further legislative or regulatory clarifications.[34]

Proprietary trading by CASPs, which involves trading on their own account, also introduces significant leverage risks when the trading positions are funded by borrowings or use derivatives. Such activities can also exacerbate conflicts of interest, increase market manipulation risks, and amplify systemic vulnerabilities, particularly when proprietary trading is conducted alongside other high-risk activities like margin trading. Regulatory approaches to proprietary trading also vary significantly. Canada, Hong Kong and the EU prohibit proprietary trading by CASPs operating trading venues to prevent conflicts of interest, while Armenia, The Bahamas, Bermuda, Chile, Indonesia, Philippines, Thailand, and Türkiye allow proprietary trading for CASPs but subject them to specific requirements to address conflicts of interest. In other jurisdictions, including Argentina, Japan, Singapore, and South Africa, proprietary trading is not explicitly addressed, leaving its regulatory status unclear and the associated risks unmitigated.

Activities generating liquidity risks

CASPs generate liquidity risk when they engage in activities that give rise to asset and maturity transformation. Yield or earn programs, and in certain cases, staking,[35] are prominent examples of such activities. These programs involve users locking their crypto-assets with CASPs in exchange for rewards. Participation in many yield and rewards programs often grants the CASP the right to use the client assets to fund the CASP's proprietary activities, such as margin trading or other lending activities. Liquidity risks emerge when CASPs use client assets, which may be subject to clients' right of redemption or withdrawal within a short notice period, to fund its own proprietary activities, such as lending and proprietary trading, which may in turn be less liquid and have a maturity period longer than the redemption timeframe for clients to withdraw their funds.

Regulatory approaches to these activities also vary significantly. The Bahamas, Bermuda, and Hong Kong cover these activities in their CASP regulatory frameworks, imposing additional risk management and prudential requirements to manage such liquidity risks. Canada and Hong

---

33 While Hong Kong currently prohibits CASPs from providing crypto-asset derivatives trading, Hong Kong is considering allowing the provision of crypto-asset derivatives by imposing robust risk management measures.

34 In Indonesia and Thailand, authorities are in the process of updating regulations to ensure crypto-asset derivatives are subject to comprehensive oversight.

35 For example, liquidity risk may arise in CASPs if they provide "liquid staking" whereby the CASP provides staking-as-a-service to its clients and while the user's assets are locked in staking, the CASP issues a liquid staking token to the user, representing a claim on the users' staked position and rewards. These liquid staking tokens can be used by the user in crypto-asset markets for further borrowing, lending or other trading activities. This practice can lead to liquidity mismatches.

Kong do not allow CASPs to provide yield or earn programs where client assets are rehypothecated, pledged, or otherwise used by the CASP, but those programs that do not use client assets are allowed (Hong Kong) or may be allowed subject to compliance with securities laws (Canada). Other jurisdictions only partially address the risks of yield or earn programs, such as Australia which covers them if the activity meets existing financial product definitions. Most other jurisdictions, including Argentina, Armenia, the EU, Japan, Singapore, and South Africa, do not explicitly address yield, earn, or liquid-staking programs in their regulatory frameworks.

The issuance of crypto-assets by CASPs, particularly their own tokens, introduces additional liquidity risks. These risks arise when CASPs issue tokens that represents a claim towards or liability of the CASP and engage in maturity or liquidity transformation with the proceeds of issuing such tokens. Poorly designed or inadequately disclosed token issuance processes can also lead to investor losses or market instability. Regulatory approaches to token issuance vary widely. Bermuda and The Bahamas permit CASPs to issue their own tokens, provided they adhere to licensing and disclosure requirements. Bermuda regulates token issuance under its Digital Asset Business Act,[36] while The Bahamas requires CASPs to prepare offering memoranda for initial token offerings to ensure transparency and investor protection. In Armenia and the EU, CASPs wanting to issue tokens need to fulfil the requirements for issuers depending on the nature of the token. Conversely, Canada and Türkiye explicitly prohibit CASPs from issuing their own crypto-assets, reflecting a restrictive stance on primary market activities. In other jurisdictions, such as Singapore, the regulatory treatment of token issuance remains unclear, with frameworks either silent on the issue or addressing it only indirectly. This lack of clarity increases the risk of liquidity mismatches and of market disruptions going unaddressed.

Activities generating operational and technology risks

Operational and technology risks arise when CASPs engage in activities that expose them or their clients to the risk of loss, such as asset mismanagement, technological failures, or cybersecurity breaches. These risks can undermine trust in crypto-asset markets and have significant implications for financial stability if left unaddressed. Custody services are a key activity in this category.

Custody services are critical for safeguarding client assets and maintaining trust in crypto-asset markets. Operational risks, such as mismanagement, fraud, or inadequate security protocols, can lead to the loss of client assets or disruptions in service. Additionally, the reliance on technological infrastructure introduces risks related to system outages, data integrity, and cybersecurity breaches. Regulatory approaches to custody services are relatively comprehensive compared to other CASP activities. Jurisdictions such as Armenia, Bermuda, Canada, and Türkiye require strict asset segregation and client protection measures to mitigate operational risks. For example, Armenia and Bermuda mandate bankruptcy-remote arrangements to ensure client assets are protected in the event of insolvency, while Türkiye requires that 90% of client assets be stored in cold wallets to reduce exposure to cyber threats. Argentina, Switzerland, and South Africa impose general oversight requirements related custody practices, including measures to address technology-related vulnerabilities.

[36] In Bermuda issuance of crypto-assets are covered under the Digital Asset Businesses Act, unless the issuance is for capital raising purposes, in which case this activity would fall under the Digital Asset Issuance Act (2020).

Implications of inconsistent treatment of CASP activities

The CA recommendations are intentionally high-level to allow jurisdictions flexibility in regulating CASP activities that pose financial stability risks. While the recommendations do not provide a specific list of activities to be regulated, the FSB's analytical work has identified key CASP activities – such as borrowing, lending, margin trading, and proprietary trading – that could generate significant financial stability risks, including through leverage and liquidity mismatches. Jurisdictions that have been more successful in comprehensively regulating CASP activities often apply rules similar to those for securities intermediaries, such as brokers and dealers. In contrast, jurisdictions that primarily rely on payment regulations or layer additional requirements beyond AML/CFT obligations onto digital asset businesses have generally thus far failed to address activities with higher financial stability risks. Jurisdictions that fail to comprehensively address these activities in their regulatory frameworks are not consistent with CA Recommendation 2, as they leave these risks unaddressed. This inconsistency creates challenges such as regulatory arbitrage, data gaps, and market fragmentation. CASPs may migrate to jurisdictions with weaker or less comprehensive frameworks, concentrating high-risk activities and increasing cross-border vulnerabilities.

Box 3: Comprehensive approaches to CASP activities

Thailand and Bermuda illustrate two distinct approaches to comprehensively regulating CASP activities: Thailand focuses on targeted restrictions and activity-specific oversight, while Bermuda employs a broader framework to encompass a wide range of activities.

Thailand's framework under the Digital Asset Law categorises CASPs into six license types: exchanges, brokers, dealers, fund managers, investment advisors, and custodial wallet providers. Each license type is tailored to specific activities, such as trading, brokerage, fund management, or custody services. High-risk activities, including borrowing, lending, margin trading, and derivatives, are explicitly prohibited to reduce credit risk. CASPs are also prohibited from facilitating the use of crypto-assets as a means of payment. To avoid conflicts of interest, the framework imposes segregation of certain activities, such as prohibiting exchanges from also acting as dealers and custodial wallet providers from engaging in other licensed activities. These measures aim to ensure that CASPs operate within clearly defined boundaries while maintaining strong governance and oversight. Thailand's approach reflects a cautious but comprehensive stance, emphasising risk mitigation while allowing for regulated innovation.

Bermuda's Digital Asset Business Act (DABA) provides a broad and adaptable framework that captures a wide variety of activities conducted by Digital Asset Businesses (DABs). Regulated activities include the custody of digital assets, with requirements for asset segregation and fiduciary protections, as well as borrowing and lending, where entities must maintain reserves to mitigate counterparty risks. Margin and derivatives trading is also regulated, with requirements such as leverage limits and collateral adequacy. DABA further governs the issuance of digital assets, including token offerings, by mandating proper disclosures and governance measures. Digital asset exchanges are required to implement strong governance, risk management, and operational resilience practices to protect market integrity. Additionally, a "digital asset services vendor" category ensures that emerging or intermediary activities not explicitly defined are still captured under the regulatory perimeter. Through this comprehensive approach, Bermuda aims to address evolving risks while fostering a stable and transparent digital asset ecosystem.

2.2.3. Licensing and authorisation requirements for CASPs

As set out in CA recommendations 4, 5 and 9, authorities should establish comprehensive governance, risk management, and prudential requirements for CASPs. These requirements are

often a prerequisite for CASPs to obtain a license or authorisation before they begin operations. The regulatory requirements for licensed or authorised CASPs implemented thus far in most jurisdictions are broadly aligned with expectations for robust governance, effective risk management, and financial resilience. While the core principles are consistent – focusing on sound organisational structures, safeguarding client assets, and mitigating financial and non-financial risks – implementation details vary to address local priorities and market dynamics. Some jurisdictions, such as the EU, Türkiye, and Hong Kong, have developed comprehensive and detailed frameworks, while others, like Armenia, Argentina and South Africa, focus on foundational requirements. Differences in approaches, such as the use of proportional governance requirements, stress testing, or specific cybersecurity measures, highlight how jurisdictions tailor their regulations to address risks and challenges within the evolving crypto-asset market.

Governance Requirements

Governance requirements across jurisdictions emphasise the importance of organisational structures, fit-and-proper criteria for qualifying shareholders, directors and senior management, and conflicts of interest management, but implementation varies based on local priorities. Argentina requires companies to adopt specific corporate types or register branches in the jurisdiction, while Indonesia enforces governance principles for directors and commissioners, with clear internal controls and risk management functions. Armenia focuses on internal control systems and conflict of interest policies, allowing its Central Bank to impose additional governance standards if needed. Australia, Canada, and South Africa require general governance frameworks proportional to business complexity, with South Africa further emphasising policies for data integrity, continuity, and remuneration.

The EU, Chile, and The Bahamas scale governance requirements based on the size and complexity of the CASP, ensuring proportionality. Switzerland mandates authorisation for governance changes tied to crypto-related activities, requiring forward-looking risk analyses. Thailand requires non-executive directors to ensure checks and balances, while the EU and Singapore mandates local incorporation and residency requirements for directors. Hong Kong and Bermuda emphasise conflict of interest management and require board-approved governance frameworks. Hong Kong also requires the senior management of CASPs to bear primary responsibility for ensuring the maintenance of appropriate standards of conduct and adherence to internal procedures. Japan and Brazil focus on basic governance standards, such as minimum capital and eligibility requirements for management, with Japan mandating the establishment and public disclosure of a conflicts of interest policy and Brazil still developing its framework.

Financial Risk Management Requirements

Jurisdictions that have risk management frameworks universally address financial risks (liquidity, credit, and market risks) and non-financial risks (operational, IT, and cyber risks), but the level of detail and implementation varies.

The EU, Hong Kong, Bermuda, Thailand, and the Philippines have implemented more comprehensive risk management requirements for CASPs, addressing credit, market and liquidity risks through detailed and structured measures. In the EU, MiCAR requires CASPs to

implement internal frameworks to manage liquidity, credit, and market risks. Hong Kong mandates that VASPs maintain sufficient liquid assets equivalent to at least 12 months of operating expenses, implement risk management frameworks to monitor financial risk exposures, and adopt controls to mitigate market volatility. Bermuda requires stress testing to assess resilience under adverse market and liquidity conditions, while Thailand prohibits the provision of credit for crypto-asset investments, enforces liquidity management, and mandates risk management frameworks to address market risks. The Philippines emphasises liquidity management to ensure customer withdrawals and payment obligations are met, requires credit risk assessments for counterparties, and mandates the implementation of market risk frameworks to address price volatility.

Jurisdictions with moderately comprehensive frameworks address some, but not all, of these key risks. In Canada, CASPs are required to maintain sufficient liquidity to meet client obligations and ensure financial stability, with additional protections such as insurance for fiat client funds under the Canadian Investor Protection Fund; however, there is limited focus on credit and market risk management. Indonesia requires CASPs to conduct self-risk assessments covering market and liquidity risks but does not explicitly address credit risks.

Some jurisdictions have less comprehensive financial risk management requirements for CASPs, reflecting earlier stages in the policy development process or higher priorities on other risks such as investor protection and fraud. In Argentina, measures are primarily focused on monitoring market risks through the submission of monthly trading volumes and details of the most traded virtual assets, but there is no explicit framework for liquidity or credit risk management. South Africa emphasises financial soundness for CASPs holding client funds, requiring them to maintain sufficient resources to meet liabilities, but does not address market or credit risks.

Non-financial Risk Management Requirements

Jurisdictions have established requirements for non-financial risk management, including operational, information technology (IT), and cyber risks, through varying levels of comprehensiveness. The EU, Hong Kong, Bermuda, and Thailand have more comprehensive frameworks for managing these risks. In the EU, the Digital Operational Resilience Act requires CASPs to implement information and communication technology risk management frameworks, conduct resilience testing, and report significant incidents. MiCAR further mandates internal controls to address operational risks and segregation of client assets to mitigate custody risks. Hong Kong requires cybersecurity compliance through periodic independent technology audits, mandates internal controls to manage operational risks, and requires compensation arrangements to cover potential losses of client virtual assets. Bermuda emphasises IT and cyber risk mitigation through its Digital Asset Business Operational Cyber Risk Management Code of Practice, requiring independent audits, stress testing, and robust controls for operational resilience. Thailand mandates robust IT security systems, regular penetration testing, and compliance with the Personal Data Protection Act to safeguard client data and mitigate cybersecurity risks. Thailand also requires the segregation of client assets to reduce operational risks.

Jurisdictions with moderately comprehensive frameworks address some, but not all, key non-financial risks. Japan mandates secure custody of client assets through cold wallet storage,

conducts inspections of IT risk management environments, and requires reporting of blockchain-related incidents, such as deficiencies in wallet security. While its framework focuses on specific operational and cyber risks, it does not currently include resilience testing. The Philippines requires compliance with BSP Circular No. 808, which outlines IT risk management standards, including securing IT systems, conducting regular vulnerability assessments, and implementing business continuity and disaster recovery plans. Türkiye mandates that 90% of customer crypto assets be stored in cold wallets to mitigate cyber risks and holds platforms liable for losses caused by IT system outages. Indonesia requires CASPs to implement comprehensive risk management frameworks to address operational, cybersecurity, and reputational risks, with annual evaluations to ensure effectiveness. Chile has similar requirements on non-financial risk management dimensions and also mandates reporting of significant operational incidents within two hours. In addition, it requires custodians to submit annual external audit reports verifying custody balances.

Jurisdictions with less comprehensive frameworks focus on some but not all non-financial risks. Argentina enforces information security requirements and mandates annual system audits for VASPs to mitigate operational and cybersecurity risks. Korea mandates the establishment of information security management systems but does not explicitly address broader operational or IT risks.

Prudential Requirements

Prudential requirements focus on minimum capital, liquidity, and segregation of client assets, with thresholds varying by jurisdiction and activity type. The EU, Argentina and Indonesia impose capital thresholds tied to activity type, such as USD 150,000 for Category 1 entities in Argentina and IDR 1 trillion for centralised bourses in Indonesia. Türkiye introduces additional equity requirements for custodians holding more than TRY 1 billion in assets, while Chile adopts risk-weighted capital requirements based on crypto-asset categories or service type. The Philippines and Singapore require minimum paid-in capital depending on the type of service, with Singapore also requiring monthly safeguarding reports for client funds. Japan focuses on foundational requirements, such as JPY 10 million in minimum capital for CASPs and secure storage of client assets. In Bermuda, digital asset businesses are required to ensure they maintain minimum net asset requirements, which may be based on risk capital models while BMA may impose higher requirements based on the nature, scale, complexity and overall risk profile of the digital asset business.

Bermuda, Hong Kong and Thailand have requirements for CASPs to hold liquidity reserves, with Bermuda requiring minimum liquidity and working capital ratios, Hong Kong requiring sufficiently liquid assets to cover 12 months of operating expenses and Thailand mandating daily liquidity reporting for custodial providers. Australia imposes financial and cash flow modelling requirements but does not yet require stress testing or recovery plans for CASPs. South Africa has financial soundness requirements for CASPs, which aims to ensure their liabilities can be met. Brazil is finalising its prudential frameworks.

2.2.4. Multifunction CASPs

As set out in CA Recommendation 9, authorities should ensure that CASPs and their affiliates that combine multiple functions and activities, where permissible, are subject to appropriate

regulation, supervision and oversight that comprehensively address the risks associated with individual functions and the risks arising from the combination of functions, including but not limited to requirements regarding conflicts of interest and separation of certain functions, activities, or incorporation, as appropriate.

Jurisdictions adopt diverse approaches to regulating CASPs that combine multiple functions, such as trading, custody, and market-making. The EU's MiCAR requires CASPs to establish governance arrangements and policies to manage conflict of interests arising from different businesses. NCAs oversee CASPs, while at the EU level ESMA also has powers to restrict or prohibit services that could threaten market integrity or investor protection, as well as coordinate the supervision conducted at the national level and resolve disputes among national authorities. Similarly, in Hong Kong, the Securities and Futures Commission (SFC) imposes restrictions on activities like proprietary trading and market-making on a proprietary basis to mitigate conflicts of interest, while also requiring asset segregation and trust arrangements for client funds. Argentina prohibits certain financial entities, such as markets and clearinghouses, from operating as VASPs but allows integration with their platforms under specific conditions.

Several jurisdictions adopt a risk-based or proportional approach to regulating multi-functional CASPs. Bermuda and The Bahamas impose enhanced governance requirements, including asset segregation and independent compliance functions, for providers offering multiple services. The Philippines and South Africa take a disaggregated approach, assessing each service individually under sectoral frameworks. In Switzerland, licensing requirements for each activity must be met when combining functions, and additional risks, such as conflicts of interest, must be addressed. Thailand and Singapore restrict crypto-asset activities to licensed entities, including those within financial groups, generally barring direct involvement by parent entities but allowing affiliated entities to conduct such activities on a case-by-case basis. Türkiye also restricts crypto-asset services (including custody) to licensed CASPs.

Some jurisdictions impose specific restrictions or conditions on the combination of functions. Armenia permits the combination of trading and exchange services but prohibits platform operators from trading on their own platforms. Chile requires each service within the scope of its Fintech Law to be authorised by its financial regulator and comply with relevant requirements. Nigeria treats all crypto-asset functions as standalone, requiring individual compliance for each activity.

The approaches vary significantly in detail and regulatory stringency. Jurisdictions like the EU, Hong Kong, and The Bahamas provide comprehensive and prescriptive frameworks to manage risks associated with multi-functional CASPs. Others, such as Argentina, Armenia, and Switzerland, impose targeted measures to address conflicts of interest and ensure compliance with activity-specific rules. Meanwhile, some jurisdictions, including Australia, Canada, and Korea, have yet to develop detailed regulatory approaches for CASPs offering multiple services. This variation underscores differing levels of regulatory maturity and focus across jurisdictions.

2.3. Examinations and inspections

Supervisory approaches to CASPs can be grouped into three categories (see Table 3). Some jurisdictions have advanced comprehensive frameworks that explicitly address financial stability risks. Others have partial frameworks that cover broader operational and governance risks but

do not fully integrate financial stability considerations. A third group focuses primarily on AML/CFT compliance with relatively limited oversight of other risks. The limited focus on financial stability risks highlights that implementation remains at an early stage, even in jurisdictions with comprehensive regulatory frameworks.

Comprehensive supervision and oversight will be critical to safeguarding financial stability as the sector continues to evolve. Exams specially tailored to CASPs remain limited even in the jurisdictions most focused on financial stability risk, primarily due to the recent adoption of regulatory frameworks or the fact that implementation is still underway.

However, this lack of detail is concerning. Supervision is essential to assess the effectiveness of CASPs' governance, risk management, and resilience. The near absence of concrete supervisory actions or detailed reporting (see section 4.1) may in turn raise questions about the effective implementation of regulatory frameworks and their capacity to mitigate financial stability risks.

Table 3: Supervisory frameworks for CASPs

Jurisdiction	Category	Supervisory Mandate	Exams Conducted
Argentina	Limited	Limited supervision beyond AML/CFT compliance.	Conducted comprehensive on-site inspections in collaboration with the National Securities Commission.
Armenia	Comprehensive	Supervisory powers authorised under Law on crypto-assets to conduct on-site and off-site inspections.	No reported activity as no licenses have yet been granted.
Australia	Partial	Supervises consumer protection, market integrity, and operational risks under financial services laws.	No specific exams related to financial stability conducted.
Bahamas	Limited	Supervises regulatory compliance and enforcement for digital asset businesses (DABs).	Conducted on-site examinations of wallet service providers.
Bermuda	Comprehensive	Supervises financial stability risks, including credit, market, liquidity, operational, and systemic risks. Uses a risk-based approach for resource allocation.	Conducts on-site reviews based on risk ratings, thematic studies, and market monitoring.
Brazil	Under development	Developing a regulatory framework for financial stability risks. Plans to supervise governance, risk management, and IT/cyber risks.	Conducted preliminary examinations, including mapping crypto-asset offerings and assessing cross-border transactions.

Jurisdiction	Category	Supervisory Mandate	Exams Conducted
Canada	Partial	Supervises compliance and operational risks under securities laws.	Conducted examinations of restricted dealer CTPs to ensure compliance with registration conditions.
Chile	Comprehensive	Uses a risk-based supervision model to oversee compliance with laws and regulations. Examinations will consider prudential and market conduct requirements, in line with regulation.	No exams conducted yet; licensing process for financial service providers (FSPs) still underway.
France	Comprehensive	Supervisory powers authorised in domestic implementation of MiCAR. No specific areas of supervision defined.	No reported activity beyond AML/CFT compliance, despite 6 CASP licenses granted.
Germany	Comprehensive	Supervisory powers not yet authorised as domestic implementation of MiCAR remains in progress.	Conducted on-site inspections focusing on IT systems and business organisation.
Hong Kong	Comprehensive	Conducts both prudential and business conduct supervision.	Conducted on-site inspections of deemed VATP applicants, identifying gaps in cybersecurity, safe custody of client assets and KYC processes.
Hungary	Comprehensive	Supervisory powers authorised in domestic implementation of MiCAR. No specific areas of supervision defined.	No reported activity as no licenses have yet been granted.
Indonesia	Comprehensive	Supervisory powers authorised under Financial Sector Omnibus Law to conduct on-site and off-site inspections.	On-site examinations focus on trade operations, governance, compliance with legal provisions.
Italy	Comprehensive	Supervisory powers authorised in domestic implementation of MiCAR. No specific areas of supervision defined.	No reported activity beyond AML/CFT compliance
Ireland	Comprehensive	Supervisory powers authorised in domestic implementation of MiCAR.	No reported activity despite 2 CASP licenses granted.

Jurisdiction	Category	Supervisory Mandate	Exams Conducted
		No specific areas of supervision defined.	
Japan	Partial	Supervises internal controls, IT risk management, governance.	Conducted comprehensive inspections covering internal controls, IT risk management, and governance.
Korea	Partial	Supervises client asset safeguarding and prohibitions on market abuse.	FSC and FSS have conducted on-site inspections covering market abuse.
The Netherlands	Comprehensive	Supervisory powers authorised in domestic implementation of MiCAR. No specific areas of supervision defined.	No reported activity despite 14 CASP licenses granted.
Philippines	Comprehensive	Supervises IT infrastructure, cybersecurity, consumer protection, and governance systems.	Conducts on-site and off-site examinations, thematic reviews, and prudential assessments.
Poland	Comprehensive	Supervisory powers not yet authorised as domestic implementation of MiCAR remains in progress.	No reported activity as supervisory mandate not yet fully implemented.
Singapore	Partial	Supervises AML/CFT, IT risk management, governance, operational risk management.	Conducts on-site inspections and ongoing supervision covering areas such as AML/CFT, governance, IT risk management and internal controls.
Spain	Comprehensive	Supervisory powers authorised in domestic implementation of MiCAR. Supervises operational, governance and cybersecurity aspects as established in MICAR.	3 CASP licenses recently granted. No reported activity yet due to the recent authorisation.
Switzerland	Comprehensive	Supervises custody, operational risks, and systemic risks of entities already under direct FINMA supervision.	Conducts on-site inspections focusing on custody and operational risks.
Thailand	Comprehensive	Supervises compliance with Digital Asset Law, including onsite inspections and ongoing monitoring.	Offsite monitoring of IT and safeguarding of client assets, onsite inspections determined based on reporting and risk assessments.

Jurisdiction	Category	Supervisory Mandate	Exams Conducted
Türkiye	Comprehensive	CMB has powers to conduct supervision, including on-site examinations, of CASPs to verify compliance with all relevant requirements.	No reported activity as no CASP has been authorised by the CMB. Licencing applications of CASPs are being evaluated.
UK	Limited (existing[37])/ Under development	Currently, no supervision beyond AML/CFT compliance and financial promotions. A comprehensive supervisory framework for CASPs is under development by the FCA.	Supervision conducted for AML/CFT compliance and financial promotions.

2.3.1. Comprehensive supervisory programs

A group of jurisdictions have established supervisory frameworks that explicitly address financial stability risks by promoting resilience and soundness for CASPs.

These supervisory frameworks are largely modelled on those applicable to traditional financial institutions, with enforcement tools and powers similar to those used by financial regulators. The Bermuda Monetary Authority (BMA) uses a risk-based methodology to prioritise financial stability risks such as credit, market, liquidity, operational, and systemic risks (See Box 4). On-site inspections and thematic studies are conducted based on entities' risk and impact ratings, ensuring that supervisory resources are allocated effectively. However the maximum length of onsite activity (three days) may not be sufficient to comprehensively supervise CASP activities and risks.

Box 4: Proportionate supervision of CASPs - experiences from Bermuda

Bermuda employs a proportionate, risk-based approach to supervise Digital Asset Businesses (DABs) under the Digital Asset Business Act (DABA). Each DAB is assessed using two key ratings: a risk rating (low, medium, or high) and an impact rating (Category 1, 2, or 3). Risk ratings evaluate financial risks (liquidity, credit, and market) and non-financial risks (operational, IT, and cyber), while impact ratings measure the entity's scale, complexity, and significance within the digital asset ecosystem. These ratings determine the level of supervisory intensity, ranging from light-touch supervision for low-risk entities to high-frequency, in-depth engagement for systemically important firms.

This approach ensures supervision is tailored to the nature, scale, and complexity of each DAB. High-risk or high-impact entities undergo frequent reviews, including annual on-site inspections and stress testing, to assess their resilience to adverse conditions. Stress testing is a critical tool used to evaluate financial and operational stability, ensuring that DABs can withstand market volatility, liquidity pressures, or operational disruptions. Emerging risks, such as novel business models or cross-border activities, are proactively identified and addressed. In addition, BMA conducts off-site monitoring of

[37] CASPs that are designated as systemic would fall under the remit of the Bank of England and its powers to impose requirements, enforce against them and conduct supervision would apply. No systemic CASPs have been identified in the UK.

DABs. For example, new firms and DABs operating in its regulatory sandbox submit monthly data reports to BMA to facilitate monitoring.

The BMA complements entity-level supervision with systemic oversight through forums like the Macro-Micro Prudential Forum and the Financial Policy Council. These forums assess cross-sectoral risks and financial stability implications, ensuring a coordinated response to potential threats. By combining proportional supervision with forward-looking risk assessments, Bermuda's framework provides robust oversight while remaining flexible to innovations in the digital asset sector.

Thailand's SEC has conducted both off-site monitoring and on-site inspections of CASPs. These activities focus on compliance with financial, IT, and capital requirements. The SEC takes a risk-based approach to determine when on-site inspections are needed, and it actively monitors unlicensed CASPs operating in the jurisdiction. Specific supervisory actions include reviewing IT audits, capital maintenance reports, and ensuring corrective measures are taken for non-compliance. In Türkiye, the CMB has powers and mandates to conduct direct oversight, such as on-site examinations, to verify compliance with relevant CASP requirements. While CMB has not yet authorised CASPs in Türkiye, CMB plans to conduct on-site inspections to verify compliance with licensing, operational, and custody requirements, ensuring that CASPs maintain accurate, traceable records of transactions, wallets, and customer funds.

Hong Kong's SFC conducts both off-site monitoring and on-site inspections on CASPs. These activities focus on assessing CASPs' compliance with financial and non-financial requirements. Separately, on-site inspections of deemed CASPs applicants revealed gaps in cybersecurity, safe custody of client assets and KYC processes, prompting the SFC to issue clarifications on expected standards.

In the Philippines, the central bank also adopts a risk-based approach to supervision, focusing on IT infrastructure, cybersecurity, consumer protection, governance systems, and AML/CFT compliance. Both on-site and off-site examinations are used to assess the broader impact of VASPs on financial stability. Switzerland also incorporates financial stability into its supervisory framework with FINMA conducting on-site inspections that focus on custody, operational risks, and compliance with the travel rule, while systemic risks are monitored through regular surveys and data analysis. However, Switzerland's supervisory framework only applies to firms already under FINMA supervision or entities which meet the criteria for existing financial regulations, with some crypto-asset service providers falling outside the purview of FINMA's supervision.

In the EU, CASP supervision is conducted by NCAs at national level with ESMA tasked to ensure convergence of supervisory practices at the EU level. To carry out this responsibility, ESMA conducts peer reviews to assesses and report on the supervisory practices of EU NCAs. NCAs are granted extensive supervisory powers, including the authority to request information and documents, conduct on-site inspections, and prevent market abuse. However, bearing in mind MiCAR entered into force in December 2024 for CASPs, to date NCAs have not yet fully implemented supervisory powers and inspection activity remains limited. For example, due to an early implementation of a national regulatory framework for CASPs in 2020 (i.e. before EU-wide implementation of MiCAR) Germany's BaFin has conducted several on-site inspections of CASPs, emphasising IT systems, business organisation, and AML/CFT processes; while Ireland, Italy, France, the Netherlands, and Spain have reported limited supervisory activities at this stage following the recent authorisation of numerous CASPs under MiCAR.

In Chile, the CMF supervises CASPs' compliance with laws and regulations using a risk-based model. While licensing processes are still underway, the CMF is preparing to implement supervisory activities, including a four-tier risk management assessment scale for intermediaries and custodians of financial instruments. This scale considers the assessment of the role of the board, as well as of a risk management system that should cover credit, market, liquidity, operational, custody, conduct and ML/FT risks. In line with the regulation, the supervisory process considers risk-based capital and proportionality in the application of prudential requirements, as well as risk-related reporting.

2.3.2. Partial Supervisory programs

Several jurisdictions have supervisory frameworks that address broader risks, such as IT security, governance, and operational risks, but do not explicitly focus on financial stability. For example, Australia's ASIC supervises CASPs under existing financial services laws, emphasising consumer protection, market integrity, and operational risks. While ASIC's framework is technology-neutral, no specific exams related to financial stability have been conducted. Similarly, Canada's approach under the Canadian Securities Administrators focuses on compliance and operational risks. The Ontario Securities Commission has conducted examinations of restricted dealer crypto asset trading platforms (CTPs) to ensure compliance with registration conditions, but no exams specific to financial stability have been conducted.

Japan's FSA conducts comprehensive inspections covering internal controls, IT risk management, and governance. In Singapore, the Monetary Authority of Singapore (MAS) primarily focuses on financial integrity risks, conducting on-site and off-site reviews of CASPs while leveraging blockchain analytics tools to monitor compliance. Korea also primarily supervises financial integrity risks, but also supervises safeguarding of customer assets and market abuse. Although these jurisdictions address broader risks, they have yet to explicitly incorporate financial stability into their supervisory mandates.

2.3.3. Limited supervisory programs

A third group of jurisdictions remains primarily focused on AML/CFT compliance, with limited supervisory frameworks addressing broader risks or financial stability. Argentina's Financial Intelligence Unit (FIU) supervises CASPs for AML/CFT compliance through on-site and off-site inspections, conducted in collaboration with the National Securities Commission. Similarly, The Bahamas' Securities Commission supervises digital asset businesses (DABs) for AML/CFT compliance, conducting on-site examinations of wallet service providers. However, many DABs in The Bahamas are still in early operational stages, and supervisory efforts remain concentrated on AML/CFT training and enforcement.

The United Kingdom's Financial Conduct Authority (FCA) supervises CASPs under the Money Laundering Regulations. The FCA has conducted firm visits and inspections as part of its AML/CFT supervision, with recent multi-firm assessments of AML/CFT frameworks. While these jurisdictions have implemented AML/CFT measures, their supervisory frameworks do not yet extend to broader risks or financial stability considerations.

2.4. Enforcement

Enforcement is a critical aspect of effective crypto-asset regulation, as highlighted in CA Recommendation 1 of the FSB's high-level recommendations: "Authorities should have and utilise the appropriate powers and tools, and adequate resources to regulate, supervise, and oversee crypto-asset activities and markets, and enforce relevant laws and regulations effectively, as appropriate." The variation in enforcement frameworks across jurisdictions reflects different stages of implementation and diverse approaches to managing risks in this rapidly evolving market.

Jurisdictions can generally be grouped into three categories based on the comprehensiveness of their enforcement tools: Comprehensive Enforcement Frameworks, Partial Frameworks with Gaps, and Minimal or Undefined Frameworks (see Table 4). Many jurisdictions have implemented robust frameworks with a wide range of enforcement measures, while others are still developing or refining their approaches. These categories highlight both the strengths and areas for improvement in national enforcement strategies, offering a snapshot of the global regulatory landscape for crypto-assets.

Table 4: Comprehensiveness of crypto enforcement tools across jurisdictions

Comprehensive enforcement frameworks	Partial frameworks with gaps	Minimal or undefined frameworks
Armenia, Australia, The Bahamas, Bermuda, Canada, EU members, Hong Kong, Philippines, Singapore, Switzerland, Thailand, Türkiye, UK	Argentina, Chile, India, Korea, Mexico, Nigeria, Saudi Arabia, Uruguay	China, Lebanon

2.4.1. Comprehensive Enforcement Frameworks

Many jurisdictions have comprehensive enforcement capabilities, employing a range of tools to regulate crypto-assets effectively. These include license suspension, the power to impose penalties, and international cooperation mechanisms. Jurisdictions such as Australia and Singapore use these tools effectively. In the EU member states benefit from a harmonised approach under the MiCAR framework, ensuring consistency in enforcement across borders. Canada employs innovative measures such as reciprocal enforcement orders and website blocking to address non-compliant platforms. Similarly, Hong Kong combines domestic enforcement with bilateral agreements to tackle cross-border challenges. Switzerland leverages tools such as investigative agents and asset freezes, while Thailand collaborates with multiple agencies to restrict access to unlicensed platforms and enforce civil and criminal penalties. In Bermuda, the BMA has powers to impose civil penalties; restrict or revoke a license; object to existing, new, or increased control of shareholder controllers; apply to the court for injunctions or winding up of a CASP; and prohibit individuals from performing certain or all roles or functions if they are not fit and proper persons. In Türkiye, CMB has a wide range of powers to address non-compliance and unauthorised activities in the crypto-asset sector, including the ability to block internet access to unauthorised service providers. In Armenia, the central bank also has powers to revoke or withdraw licenses and authorisations as well as impose penalties. Finally, authorities in the Bahamas and the Philippines have powers to suspend licenses, stop

unregistered activities, and impose monetary penalties. These jurisdictions exemplify a comprehensive approach, ensuring market integrity, consumer protection, and effective oversight of crypto-assets.

Enforcement experiences in these jurisdictions highlight proactive and diverse measures. Australia has taken action against major entities like Binance Australia and Kraken, addressing unlicensed conduct and consumer protection failures. Canada issued hundreds of investor warnings in 2024 and imposed sanctions on offshore platforms like XT.com and CoinEx. Switzerland conducted 44 investigations into unauthorised crypto activities, issued cease-and-desist orders, and initiated criminal proceedings in some cases. The UK disrupted 30 unregistered crypto ATMs, issued 1,700 consumer alerts, and took down over 900 scam websites. However, these jurisdictions face common challenges, such as cross-border enforcement, pseudonymous transactions, regulatory arbitrage, and the technical complexity of DeFi and blockchain analytics. For example, Canada and Switzerland have highlighted the difficulty of enforcing freeze orders or addressing forum shopping by crypto companies. These challenges are mitigated through international cooperation frameworks like the IOSCO MMoU and investments in advanced technological tools.

2.4.2. Partial enforcement frameworks

Several jurisdictions have made progress in regulating crypto-assets but lack one or more critical enforcement tools. Argentina has mechanisms to revoke registrations and block URLs of unregistered entities but does not explicitly address cross-border enforcement. Under its AML-CFT framework, India blocks apps and websites of unregistered CASPs, including offshore ones, and has recovered fines from non-compliant offshore CASPs, requiring them to either register with the Financial Intelligence Unit (FIU)-IND or cease services for Indian users. Korea has frameworks for inspections and penalties but lacks explicit cross-border enforcement tools. Mexico allows for the revocation of authorisations and imposes sanctions but does not provide clear mechanisms for addressing unregistered activities or international cooperation. Chile has established broad enforcement and sanctioning powers for the CMF, however the enforcement framework is still under development as CASP licenses have not yet been granted. In Nigeria, the SEC has enforcement powers to take action against entities dealing in crypto-assets. Saudi Arabia restricts unlicensed activities domestically but does not explicitly include monetary penalties or cross-border enforcement in its framework. Uruguay has supervisory powers for money laundering and terrorism financing prevention and can revoke authorisations but lacks tools to address unregistered activities or cross-border challenges. These jurisdictions have a solid foundation but would benefit from addressing these gaps to enhance their enforcement frameworks.

Enforcement actions in these jurisdictions are more limited and often focus on specific violations. Argentina has applied remedial measures to one VASP for AML/CFT compliance, while Mexico imposed a pecuniary sanction on a Financial Technology Institution for misleading information. Korea is in the early stages of enforcement under its new regulatory framework, which focuses on user protection and unfair trade practices. Challenges in these jurisdictions include incomplete regulatory frameworks, limited cross-border enforcement mechanisms, and adapting to the rapid pace of technological innovation. Mexico, for instance, highlights the difficulty of addressing emerging technologies like stablecoins within existing legal frameworks, while Korea is revising its regulations to address fraudulent behaviour and improve listing disclosures. These

jurisdictions are taking steps toward stronger enforcement but require further development to address these challenges comprehensively.

2.4.3. Minimal or undefined frameworks

A smaller number of jurisdictions have limited or unclear enforcement powers, which may hinder their ability to regulate crypto-assets effectively. Lebanon and China do not specify any enforcement capabilities nor explain underlying regulations. These jurisdictions may face challenges in addressing risks associated with unregistered or non-compliant entities and should develop appropriate regulation enabling enforcement measures to better address the challenges of the crypto-asset market.

2.5. CA implementation progress: overall findings

The review of implementation of the CA recommendations highlights notable progress in regulating crypto-asset activities but reveals significant gaps and diverging approaches that pose risks to financial stability. While some jurisdictions have implemented regulatory frameworks, few of those jurisdictions have frameworks that are fully aligned with the FSB CA recommendations.

A critical gap is the lack of comprehensive coverage of CASP activities that give rise to leverage and liquidity risks, such as crypto-asset borrowing, lending, and margin trading. Only two jurisdictions comprehensively cover these activities in their crypto-asset regulatory frameworks, whereas for other jurisdictions these activities are beyond the scope of their regulatory frameworks. Supervision and enforcement also lag behind regulatory development, with many jurisdictions yet to implement supervisory and enforcement tools to ensure comprehensive oversight and compliance with regulatory requirements.

This uneven implementation indicates that jurisdictions should undertake further efforts to achieve full and consistent implementation of the CA recommendations. Uneven and fragmented implementation can create opportunities for regulatory arbitrage and complicate cross-border oversight of the rapidly evolving, inherently global crypto-asset market.

3. Implementation of the GSC recommendations

The GSC recommendations seek to promote consistent and effective regulation, supervision and oversight of stablecoin arrangements across jurisdictions to address the financial stability risks posed by stablecoins. The recommendations are intended to be flexible so that they can be incorporated into the wide variety of regulatory frameworks potentially applicable to stablecoins around the world.

Progress in the implementation of comprehensive regulatory frameworks for GSCs remains uneven and slower compared to the CA recommendations (see tables 2 and 5). To date, five jurisdictions (21%) reported having a finalised regulatory framework for stablecoins, compared to 11 (39%) for crypto-assets. However, 10 jurisdictions (34%) are in the process of consulting on or finalising GSC frameworks, suggesting significant progress may be made in the coming

year or two, while three jurisdictions (10%) have partial regulations in place and eleven (38%) remain at an early stage with no framework.

Table 5: Summary of GSC implementation status by jurisdiction

Jurisdiction	Stage of progress[38]	Implementation summary
Argentina	1	Argentina has no specific regulation in force that addresses stablecoins.
Armenia	4	Parliament approved a regulatory framework conferring mandate to the CBA for regulating and overseeing stablecoin arrangements, including licensing requirements for stablecoin issuers. The framework came into force in July 2025. Detailed regulations remain under development.
Australia	3	Stablecoins may meet existing definitions of 'financial products,' and depending on their structure may be considered a non-cash payment facility, managed investment scheme, debentures, or derivatives. The Australian Government has proposed plans to regulate stablecoins linked to the value of fiat currency.
The Bahamas	5	The Digital Assets and Registered Exchanges Act (2024) and establishes a regulatory framework for stablecoin activities. The Bahamas SEC intends to clarify additional requirements for stablecoin issuers.
Bermuda	5	The Digital Business Act (2018) establishes a regulatory framework for the issuance of crypto-assets, including stablecoins. BMA has issued Guidance for Single Currency Pegged Stablecoins (2024).
Brazil	3	The Brazilian Parliament is discussing a bill that will regulate stablecoins similar to Law 14.478 for virtual assets.
Canada	2	Existing provincial securities laws apply where stablecoins, or the arrangements in respect of stablecoins, are securities or derivatives.
Chile	1	Stablecoins are treated and regulated the same as all other crypto-assets. Central Bank of Chile may regulate the standards and minimum conditions for the use of stablecoins in the context of the settlement of payment orders carried out in systems that it regulates or recognises.
China	1	All crypto-asset activities are prohibited in China.
EU	5	MiCAR establishes EU-wide regulation and supervisory requirements for stablecoin issuers. Supervision of stablecoin issuers is delegated to NCAs with EBA co-supervising "significant" issuers. The regulatory framework on stablecoins, including supporting regulations and guidance, is fully in force since June 2024.
Hong Kong	5	The Stablecoins Ordinance (2025) establishes a regulatory framework for stablecoin issuers and empowered the HKMA to implement a licensing and supervision regime for such issuers. The regulatory

[38] Stages of progress include: 1: No framework in place; 2: Partial regulations in place; 3: Plans for framework under public discussion 4: Framework proposed but not finalised; 5: Regulatory framework finalised. See Annex 1 for more detail.

Jurisdiction	Stage of progress[38]	Implementation summary
		framework, including supporting guidance, is fully in force since August 2025.
India	1	The government of India is examining policy approaches to implement the GSC recommendations.
Indonesia	1	OJK and Bank Indonesia plan to develop regulation for stablecoins in close coordination.
Japan	5	The Payment Services Act was amended in 2022 (effective 2023) to include requirements for electronic payment services, which covers stablecoin activities.
Kazakhstan	1	The issuance, use, and operation of exchanges dealing with stablecoins are prohibited in the Republic of Kazakhstan, except for activities within the territory of the Astana International Financial Centre.[39]
Korea	3	Korea plans to finalise legislation and regulations for stablecoins in the coming years.
Lebanon	1	The Banque de Liban has issued public announcements warning against using crypto-assets and no stablecoin issuers have been licensed while the regulatory framework for crypto-assets remains under development.
Mexico	1	The Fintech Law (2018) establishes regulations for the operations of stablecoin activities and empowers the Banco de Mexico to authorise financial technology institutions and credit institutions to operate with crypto-assets. Currently, Banco de Mexico has not designated any crypto-assets as legal assets and for financial institutions, restricts the use of crypto-assets to internal transactions not involving the public.
Nigeria	3	The Investment Securities Act (2025) establishes a regulatory framework for crypto and other digital assets, including stablecoins. The Nigeria SEC is reviewing the need for further rulemaking.
Philippines	2	Stablecoins may be regulated under the principles and requirements applicable to e-money issuers, however, there is no separate regulatory framework for stablecoins.
Saudi Arabia	1	Stablecoin activities are prohibited and no CASPs have been licensed while the regulatory framework for stablecoins remains under development.
Singapore	4	All crypto-asset activities, including stablecoins, are subject to the DPT regime in Singapore. MAS plans to introduce a bespoke framework for single currency stablecoins that will subject stablecoin issuers that opt in to higher requirements.

[39] The regulatory framework of the Astana International Financial Centre was not in scope for this review.

Jurisdiction	Stage of progress[38]	Implementation summary
South Africa	1	South Africa is currently formulating its policy approach to stablecoin regulation under the auspices of the Intergovernmental Fintech Working Group.
Switzerland	3	Depending on the specific purpose and characteristics of a stablecoin arrangement, different financial market laws may apply. FINMA published guidance (2019) with an indicative classification of different categories of stablecoins under supervisory law. Swiss authorities are currently drafting a bill to amend financial market legislation.
Thailand	2	Stablecoins may be used as investment vehicles and subject to oversight by the Thailand SEC. The Bank of Thailand currently has no specific regulations governing the use of stablecoins for payments. However, innovations similar to stablecoins are being tested within a regulatory sandbox and may inform future regulatory approaches.
Türkiye	1	Under the Capital Markets Law, there is no regulation specific to stablecoins.
UK	4	The UK Treasury has published draft legislation for regulating crypto-asset activities, including stablecoin issuance. The UK FCA and the Bank of England have published consultations and proposed regulatory approaches to stablecoins.
Uruguay	3	The Virtual Asset Act (2024) clarifies the legal classification and licensing requirements of crypto-asset activities, including stablecoins. The Banco Central Del Uruguay is developing more detailed regulations to implement the Virtual Asset Act.
US	4	The GENIUS Act (2025) establishes regulation and oversight requirements for stablecoin issuers. The US Federal Banking Agencies, among other agencies, are in the process of implementing the legislation.

3.1. Regulatory frameworks for stablecoins

Jurisdictions exhibit varying approaches and stages in regulating stablecoin issuers and their arrangements. Some jurisdictions have implemented, or are in the process of implementing, specific regulatory frameworks tailored to stablecoins, including Armenia, The Bahamas, Bermuda, the European Union, Hong Kong, Japan, Singapore, and the US. Others, such as Australia, Canada, Chile, Mexico and Uruguay classify stablecoins under existing financial product laws but apply different approaches: Australia, in certain cases, treats stablecoins as financial products, such as non-cash payment facilities or derivatives; Canada[40] primarily

[40] Stablecoin issuers are required to comply with applicable securities laws. In addition, CASPs are required to confirm that a stablecoin satisfies certain terms and conditions in order to offer the stablecoin to clients.

classifies them as securities or derivatives; Chile, Mexico[41] and Uruguay[42] consider them as payment instruments under existing regime but the specific stablecoin regulation has yet to be drafted in such countries

A group of jurisdictions, including Argentina, Nigeria, South Africa, and Türkiye, apply the same rules as other crypto-assets to stablecoins, while South Africa primarily regulates them from the AML/CFT perspective. Several jurisdictions,[43] including some with partial frameworks, are exploring or drafting tailored regulatory approaches for stablecoin issuers to address regulatory gaps or complement existing rules. Meanwhile, another group of jurisdictions, including Argentina, India, Indonesia, and Kazakhstan have no specific framework or approach in place. As mentioned earlier, China, and Saudi Arabia have imposed a prohibition on crypto-asset activities, including stablecoins.

While jurisdictions vary in their approaches to regulating stablecoins, there is a noticeable trend toward recognising the limitations of applying existing regulatory frameworks (unless materially adjusted), such as securities or payment regulations, to stablecoin issuers and activities. In jurisdictions where securities regulation is being used as a temporary measure, authorities acknowledge its limited adequacy for addressing the unique risks and characteristics of stablecoins. Similarly, existing payment regulations are often insufficient to fully capture the complexities and potential risks posed by stablecoin arrangements (e.g., reliance on public blockchains), prompting jurisdictions to adopt tailored rules to address their novel risks and use cases. Importantly, no jurisdiction that has finalised a comprehensive framework for stablecoins has explicitly classified stablecoins as securities or collective investment schemes. Instead, regulatory efforts are increasingly converging toward treating stablecoins as payment instruments. Among jurisdictions that have implemented specific frameworks, such as the EU, Hong Kong, and Japan, stablecoins are typically regulated in ways that align more closely with e-money or banking regulations, although the store of value use case is not neglected.[44] This reflects their possible use in payment systems and highlights the growing recognition of the need for tailored regulatory frameworks that go beyond the temporary application of existing rules.

3.2. Licensing and authorisation

3.2.1. Entities allowed to obtain a license or authorisation

Jurisdictions with a stablecoin regulatory framework in place prescribe either a dedicated stablecoin licence or a banking licence to commence the stablecoin issuance business. In most jurisdictions that have implemented a dedicated regulatory framework for stablecoins, banks are

---

41 Depending on the circumstances, stablecoins can meet the conditions for being classified as *Electronic Payment Funds (IFPE)* which would mandate the application of the relevant regime, including the obligation for issuers to secure an IFPE license. However, Mexico has no stablecoin regulation at the moment.

42 In Uruguay, stable virtual assets that meet the conditions of electronic money are treated under the Financial Inclusion Law. Some types of stablecoins, however, are not covered by this regime.

43 Australia, Brazil, Philippines, Saudi Arabia, Switzerland, Thailand, United Kingdom and Uruguay.

44 Hong Kong's legislation sets that stablecoins are used or intended to be used as medium of exchange for one or more of the three purposes stated including investment. EU MiCAR refers in the preamble that asset-referenced tokens (ART) 'could be widely adopted by holders to transfer value or as a means of exchange' implying that have also other functions. Indeed, the EU legislation has established that ARTs and foreign denominated EMTs cannot be used as means of payments beyond certain limits.

explicitly permitted to issue stablecoins, often leveraging their existing regulatory status.[45] However, some jurisdictions require the bank to issue its stablecoins through a subsidiary not licensed to take deposits.[46] In Bermuda, a bank wanting to issue a stablecoin needs to secure a separate licence (single currency pegged stablecoin). Three jurisdictions, the EU, Japan and Singapore, indicate the possibility for a bank to issue a balance sheet backed stablecoin, namely without the requirement to establish a dedicated reserve of assets.[47]

In addition to banks, electronic money institutions (EMIs) and payment service providers are also commonly allowed to issue stablecoins. The EU restricts the issuance of electronic money tokens (EMTs) to banks and EMIs. In Armenia, payment service providers and banks authorised to issue e-money are similarly allowed to issue stablecoins. In Japan, apart from banks, only trust companies and funds transfer service providers are permitted to issue stablecoins, reflecting a focus on leveraging payment firms' expertise and infrastructure.

Several jurisdictions also allow non-bank entities to issue stablecoins, provided they meet specific licensing requirements. For instance, in Bermuda and The Bahamas, non-bank entities can obtain licenses to issue stablecoins under principles-based frameworks that assess issuers on a case-by-case basis. In Hong Kong, non-bank entities can apply for stablecoin licenses, but they must demonstrate adequate capabilities and resources before issuing additional types of stablecoins. In the US, non-banks will be able to obtain a license from the OCC to issue a payment stablecoin.[48] In Singapore, under the forthcoming regime, non-bank entities can apply to be MAS-regulated stablecoin issuers if their stablecoin meets requirements. Similarly, in the UK, the regulatory regime under discussion does not propose restrictions on the type of firm that can issue stablecoins, though systemic issuers would be subject to heightened requirements. The EU allows non-bank entities to obtain a specific license to issue asset-referenced tokens (ARTs), provided they meet the authorisation requirements. In Australia, if a stablecoin is not a financial product there are no restrictions for banks regarding issuance beyond general consumer laws. If the stablecoin is a financial product then the entity would require a licence from the local market supervisor (unless an exemption applies).

Restrictions on activities once a license is granted also vary. For instance, Singapore intends to prohibit stablecoin issuers from conducting any other activity, while Hong Kong requires prior approval from the supervisor to expand business activities.[49] In contrast, the EU and Bermuda do not impose hard rules on the scope of activities, although authorities retain the power to intervene if necessary. In the EU specific rules are set for the case of the same token issued by more than one entity all established in the EU, including requirements for a single reserve of assets, custody policy as well as coordinated recovery and resolution plans. Meanwhile, in Switzerland, existing stablecoins in the market are from issuers using the so called 'default

---

45 This is the case in the EU, Hong Kong and Japan.

46 In the US, pursuant to the GENIUS Act, subsidiaries of insured depository institutions, rather than the insured depository institutions themselves, may issue payment stablecoins. Other entities that will be permitted to issue payment stablecoins under the GENIUS Act include non-bank entities, federal branches, and uninsured national banks.

47 In such cases stablecoins are considered as any other liability of the bank against its entire estate vis-á-vis token holders.

48 In the US, the GENIUS Act will prohibit a public company, and its wholly or majority owned subsidiaries or affiliates, that is not predominantly engaged in one or more financial activities from issuing a payment stablecoin unless the public company obtains a unanimous vote from the Stablecoin Certification Review Committee.

49 In Hong Kong a licensee should demonstrate to the authority, before issuance of an additional type of specified stablecoins, that it has adequate capabilities and resources for any new business activity.

guarantees from banks', which means they do not require a licence under banking law, but instead only need to be affiliated to a self-regulatory organisation for AML/CFT purposes only. This regime gives rise to risks for stablecoin holders and the guaranteeing banks. Given the absence of any registration obligation with the regulatory authority for such issuer, Swiss authorities' knowledge of issuers relying on such bank guarantees is somewhat limited. Swiss authorities are currently drafting a bill to amend Swiss financial market legislation, examining notably whether the legal framework for payment service providers (including stablecoin issuers) needs to be amended.

The range of regulatory frameworks for stablecoin issuers reflects differing maturity of regulatory processes as well as different approaches to financials sector regulation and priorities with respect to stablecoin activities in a jurisdiction. While stricter frameworks provide for better safeguards at a price of higher compliance cost for firms, more lenient regimes could attract issuers seeking lighter requirements, hence raising the risk of regulatory arbitrage. Divergences in licensing regimes could present challenges to global stablecoin issuers who need to comply with different rules across jurisdictions. An uneven playing field is not conducive to sound and efficient market functioning. As the stablecoin market evolves, international coordination will be critical to balancing innovation and financial stability while addressing these regulatory disparities.

Box 5: Stablecoins issued from multiple jurisdictions[50]

Stablecoins issued from multiple jurisdictions would involve issuance by the same or affiliate entities (i.e., co-issuers) operating across different jurisdictions (hereafter referred to as a "multi-jurisdictional stablecoin arrangement"). These issuers may market their stablecoin as the same token or as different tokens, but each token may be fungible with the others in the arrangement. Such issuers could share technical infrastructure and commit to apply the same risk management principles but are held to comply with, inter alia, various reserve of assets and redemption requirements. Concern about the multi-jurisdictional stablecoin arrangement has gained prominence among many FSB members as issuers seek to increase their scale of operations (a driver of profitability in observed business models) by proposing to clients a token that is negotiable in various jurisdictions although subject to different regulatory frameworks. However, the fungibility of these tokens across jurisdictions can introduce operational complexity, financial stability risks and regulatory challenges.

Many FSB members believe the multi-jurisdictional stablecoin arrangement could pose higher liquidity and operational issues, leading to financial stability risks. In particular, liquidity risk could be exacerbated in arrangements wherein each co-issuer could be liable for the entire stock of tokens in circulation while holding only a fraction of the overall reserve of assets. Multi-jurisdictional stablecoin arrangements generally represent that reserve assets can be moved across jurisdictions via "reserve rebalancing" from one co-issuer to another as needed to fulfil redemption requests. However, jurisdictions appear to be differing in their approaches to stablecoin regulation, with some imposing stricter prudential, reserve (including on location of reserve assets) and redemption requirements than others, which may cause challenges in reserve management.

These variations can create situations where not all entities within the same multi-jurisdictional stablecoin arrangement are held to the same standards of prudential resilience and heighten the risk of under-collateralisation at the entity or consolidated level. In particular, the quantification of the redemption risk borne by each co-issuer may be hindered by the use of unhosted wallets which can prevent proper identification of token holders' geographic location (which tends to correlate with

[50] The analysis in this box is derived from responses to the FSB questionnaire.

destination of redemptions). But the extent of this risk will depend on the extent of the continued use of unhosted wallets in the future. The multi-jurisdiction stablecoin arrangement's riskiness could also be magnified by reporting gaps and the issuance by entities in jurisdictions without comprehensive regulatory frameworks.

Redemption risk may not be equally borne by all co-issuers when they are held to different obligations in terms of redemption timeline and costs: for instance, token holders under stress conditions have an incentive to seek redemption from the co-issuer obliged to pay back with the shortest timeline and without charging fees. On the other hand, to the extent permitted by regulations, issuers may have an incentive to maintain the greatest amount of reserve assets in the jurisdiction offering the highest level of flexibility in terms of eligible assets they may even have an incentive to represent that most of their tokens are held by the residents of such jurisdiction. Moreover, issuers may have an incentive to seek a licence from those jurisdictions whose regulation is perceived as more token-holder friendly and use that as a marketing tool.

Other factors could exacerbate these concerns depending on how precisely the issuance was organised. For example, issues may arise if multi-jurisdictional stablecoin arrangements operate with insufficient transparency, such that the full extent of global operations, the geographical location of reserves, or the location of direct claims for redemption are not clearly disclosed. Particular care would also need to be taken to ensure that such multi-jurisdictional stablecoin arrangements are not exposed to additional risks, such as the potential for illicit actors to spread misinformation to push the price of tokens below par, purchase them on the secondary market, and seek redemption in jurisdictions where redemption fees are lowest.

Some FSB members believe the soundness of the multi-jurisdictional stablecoin arrangement depends on strong cross-border cooperation between supervisory authorities to ensure the size, quality, and location of reserves are sufficient at all times**.** However, differing legal frameworks across jurisdictions and insufficient cross-border supervisory cooperation may incentivise regulatory arbitrage, potentially undermining financial stability, especially in the least regulated jurisdictions. Prudential frameworks, which often determine requirements based on jurisdictional holdings or size, may not reflect consolidated risks. Contractual obligations between co-issuers (e.g., reserve rebalancing) may not be enforceable, particularly in stress scenarios or may be halted by measures adopted by a local authority to mitigate risks to their domestic financial system. From a regulatory perspective, the multi-jurisdictional stablecoin arrangement may pose significant challenges if each authority approaches the arrangement independently. However, strong supervisory cooperation may enable authorities to access information, acquire a consolidated view of the entity and conduct thorough oversight and enforce prudential requirements across borders.

Various jurisdictional authorities have expressed concerns about the permissibility of multi- jurisdictional stablecoin arrangements, while some others have enabled them while they assess how to mitigate the inherent risks. The borderless and fast-evolving nature of crypto-asset markets also challenges regulators' ability to respond promptly to emerging risks. More aligned approaches to redemption rights, reserve requirements, and governance arrangements, may be warranted by jurisdictions hosting multi-jurisdictional stablecoin arrangements.

Comprehensive and aligned implementation of the GSC recommendations across jurisdictions offers the opportunity to mitigate the inherent risks of the multi-jurisdictional stablecoin arrangement. In the absence of greater regulatory uniformity, the effectiveness of the 'rebalancing mechanism' – which is key for the smooth functioning of the arrangement – can be compromised by actions of individual jurisdictions to protect their domestic financial system or operational incidents. The use of the arrangement across jurisdictions not having fully and properly implemented the GSC recommendations (with particular focus on international cooperation) poses risks to financial stability.

3.2.2. Licenses and authorisations granted

Despite the implementation of licensing and authorisation frameworks for stablecoin issuers in several jurisdictions, the number of licenses and authorisations granted remains limited, particularly relative to the number of existing stablecoin issuers in the market today. In the EU, as of August 2025, 16 EMTs have been issued in accordance with MiCAR by 10 different entities (one credit institution and nine e-money institutions). No ARTs have been issued yet. In Japan, a company has received regulatory approval to issue a yen-denominated stablecoin and is currently preparing for its launch as of 3 September 2025. In Bermuda, BMA has issued over 10 DAB licenses to stablecoin issuers. No other jurisdiction included in the peer review has granted a license or authorisation for stablecoin issuance. This is mostly the consequence of the recent enactment of the regime in some jurisdictions (e.g., Hong Kong) and in some other cases the regulation is not applicable until rules and regulations are developed and come into force (e.g., US). In the US, several stablecoin arrangements operate from the US under existing state regulatory frameworks for money services business and will transition to federal regulation, as appropriate or required, when provisions of the recently enacted federal framework come into force.[51]

Several jurisdictions have accepted or registered an undertaking or handling of stablecoins issued from another jurisdiction. For example, Canada has accepted an undertaking from one such issuer although the undertaking does not constitute compliance with securities laws, and in Japan, one intermediary has been registered to handle a stablecoin issued in another jurisdiction.

The limited number of licenses and authorisations granted contrasts with the increase growth observed in the market, suggesting stablecoin issuers continue to operate from jurisdictions beyond the FSB membership and those jurisdictions included in this review. The continued operation of stablecoin issuers from jurisdictions with limited or even no regulatory framework creates regulatory challenges for all other jurisdictions to address the risks of these stablecoins operating from jurisdictions beyond their own.

3.2.3. Access to central bank payment systems

Approaches to stablecoin issuers' access to central bank payment systems for their settlement with other financial institutions and their ability to hold reserves with the central bank varies across jurisdictions, reflecting differences in regulatory frameworks, central bank policies and priorities. In the EU, issuers of EMTs may have direct access to central bank payment systems due to their status as credit institutions or electronic money institutions, but the latter are not allowed to hold reserves at the central bank. Issuers of ARTs, without such institutional status,[52] can only access these systems indirectly through intermediaries. The UK proposes to require systemic stablecoin issuers to hold some of its reserve assets in central bank deposits to ensure it can fulfil redemption requests, emphasising that systemic stablecoins must meet the same standards as other forms of money to ensure trust in money itself, which UK authorities believe is crucial for financial stability. In Armenia, banks and payment service providers authorised to

---

51 US state regulatory frameworks for money services businesses are not in scope of this review.

52 If an issuer is a payment institution it also has access direct to the payment system.

issue e-money tokens have direct access to the central bank's payment system, while other stablecoin issuers can only access domestic systems indirectly via banks.

In contrast, some jurisdictions explicitly prohibit central bank access for stablecoin issuers. For example, in Hong Kong, stablecoin licensees that are not licensed by HKMA as banks or branches have no direct access to the central bank's payment system and rely on the banking system for subscription and redemption of stablecoins. Similarly, in Singapore, stablecoin issuers are explicitly denied direct access to the central bank's payment system. In Bermuda, where there is no central bank, stablecoin issuers do not have access to domestic payment systems beyond operational and client accounts. These prohibitions reflect a cautious approach to granting stablecoins access to critical financial infrastructure and emphasise reliance on existing banking systems.

The GSC recommendations do not specify whether stablecoin issuers should have access to central bank payment systems or not, which raises policy questions. On the one hand, differentiated access of stablecoin issuers to central bank payment systems based on the entity type or jurisdiction could create an uneven playing field or affect run dynamics. For example, during periods of stress, users may perceive stablecoins whose issuer has access to the central bank as safer than those issuers that do not have access. This issue may be even more challenging for the same stablecoin issued from multiple jurisdictions. On the other hand, central bank access is a complex and jurisdiction specific policy choice which may depend on factors beyond a jurisdiction's regulatory framework for stablecoins.

3.2.4. Restrictions on the listing of stablecoins with CASPs or other trading platforms

Jurisdictions' approaches to listing of stablecoins on trading platform can be grouped in three categories reflecting differences in regulatory maturity, risk assessment and priorities.

Some jurisdictions, such as such the EU,[53] Hong Kong, the Bahamas, and Japan, restrict listing for some or all users to locally licensed stablecoins. In particular, in Hong Kong, unlicensed stablecoins can be listed for professional investors but are restricted to licensed stablecoin issuers for retail investors.[54] In addition, Japan prohibits the circulation or intermediary activities relating to foreign-issued stablecoins unless they obtain the specific requisite "Electronic Payment Instruments Exchange Service Provider" license – and currently only one entity has this license.

Where there is no licensing requirement for trading stablecoins (e.g. because there is not a stablecoin regulation) CASPs have the onus of ensuring that only stablecoins fulfilling certain conditions can be negotiated. In this category are: Switzerland requiring CASPs to ensure that only appropriately supervised crypto-assets, including stablecoins, are approved for trading; Canada, where stablecoin issuers are required to comply with applicable securities laws and CASPs are required to confirm that a stablecoin satisfies certain terms and conditions in order to offer the stablecoin to clients; Bermuda where DABs operating a trading platform must conduct proper due diligence to ensure risk profiles of digital assets admitted meet pre-defined criteria;

---

53 The EU required the delisting of non-MiCAR compliant stablecoins by 31 December 2024, although the enforcement in case of non-compliance was delayed to 31 March 2025.

54 Prior to the implementation of Hong Kong's stablecoin regime, no CASPs could list a stablecoin for retail investors on its platform.

and the Philippines where VASPs are required to inform the central bank of any newly listed tokens which is expected to have been subject to VASPs' due-diligence. Singapore does not prescribe restrictions on offering of stablecoins but requires CASPs to perform token assessments before listing, which are subject to supervision.

The third category is made by jurisdictions which do not set any constraint such as South Africa, Türkiye, and Thailand. Several jurisdictions, including, Armenia, Brazil, India, Korea, Lebanon, the UK and the US currently lack specific rules or are in the process of developing one.

Box 6: Approaches to restrict trading in foreign or unlicensed stablecoins

Stablecoins are currently mainly issued from a limited number of jurisdictions but are widely used globally, including in jurisdictions where there is no domestic issuance. To maintain financial stability, jurisdictions should aim to address potential risks posed by foreign-issued stablecoins by ensuring they meet domestic regulatory requirements before they are approved for trading on domestic CASPs.[55] Coordination between central banks, market regulators, and supervisory authorities is critical to achieving a consistent and effective regulatory approach.

Both the EU and the US provide examples of practices to address foreign or unlicensed stablecoins.

In the EU, MiCAR requires that ARTs and EMTs be issued and offered only by authorised entities domiciled in the EU. CASPs had to cease offering, trading, or facilitating access to non-compliant ARTs and EMTs by the end of 2024 (although enforcement was postponed to Q1 2025). CASPs are also expected to implement communication campaigns to raise investor awareness and facilitate the liquidation or conversion of non-compliant stablecoins into MiCAR-compliant alternatives.

In the US, when the GENIUS Act is fully implemented, [56] it will be unlawful for any person other than a permitted payment stablecoin issuer to issue a payment stablecoin in the US. Beginning three years after the Act's enactment, it shall be unlawful for a digital asset service provider to offer or sell a payment stablecoin to a person in the US unless the payment stablecoin is issued by a permitted payment stablecoin issuer in the US. However, such prohibitions shall not apply to a foreign payment stablecoin issuer that:

1. Is subject to regulation and supervision by a foreign payment stablecoin regulator in a jurisdiction that has a regulatory and supervisory regime with respect to payment stablecoins that the Secretary of the Treasury determines to be comparable to the US regulatory and supervisory regime established by the GENIUS Act;
2. Is registered with the Comptroller of the Currency;
3. Holds reserves in a US financial institution sufficient to meet liquidity demands of US customers, unless otherwise permitted under a reciprocal arrangement established pursuant to other provisions of the GENIUS Act; and
4. Is domiciled and regulated in a foreign country that is not subject to US comprehensive economic sanctions by the US and is not in a jurisdiction that the Secretary of the Treasury has determined to be a jurisdiction of primary money laundering concern.US

55 See section 6,4 in FSB (2024), *Cross-border Regulatory and Supervisory Issues of Global Stablecoin Arrangements in EMDEs*, July.

56 The GENIUS Act, and the amendments made by this Act, take effect on the earlier of (1) the date that is 18 months after the date of enactment of the Act; or (2) the date that is 120 days after the date on which the primary Federal payment stablecoin regulators issue any final regulations implementing the Act.

Furthermore, it shall be unlawful for any digital asset service provider to offer, sell, or otherwise make available in the US a payment stablecoin issued by a foreign payment stablecoin issuer unless the foreign payment stablecoin issuer has the technological capability to comply, and will comply, with the terms of any lawful order and any reciprocal arrangements or other bilateral agreements between the United States and jurisdictions with payment stablecoin regulatory regimes that are comparable to the requirements established under the GENIUS Act.

A foreign payment stablecoin issuer shall be subject to reporting, supervision, and examination requirements as determined by the Comptroller of the Currency and shall consent to US jurisdiction relating to the enforcement of the GENIUS Act.[57]

The EU and US approaches underscore the need for jurisdictions to regulate not only the issuance of stablecoins by domestic entities but also the availability of foreign issued tokens through CASPs and other service providers. Effective regimes should ensure that all stablecoins offered within a jurisdiction are subject to rules designed to protect users and mitigate risks to financial stability.

3.3. Regulatory requirements for stablecoin issuers

Few jurisdictions fully meet all aspects of the GSC recommendations for stablecoin issuers, with gaps observed even in jurisdictions with more developed frameworks in place or in progress (see Table 6). Jurisdictions such as Armenia, the EU, Hong Kong, Japan, and US have made notable progress, proposing or implementing detailed requirements for stablecoin issuers related to governance, stabilisation mechanisms, collateralisation, and custody. However, in Japan for example, gaps remain in areas such as stress testing, contingency funding and continuity plans, recovery and resolution planning and conflicts of interest. Regarding the US, while the Genius Act was signed into law in July 2025, its implementation requires the development of rulemaking by relevant US authorities; before such regulation is issued it is not possible to express any opinion on the comprehensiveness of provisions in the area of capital requirements, risk management, and governance arrangements. While the baseline capital requirement of Hong Kong's regime is not risk sensitive and may not be adequate to absorb losses at all times, the HKMA may impose higher additional financial resource requirements where necessary.

Bermuda's framework is mostly aligned with the GSC recommendations, however redemption at par into fiat is not required for stablecoins that reference a single fiat currency. Other jurisdictions, such as The Bahamas, demonstrate partial alignment, with some weaknesses in areas such as risk management, stabilisation mechanisms and recovery and resolution planning. Singapore and the UK have proposed detailed frameworks but still require legislative changes to finalise and implement their proposed frameworks.

Meanwhile, jurisdictions like Australia, Brazil, Canada, Chile, Korea, Nigeria, Philippines, Korea, Türkiye, Switzerland Uruguay are in the early stages of drafting frameworks, with more detailed elements yet to be proposed.

Significant variation exists in how jurisdictions are implementing the GSC recommendations, particularly in governance, risk management, redemption, and prudential requirements. For example, while the EU and Hong Kong mandate robust governance structures and clear

[57] The Secretary of the Treasury will issue rules as required to carry out the relevant section of the GENIUS Act not later than one year from the date of enactment.

redemption timelines, other jurisdictions like The Bahamas relies on disclosure-based approaches, providing less comprehensive and sound regimes. Risk management requirements also vary widely, with some jurisdictions integrating stress testing and liquidity risk management (such as Bermuda, the EU, and Hong Kong), while others lack explicit measures to address operational and financial risks. Similarly, stabilisation mechanisms and custody practices range from prescriptive frameworks requiring full reserve backing and local custody (e.g., EU and Japan) to more flexible, disclosure-driven models (e.g., The Bahamas). These differences highlight the risk of regulatory fragmentation given the global nature of the stablecoin market and the potential benefits of greater alignment to ensure consistency with the FSB and GSC recommendations.

Jurisdictions also adopt different approaches to applying proportionality in regulatory frameworks for stablecoin issuers. Two primary methods have been identified: (i) bifurcation of regulatory requirements, where systemic and non-systemic issuers are subject to different standards, with more stringent requirements imposed on the former; and (ii) supervisory discretion, where all issuers are subject to baseline obligations, but supervisors may impose additional requirements on systemic issuers based on their regulatory powers.

Under the bifurcation approach, issuers that meet prescribed thresholds would be classified as systemic (or significant, as defined by some regimes) are immediately subject to heightened requirements. For instance, the EU requires significant issuers to maintain a higher capital ratio of 3% (compared to 2% for non-significant issuers), conduct enhanced stress testing, and implement more robust risk management arrangements. The UK also plans to apply differentiated rules based on issuer size, with systemic payment systems using stablecoins subject to oversight by the Bank of England (for prudential purposes), the FCA (for conduct purposes) the Payment Systems Regulator (for competition purposes) and other non-systemic stablecoins subject to oversight by the FCA.

In contrast, jurisdictions such as the Bahamas, Bermuda, Japan, Singapore, and Hong Kong adopt a supervisory discretion-based approach. This method allows authorities to tailor oversight intensity and impose additional requirements on systemic issuers as needed. However, the effectiveness of this approach depends on the availability of sufficient human and technical resources to ensure that supervisory actions adequately address risks.

It is important to note that while a systemic vs. non-systemic distinction is one way to implement proportionality, the FSB's recommendations for global stablecoin arrangements do not mandate for the bifurcation approach. Jurisdictions retain flexibility to apply proportionality through mechanisms suited to their regulatory frameworks and supervisory capacities However, jurisdictions must ensure that their regulatory regime and supervisory approach is adequate to address the risks emanating from global stablecoin arrangements.

Table 6: Selected requirements for stablecoin issuers[58]

Jurisdiction	Risk Management	Stress testing	Contingency plans[59]	Redemption requirements	Stabilisation Mechanisms	Custody of reserves	Prudential Requirements	Recovery and Resolution plans
Armenia	Under Development	Yes	Yes	"timely"	Full reserve backing	Local	Risk based	Required
The Bahamas	Principles based	None	None	Disclosure only	Disclosure only	Offshore allowed	Principles based	Required
Bermuda	Comprehensive	Yes	Yes	Disclosure only	Full reserve backing	Offshore allowed	Risk based	None
EU	Comprehensive	Yes	Yes	"No Delay"	Full Reserve or balance sheet backing	Local required	Risk based + supervisory discretion	Required
Hong Kong	Comprehensive	Yes	None for CFP, Yes for BCP	1-day	Full reserve backing	Local required[60]	Fixed minimum + supervisory discretion	Required
Japan	Comprehensive	Partially required	None	"without delay"	Full Reserve or balance sheet backing	Local required	Fixed minimum	Partially required
Singapore	Partially comprehensive	Under consideration	Under consideration	5-days	Full Reserve or balance sheet backing	Offshore allowed with conditions	Fixed minimum + supervisory discretion	None
UK (proposed)	Comprehensive	Yes	Under consideration	1-day	Full reserve backing	Offshore allowed for non-systemic Local required for GBP-denominated systemic stablecoins	Risk based	Required
US	Under development	None[61]	Under consideration[62]	"timely"	Full reserve backing	Offshore allowed[63]	Risk based, under development	Under consideration[64]

58 The jurisdictions included in this table are those jurisdictions that have either implemented or published a regulatory framework for stablecoins.

59 This includes both contingency funding plans (CFP) and business continuity plans (BCP).

60 Offshore custody may be allowed on a case-by-case basis subject to approval by the HKMA.

61 There are no statutory requirements for stress testing in the GENIUS Act, but ongoing rulemaking may create such a requirement.

62 There are no statutory requirements for business continuity planning in the GENIUS Act, but ongoing rulemaking may create such a requirement.

63 Custodians of reserve assets must be subject to supervision or regulation by a primary US federal payment stablecoin regulator, a state bank supervisor, or a state credit union supervisor. US payment stablecoin issuers must disclose the geographic location of custody for reserve assets in their monthly reports.

64 The GENIUS Act mandates the primary federal payment stablecoin regulators to perform a study of the potential insolvency proceedings of permitted payment stablecoin issuers, including an examination of, among other things, whether additional legislative or regulatory authorities are needed to implement orderly insolvency administration regimes.

3.3.1. Governance requirements

According to GSC Recommendation 4, authorities should require that GSC arrangements have in place and disclose a comprehensive governance framework with clear and direct lines of responsibility and accountability for all functions and activities within the GSC arrangement. In addition, the governance body of the GSC should disclose how governance and accountability is allocated and how potential conflicts of interest are addressed among different entities within the arrangement and in different jurisdictions.

The governance and conflicts-of-interest requirements for stablecoin issuers vary across the jurisdictions with a regime in place, reflecting different levels of regulatory maturity and focus. The EU and Hong Kong provides comprehensive and detailed frameworks and to a large extent also the regime in Bermuda is in line with GSC Recommendation 4. The EU, under MiCAR, mandates a clear organisational structure, well-defined responsibilities, and high ethical standards promoted by the management body. It also requires issuers to identify, prevent, manage, and disclose conflicts of interest, with dedicated officers and policies to ensure impartial decision-making.[65] The approach in Hong Kong also mandates the establishment of a code of conduct providing also provide examples of acceptable and unacceptable behaviour, and should explicitly prohibit any behaviour that could lead to non-compliance by the licensee with its obligations or result in unaddressed conflicts of interest. In Hong Kong issuers are requested that at least one-third of the board members should be independent non-executive directors.

Similarly, Armenia's law emphasises robust internal control systems, alongside explicit internal procedures to address conflicts of interest. However, the disclosure requirements related to governance are not aligned with GSC Recommendation 4.

Singapore, under the forthcoming regime, will require disclosure of governance arrangements, assesses the fitness and propriety of directors and CEOs and set outs guidance on managing conflicts of interest. Japan takes a different approach by restricting stablecoin issuance to specific entities, such as trust companies and banks, which aims to ensure governance through existing regulation, though disclosures and conflict-of-interest policies are not specifically addressed. Regarding the US, the GENIUS Act will require payment stablecoin issuers to disclose related party transactions and mandates that the federal regulators consider, among other factors, the competence, experience and integrity of the officers, directors and principal shareholders of a payment stablecoin issuer, its subsidiaries and its parent company.

Lastly, jurisdictions such as Switzerland and The Bahamas provide more limited governance or conflict-of-interest requirements in their frameworks. Switzerland's governance considerations depend on the issuer's activities, potentially requiring compliance with the Banking Act or payment systems regulations, while The Bahamas relies on broader governance principles and disclosure frameworks.

---

65 In particular, in the EU such arrangements must be documented and disclosed through publicly accessible white papers which include statements from the management body and summaries of governance features. MiCAR also requires the disclosure of conflicts of interest (Article 32), reserve management policies (Article 36), and audit results (Article 30), ensuring transparency and accountability.

Only the EU and Hong Kong appear to have fully implemented GSC Recommendation 4. While several jurisdictions have taken steps to implement governance frameworks for stablecoin issuers, they do not always require issuers to have in place and disclose a comprehensive governance framework that establishes clear and direct lines of responsibility and how potential conflicts of interest are addressed. Full alignment with GSC Recommendation 4 is of critical importance given the central role played by governance arrangements for the sound conduct of business.

3.3.2. Risk management requirements

Jurisdictions demonstrate varying levels of alignment with GSC Recommendation 5, which calls for comprehensive risk management, continuous risk assessments, and robust liquidity risk management for stablecoin arrangements. While some have implemented detailed frameworks addressing operational, financial risks (with a focus on liquidity), others have made progress in certain areas but still face gaps, particularly in contingency planning and operational risk mitigation. A number of jurisdictions remain in the early stages of regulatory development, highlighting the need for further progress to meet global standards for financial stability.

The EU and Hong Kong have established detailed frameworks that address the key elements outlined in FSB Recommendation 5. The EU have robust risk management requirements that includes operational risk (including information technology and cyber risks, financial risks (including credit, market and liquidity) and stress testing. In the EU, issuers must conduct capital stress testing (quarterly for issuers of significant tokens, semi-annual for other issuers) that takes into account severe but plausible financial and non-financial stress scenarios. EU EMT and ART issuers must also conduct liquidity stress testing at least monthly.[66] Hong Kong's regime sets stress testing requirements for assessing reserve asset robustness under severe scenarios. Both in the EU and Hong Kong issuers are required to have in place arrangements to ensure business continuity.

In Bermuda issuers must conduct stress-testing of extreme but plausible events that demonstrate they can absorb large, sudden redemption waves without impairing par convertibility or triggering forced sales of reserve assets. In line with the principle-based approach, the regulation sets that the size of any threshold, soft buffer or management-action trigger should be calibrated to the outcomes of that liquidity stress test rather than being set by rule.

In the US, the GENIUS Act mandates regulators to establish capital, liquidity and risk management requirements for payment stablecoin issuers that are, among other provisions, tailored to the business model and risk profile of the issuer and do not exceed requirements that are sufficient to ensure the ongoing operations of the permitted payment stablecoin issuer. The UK has proposed to adopt a prudential framework that requires stablecoin issuers to conduct internal capital adequacy and risk assessments, including stress testing and wind-down planning. Additional capital and liquidity requirements are tailored to the size and complexity of issuers, ensuring alignment with international standards for financial stability and resilience.

---

66 Banks issuing EMITs are not subject to monthly liquidity stress testing requirements.

Armenia, Singapore, and Japan have implemented or are developing frameworks that address certain aspects of FSB Recommendation 5. Armenia's law includes provisions for stress testing material risks and maintaining recovery plans but does not yet comprehensively address operational risks like fraud or cyber risks. Singapore addresses operational, governance, fraud and technology risks, including cyber risk and safeguarding customer assets, though explicit stress testing and contingency funding requirements remain under consideration. Furthermore, Singapore's regime already requires providers of digital services (a category which includes issuers) to establish a recovery time objective of not more than 4 hours for each critical event. Japan aims to ensure financial stability through strict asset management practices while stress testing requirements are required for trust banks but not for "funds transfer service providers."

Implementation of GSC Recommendation 5 remains incomplete (except in the EU and Hong Kong), with several jurisdictions establishing risk management requirements that address some but not all risks of stablecoin issuers. Risk management frameworks that do not comprehensively address financial and non-financial risks, particularly liquidity risk and contingency funding plans, are not consistent with GSC Recommendation 5.

3.3.3. Redemption

As stated in GSC Recommendation 9, authorities should require that GSC arrangements provide a robust legal claim to all users against the issuer and/or underlying reserve assets and guarantee timely redemption. For GSCs referenced to a single fiat currency, redemption should be at par into fiat.

The regulatory landscape for stablecoin redemption at par value demonstrates two distinct approaches: jurisdictions that explicitly mandate redemption at par value and those that do not. Jurisdictions such as Armenia, The Bahamas, the EU, Hong Kong, Japan, Singapore, the UK, and the US require or propose requiring stablecoin issuers to redeem tokens at a 1:1 ratio with the underlying reference asset or its equivalent. For instance, under the EU's MiCAR, stablecoin holders have a direct claim against the issuer to redeem tokens at par value (for EMTs) or at market value (for ARTs), either in funds or equivalent assets (in the case of ARTs), with no fees except if the recovery plan has been activated. Similarly, the UK expects to mandate that issuers provide redemption at par value, denominated in the same currency as the stablecoin's reference value, with clear rules for systemic and non-systemic issuers. In the view of UK authorities, this is particularly important for systemic stablecoins used as money, as safeguarding trust and confidence in them is crucial for financial stability. In Singapore, under the forthcoming regime issuers must ensure redemption at par value within a stipulated timeframe, as discussed below. The Bahamas also requires 1:1 redemption, ensuring holders can exchange their stablecoins for the underlying fiat currency or equivalent asset. In Japan, the Payment Service Act ensures that redemption occurs at face value, safeguarding user rights.

Conversely, some jurisdictions do not explicitly reference par value in their redemption requirements. For instance, Canada takes a disclosure-based approach, requiring issuers to adequately inform holders of their redemption rights without prescribing specific terms such as par value. Similarly, Bermuda operates under a principles-based regime, where redemption practices are assessed as part of the issuer's overall profile, but no explicit requirement for par value is outlined. These approaches are not consistent with GSC Recommendation 9 that

authorities should require stablecoin issuers to guarantee timely redemption and for those stablecoins referencing a single fiat currency redemption should be at par into fiat.

When it comes to timely redemption, regulatory practices vary widely, with some jurisdictions specifying minimum timeframes and others requiring prompt redemption without defining exact periods. Jurisdictions such as Hong Kong, Singapore and the UK have established or propose clear timelines. In Singapore, issuers are required to process legitimate redemption requests within five business days. The UK is consulting on taking a stricter approach, proposing to mandate that non-systemic issuers process redemption requests by the end of the next business day (T+1) after receiving the request and any necessary customer information under financial crime laws. Meanwhile, it is proposed that systemic stablecoin issuers are required to process redemption requests by the end of the day on which a valid redemption request is made, and in real time wherever possible. In the view of UK authorities, this safeguards trust in systemic stablecoins used as money and therefore financial stability. Hong Kong mandates issuers to honour valid redemption requests within one business day after the day on which it is received by the issuers. These precise timeframes provide clarity and predictability for stablecoin holders, enhancing trust in the system.

On the other hand, several jurisdictions emphasise the need for "timely" redemption without specifying exact periods. For example, the EU requires issuers to honour redemption requests "at all times" without undue delay, though no minimum timeframe is defined. Similarly, Japan mandates that issuers provide redemption "without delay" under the Payment Service Act, ensuring prompt action but leaving room for interpretation. Armenia and The Bahamas also require redemption to occur in a "timely manner," though neither country prescribes a specific timeframe. In the US, the GENIUS Act will require payment stablecoin issuers to establish clear and conspicuous procedures for timely redemption, and regulatory rulemaking may provide a definition of “timely redemption.” Meanwhile, Canada and Bermuda do not currently specify redemption periods, reflecting either a principles-based approach (as in Bermuda) or a disclosure-based framework (as in Canada). In the Philippines, the existing e-money regulation under which stablecoins could be subsumed does not set rules about the timeline for redemption.

Jurisdictions’ approaches to implement the part of GSC recommendation relative to redemption costs also varies, and can be divided into three categories: (i) jurisdictions prohibiting redemption fees in the ordinary course of activity such as Armenia and the EU (fees can be applied under recovery plan), (ii) jurisdictions limiting the maximum amount of fees to incurred costs, such as Hong Kong (fees to be commensurate to operational costs of processing the redemption as well as prevailing industry practices), Singapore and UK (under draft rules), and (iii) countries without any requirement such as the Bermuda (only disclosure obligation), Philippines, and the US (only disclosure obligation). The absence of requirements for requests to be processed without undue redemption costs is evidently not aligned with GSC Recommendation 9.

The varied approaches to redemption could present challenges and exacerbate run risks for stablecoins that are issued in multiple jurisdictions (see box 6 above). Users, particularly institutional holders with better ability to operate across borders, may seek to redeem their stablecoins in a jurisdiction with stricter redemption period requirements to convert their stablecoins into fiat faster. Stablecoin issuers operating in multiple jurisdictions may face challenges to rebalance reserves across borders and meet redemption requests in different jurisdictions.

3.3.4. Stabilisation mechanisms

GSC Recommendation 9 provides two approaches for stablecoin issuers to maintain a stable value at all times: full reserve backing or balance sheet backed where the issuer is subject to adequate prudential requirements, oversight and safeguards equivalent to Basel Committee for Banking Supervision (BCBS) standards and delivers similar levels of protection to commercial bank money. All jurisdictions included in the peer review have frameworks covering fully reserve-backed stablecoins. Jurisdictions such as Armenia, Bermuda, Canada, the EU, Japan, Hong Kong, Singapore, the UK, and the US, mandate or propose mandating that stablecoins be fully backed by high-quality, liquid assets such as cash, government bonds, or other low-risk instruments. The UK has also proposed for systemic stablecoins to be backed, at least in part, by central bank deposits. Some jurisdictions, like the EU and Hong Kong, also impose over-collateralisation requirements or concentration limits to further mitigate risks.

Three jurisdictions, the EU, Japan and Singapore, indicate the possibility for a bank to issue a balance sheet backed stablecoin, without full reserve asset backing. In Singapore, banks may issue stablecoins which are backed by the balance sheet of the issuing bank rather than a specific segregated pool of assets. However, while such balance sheet-backed stablecoins represent a claim on the issuer, they are not necessarily 'deposits'; such balance sheet backed stablecoins will be distinct from stablecoins issued under the MAS's framework for single-currency stablecoins, where full reserve backing is required. In Japan, banks are allowed to issue stablecoins which may not be subject to full reserve backing. However, at this time, it is not permitted due to supervisory concerns. In the EU, banks issuing EMTs do not have to operate a reserve of assets – as it is the case for traditional electronic money – rather they have to meet stablecoins related liabilities with their entire estate. Bank issued EMTs do not represent 'deposits' rather a tokenised liability being legally comparable to electronic money.

In contrast, jurisdictions like The Bahamas and Bermuda adopt principles-based or disclosure-driven frameworks. These jurisdictions do not prescribe specific stabilisation mechanisms but instead focus on transparency and issuer accountability. For instance, The Bahamas requires issuers to disclose their stabilisation mechanisms in offering documents. While these flexible approaches allow issuers to determine their own mechanisms while maintaining supervisory oversight through disclosure and risk management principles, they are not aligned with GSC Recommendation 9 which calls for either full reserve-backed or balance sheet-backed stabilisation mechanisms, as described above. Reliance on a disclosure-based stabilisation regime can result in stablecoin issuers utilising stabilisation mechanisms that are not effective at maintaining a stable value at all times.

3.3.5. Reserve collateralisation requirements

The vast majority of jurisdictions with stablecoin framework require full reserve collateralisation at all times, ensuring that the value of reserve assets matches or exceeds the circulating supply of stablecoins. This foundational requirement is designed to maintain stability and guarantee redemption at par value. For instance, Singapore, Hong Kong, Japan, the US and the UK's proposed framework for systemic and non-systemic stablecoins explicitly require stablecoin issuers to maintain reserves at least equivalent to the nominal value of their issued tokens.

Some jurisdictions go further by requiring over-collateralisation to provide an additional buffer against risks such as market volatility, credit risk, or operational failures. For example, the EU mandates over-collateralisation for all issuers under the MiCAR framework, ensuring that reserve assets exceed the nominal value of the stablecoins in circulation (a specific formula has been introduced to calibrate the minimum overcollateralisation[67]). This additional requirement helps mitigate potential fluctuations in the value of reserve assets. The UK is also considering over-collateralisation for systemic stablecoin issuers, alongside additional capital buffers to cover operational risks and wind-down costs. Hong Kong mandates an issuer to apply an appropriate degree of over-collateralisation to provide sufficient buffer for potential changes in market prices, having regard to the market risk profile of the reserve assets. These measures aim to enhance the stability and resilience of stablecoins that could have a broader impact on financial systems.

In Canada, reserve assets must fully back the value of virtual currency-referenced assets, but their adequacy is only required to be measured at fair value at least once per day. While this ensures daily compliance, it does not mandate continuous collateralisation, leaving potential gaps in real-time reserve adequacy. Similarly, Bermuda, under its principles-based DAB regime, requires reserve assets to back issued stablecoins but does not impose detailed rules for real-time collateralisation or over-collateralisation. The Bahamas takes a disclosure-based approach, requiring issuers to disclose their stabilisation mechanisms in offering documents, but it does not explicitly mandate full collateralisation or over-collateralisation. This reliance on periodic disclosure and principles-based frameworks is not aligned with GSC Recommendation 9 which requires reserves of asset at least equal to outstanding tokens at all times and may not provide the same level of assurance as jurisdictions with continuous collateralisation requirements.

3.3.6. Asset eligibility for reserves

As stated in GSC Recommendation 9, reserve assets should consist only of conservative, high quality and highly liquid assets. Across jurisdictions, there is a broad alignment on the types of assets eligible for stablecoin reserves, emphasising a limited set of high-quality, liquid, and low-risk instruments. Most regulatory frameworks allow bank deposits, government bonds, and in some cases, money market funds (MMFs) or reverse repurchase agreements (reverse repos), provided that underlying assets meet strict criteria for liquidity, credit quality, and maturity.

Bank deposits are widely accepted or plan to be accepted as eligible reserve assets, including in Canada, Hong Kong, Japan, Singapore the UK (only for non-systemic stablecoins[68]), and the US. The EU and Japan are the only jurisdictions that currently impose a minimum amount of deposits as part of the stablecoin issuers' overall reserve. In particular, Japan requires reserve assets to be managed entirely in demand deposits or savings with depository institutions that meet soundness standards. [69] The EU sets out that non-significant and significant stablecoins

---

67 See article 6 of EBA (2024) *Final Report - Draft Regulatory Technical Standards to further specify the liquidity requirements of the reserve of assets under Article 36(4) of Regulation (EU) 2023/1114*, June.

68 For systemic stablecoins, the UK earlier proposal was to only accept central bank deposits. The Bank of England is now considering allowing a proportion of backing assets to be invested in High Quality Liquid Assets.

69 In Japan, stablecoins issued as trust beneficiary rights by trust companies or trust banks currently allow only deposits as part of their reserves. However, once the new amendment to the Payment Services Act enacted in June 2025 comes into effect, such stablecoins will also be permitted to include government bonds maturing within three months as reserve assets, with a cap of 50 percent of total reserve assets.

must hold at least 30% and 60% of their reserves in deposits, respectively.[70] In the US, the GENIUS Act directs the federal payment stablecoin regulators to issue regulation implementing reserve asset diversification requirements, including pertaining to deposit concentration at banking institutions.

Government bonds are another key component of reserve asset frameworks, with many jurisdictions imposing maturity limits to reduce maturity transformation. For example Singapore allows government-issued debt securities with residual maturities of up to three months, and once the GENIUS Act takes effect, the US will limit US government bills, notes and bonds held as stablecoin reserve assets to those with a remaining maturity of 93 days or less or those issued with a maturity of 93 days or less,[71] while the UK is considering permitting treasury debt instruments maturing in one year or less for non-systemic stablecoins. The EU and Japan also allow government bonds without specifying a maturity limit, provided they meet the necessary liquidity and safety standards.[72]

MMFs and reverse repos are permitted reserve assets in some jurisdictions. The US allows and the UK proposes to allow MMFs whose underlying assets are limited to government bonds for non-systemic stablecoins. Canada allows MMFs as reserve assets as long as the MMFs are registered in either Canada or the US. Similarly, the EU permits MMFs indirectly through UCITS-compliant funds that invest exclusively in highly liquid financial instruments. Hong Kong and the US allow, and for non-systemic stablecoins, the UK proposes to allow reverse repos backed by high-quality government or central bank securities, recognising their utility in maintaining short-term liquidity while mitigating counterparty risk.

The practices of the jurisdictions mentioned above regarding the reserves eligibility appear largely in line with the GSC recommendations; however, those jurisdictions missing requirements or adequate arrangements to mitigate concentration risk are not fully in line with Recommendation 9.

Box 7: Risk management of reserve assets

Effective reserve management is essential for stablecoin issuers to ensure stability, meet redemption requests, and maintain user trust. GSC Recommendation 9 calls for particular attention to the nature, sufficiency and degree of risk-taking in terms of duration, credit quality, liquidity and concentration of a GSC's reserve assets. Proper risk management of reserve assets mitigates risks like credit losses, market volatility and liquidity shortfalls, safeguarding financial stability and reducing systemic risks.

To reduce maturity transformation of stablecoin reserve activities, jurisdictions generally take two broad approaches:

i) Set a maximum maturity for each asset in the reserve (e.g., 3 months).

---

70 This obligation is accompanied by concentration limits differentiated by asset size of the deposit-taking bank (1.5% of its total assets) and systemic relevance of the bank; furthermore stablecoin issuers cannot include in the reserve deposits at bank not fulfilling the creditworthiness requirement

71 The GENIUS Act does not limit issuer reserves only to Treasury bills, notes, or bonds. Section 4(a)(1)(A) of the Act identifies types of assets that may be held as reserves.

72 In Japan, in addition to stablecoins issued in the form of trust beneficiary rights by trust companies or trust banks, stablecoins issued by funds transfer service providers are also permitted. There is no maturity limit on government bonds that may be included as reserve assets for stablecoins issued by funds transfer service providers. For the maturity restriction applicable to stablecoins issued in the form of trust beneficiary rights, see footnote 69.

ii) Set an average maturity for the entire reserve portfolio (e.g., at least 20% and 30% of reserve assets maturity of one and five days).

While the US and Singapore will adopt the first approach, the EU has opted for the second approach. Japan does not adopt any of the said two approaches and instead imposes qualitative requirements separately on stablecoins issued as trust beneficiary rights and those issued by funds transfer service providers. Under recent legislative amendments, Japan is introducing a maximum maturity limit of three months on government bonds held as reserve assets issued as trust beneficiary rights.[73]

More broadly, the EU, under MiCAR, has developed a comprehensive approach to managing the risks of reserve assets. Issuers of ARTs and EMTs must ensure reserve assets are held in highly liquid financial instruments with minimal market, credit, and concentration risks. Concentration limits include a 35% cap for government bonds, 10% for covered bonds, and 5% for UCITS, with additional limits on deposits in credit institutions, which cannot exceed 1.5% of the bank's total assets. Reserve assets must be valued daily, and liquidity stress tests are required to ensure resilience under stress scenarios. Issuers must prudently manage reserves to enable rapid liquidation with minimal price impact, bearing any profits or losses from reserve investments. They are also required to implement robust risk management frameworks, conduct creditworthiness assessments of counterparties, and comply with regular audits and transparent reporting. This framework ensures the stability, liquidity, and security of reserve assets, protecting token holders and in turn mitigating run risks.

3.3.7. Custody of reserve assets

GSC Recommendation 9 notes that authorities should require reserve-based stablecoin arrangements to ensure safe custody and proper record-keeping of reserve assets and that ownership rights of reserve assets are protected at all times, including through segregation requirements from other assets of the GSC, members of its group and the custodian's assets.

Most jurisdictions adopt a similar approach for the custody of stablecoin reserve assets, focusing on segregation, bankruptcy-remoteness, and the use of qualified custodians. A key requirement across jurisdictions is that reserve assets must be segregated from the issuer's own assets and protected from claims by the issuer's creditors in the event of insolvency. For example, Armenia, the EU, Hong Kong, Singapore, the US and the UK all require or propose to require reserve assets to be either legally or operationally ring-fenced from the issuer's estate. This is often achieved through statutory trusts or contractual safeguards, as seen in Hong Kong, which mandates trust arrangements supported by independent legal opinions, and the UK, which proposes statutory trusts for reserve assets held for systemic payment systems using stablecoins under the Bank of England's proposed regime. The EU requires reserve assets to be operationally segregated with licensed custodians.

Another commonality is the requirement to use qualified custodians, such as banks, investment firms, or other licensed custodial entities. In Canada, custodians must meet the qualifications defined in its securities regulations, while the EU in addition mandates issuers to conduct due diligence on custodians to ensure they have the necessary expertise, reputation, and internal controls to safeguard assets. These measures ensure that custodians are capable of protecting reserve assets effectively and diligently.

[73] See footnote 69.

Despite these common approaches, there are notable variations in implementation, particularly regarding the requirement for onshore custody versus the allowance for offshore arrangements. Such variations may result in challenges for global stablecoin issuers to meet different custodial requirements in multiple jurisdictions, which could result in cross-border frictions or impair the movement of liquidity. Some jurisdictions, such as Hong Kong, Armenia, Nigeria, and the EU, mandate local custody to enhance regulatory oversight and user protection. Hong Kong requires reserve assets to be placed with licensed banks in Hong Kong, although it may consider offshore arrangements on a case-by-case basis if risks are adequately addressed and user interests are safeguarded. Similarly, Armenia mandates that funds and securities be held onshore with local banks or authorised entities, while Nigeria explicitly requires reserves to be maintained domestically. The EU, under MiCAR, requires that reserve assets for EMTs and ARTs be held with custodians licensed within the EU, such as credit institutions (for all assets), investment firms (for securities), or CASPs (exclusively for ARTs holding crypto-assets) authorised under EU law. This ensures that custodial services are subject to uniform oversight across the EU. The UK, while not explicitly mandating onshore custody for non-systemic stablecoins, proposes statutory trust arrangements to safeguard reserve assets, ensuring they are protected regardless of location. The UK's proposed framework allows flexibility for offshore custody for non-systemic stablecoins but requires issuers to appoint independent third-party custodians and maintain robust safeguarding measures, including segregation and reconciliation, to protect stablecoin holders in the event of issuer insolvency. Meanwhile for sterling-denominated systemic stablecoins, the UK proposes to require that issuers should be set up in the UK in order to carry out business and issuance activities into the UK and with UK-based consumers, both directly and through intermediaries. The backing assets and the issuer's capital would also need to be held in the UK.

In contrast, jurisdictions like Singapore, Canada, and Bermuda permit offshore custody under specific conditions. For instance, Singapore allows overseas custodians provided they meet credit rating thresholds and maintain a branch regulated by MAS, while Canada permits both domestic and foreign custodians as long as they meet the qualifications defined in its securities regulations. Bermuda, though not explicitly requiring onshore custody, imposes contractual safeguards to ensure access to information and may request legal opinions on cross-border bankruptcy implications.

Jurisdictions also have varying approaches to self-custody of reserve assets by the stablecoin issuer. Japan and Singapore prohibit this explicitly through requirements placed on either issuers or custodians, while the Bahamas explicitly allows self-custody. Others, such as the EU, do not expressly allow or disallow self-custody, but impose stringent governance requirements on custodians, including obligations to adequately manage conflicts of interest. While a prohibition on self-custody is one way that governance risks like conflicts of interest are being managed, robust requirements and supervision are potential ways that risks can be mitigated as well. On the contrary, allowing stablecoin issuers to self-custody reserve assets, without adequate mitigations would pose material risks, and would not be compliant with FSB recommendation 9.

Another area of variation is the degree of bankruptcy-remoteness required. Some jurisdictions, such as the EU, Hong Kong, and the UK, explicitly mandate legal protections to shield reserve assets from creditor claims. In the EU, custodial arrangements must ensure that reserve assets are not encumbered or pledged and are protected against claims even in the event of custodian insolvency. In Hong Kong, effective trust arrangements should be put in place to ensure that the

reserve assets are segregated, held for and on behalf of stablecoin holders, and are available to satisfy stablecoin holders' valid redemption requests at par value. Similarly, the UK proposes statutory trust arrangements to safeguard assets for the benefit of stablecoin holders. In contrast, Bermuda takes a principles-based approach, requiring issuers to demonstrate prudence in asset protection but without prescribing explicit legal mechanisms for bankruptcy-remoteness. Brazil expects to impose operational segregation requirements but may not mandate full bankruptcy-remoteness due to legal limitations.

3.3.8. Prudential and recovery and resolution requirements

As stated in GSC Recommendation 9, GSC arrangements should also be subject to appropriate prudential requirements (including capital and liquidity requirements) to provide that losses can be absorbed and there is sufficient liquidity to deal with outflows. In addition, according to GSC Recommendation 7, authorities should require that GSC arrangements have appropriate recovery and resolution plans.

Prudential Capital Requirements

Capital requirements for stablecoin issuers vary across jurisdictions, with approaches generally falling into two categories: fixed minimums (some with supervisory discretion to increase them) and statutory risk-based requirements. Some jurisdictions, such as Hong Kong, Japan and Singapore adopt fixed minimum capital thresholds. For example, Japan requires at least JPY 100 million for trust companies and JPY 2 billion for trust banks. Similarly, Singapore expects to set a baseline of SGD 1 million or 50% of annual operating expenses, whichever is higher. In Hong Kong, a minimum paid-up share capital of HKD 25 million is mandated, However, in Hong Kong and Singapore, supervisors may impose additional requirements where necessary.[74] This first approach is not fully aligned with GSC Recommendation 9, which recommends capital buffers be consistent with the size of the GSC in circulation and proportionate to the risks of the GSC arrangement. While supervisory discretion to mandate higher capital requirements is an important tool, its effectiveness in ensuring that capital buffers are consistent with the size of a GSC in circulation is called into question if the GSC exhibits rapid growth.

Other jurisdictions, including EU, the UK and Armenia, implement, or are proposing to implement, proportionate, risk-based requirements that scale with the issuer's risk profile or business size. In the EU, non-significant issuers must meet the highest of EUR 350,000, 2% of reserve assets, or a quarter of the prior year's fixed overheads, while significant issuers face a 3% reserve-based requirement. [75] Authorities may impose additional capital buffers based on risk factors such as reserve asset quality or market volatility. In particular, in the EU, the legislation also confers the power to authorities to top-up minimum capital requirement upon certain conditions. MiCAR sets the following conditions for supervisors to increase an EMT's capital requirements based on the results of analysis of effectiveness of risk management and risk factors or based on the results of the stress test.

---

74 For example, in Singapore, solvency requirements are independently verified to ensure sufficient resources for recovery or orderly wind-down.

75 In the EU banks issuing ART and EMT are bound to apply the prudential requirements specific for them which entails compliance with higher capital requirement than that under MiCAR.

Similarly, for non-systemic stablecoins, the UK is proposing to tie capital requirements to the higher of three measures: a fixed amount based on issuance activity, an expenditure-based requirement, or a requirement linked to the amount of stablecoins in circulation. For systemic stablecoin issuers, the UK is proposing that they must hold capital in an amount at least equal to the highest of any of the following: (a) six months of operating expenses; (b) potential business losses; or (c) wind-down costs. In addition, systemic stablecoin issuers would be expected to hold capital to mitigate the risk that a shortfall in backing assets could result in a loss of confidence, including any operational risks, and the costs of distributing assets to coinholders. The proposed calibration would seek to avoid duplication amongst the risks captured.

Further differences are noted with respect to the prudential requirements applicable to banks issuing stablecoins. Divergences in stablecoin issuers' capital requirements, including differences in the treatment of banks' stablecoin activities, contribute to regulatory fragmentation (which could lead to regulatory arbitrage[76]) and may limit the ability to counter threats to financial stability. While Bermuda, the EU, Hong Kong, and Switzerland[77] require banks to comply with banking prudential requirements also for the stablecoin issuance activity, Singapore[78] applies separate requirements for banks' reserve-based stablecoin issuance and bank balance-sheet backed stablecoins - only the latter is subject to consolidated banking capital requirements. In the US, under the GENIUS Act, permitted payment stablecoin issuers will be required to meet regulatory capital requirements, but bank groups will not be required to hold additional consolidated leverage or risk-based capital for a stablecoin subsidiary.

Prudential liquidity requirements

Approaches to prudential liquidity requirements for stablecoin issuers vary across jurisdictions, with three primary categories emerging: comprehensive liquidity requirements, principles-based or less comprehensive approaches, and emerging frameworks. Jurisdictions such as the EU and Hong Kong have established detailed frameworks for liquidity management. The EU mandates regular liquidity stress testing, with monthly requirements for significant issuers, alongside strict standards for reserve asset liquidity. Hong Kong mandates regular stress tests, and requires issuers to put in place liquidity risk indicators for monitoring the reserve assets' liquidity profile, and to set and enforce internal limits and targets for such indicators.

Other jurisdictions, such as Bermuda and Japan, adopt principles-based or less comprehensive approaches. Bermuda currently applies principles-based liquidity requirements tailored to the size, complexity, and risk profile of issuers, with plans to formalise these rules in the future. Singapore's framework prescribes minimum prudential liquidity requirements but lacks requirements for liquidity stress-testing and proportionate add-ons. In Japan, trust companies and trust banks are required to manage the full amount of trust assets in safe deposits to ensure

---

76 For example, banks could find it convenient to operate their stablecoin issuance from jurisdictions that do not apply banking capital requirements as they would in their home jurisdiction.

77 Although there is no case of banks issuing stablecoins in Switzerland.

78 Singapore adopts a hybrid approach whereby banks are subject to traditional capital/liquidity requirements only for balance sheet backed stablecoins. That said, there are currently no banks issuing reserve-backed stablecoins. Furthermore, under the forthcoming MAS' Single-Currency Stablecoins regime (MAS-SCS Framework.) issuers of MAS-SCS stablecoins should only conduct this business, and no other business lines.

liquidity. However, Japan's stablecoin framework does not establish prudential liquidity requirements in addition to the stabilisation mechanism, as stated by GSC Recommendation 9.

Meanwhile, jurisdictions such as The Bahamas and Armenia are in the process of developing liquidity requirements. The Bahamas has announced plans to prescribe minimum regulatory liquidity requirements, while Armenia's draft law empowers the Central Bank of Armenia (CBA) to establish liquidity ratios and mandate stress testing for liquidity risks. In the US, the GENIUS Act requires the US federal agencies to develop liquidity standards. These varying approaches reflect a spectrum of regulatory maturity, from well-defined frameworks – aimed at ensuring the stability and resilience of stablecoin activities – to still developing frameworks whose adequacy cannot be assessed at this time.

Recovery and resolution planning

Approaches to ensure stablecoin issuers have appropriate planning to support a recovery, resolution, or wind-down procedures (including insolvency frameworks) for stablecoin issuers vary significantly across jurisdictions, reflecting differing levels of regulatory focus on operational continuity and risk mitigation. Comprehensive frameworks are seen in Armenia, The Bahamas, the EU, Singapore, and Hong Kong, where issuers are (or will be in the case of Singapore) required to prepare detailed recovery or wind-down plans for crisis management. The EU mandates that issuers maintain recovery plans outlining measures to ensure timely restoration of compliance with reserve requirements and service continuity during disruptions. Issuers must also prepare redemption plans to support the orderly redemption of tokens in cases of financial distress or insolvency. The EU's MiCAR explicitly mandates that any measures adopted under recovery and redemption plans do not endanger financial stability. Similarly, Armenia requires stablecoin issuers to develop recovery plans to address non-compliance with reserve requirements and ensure service continuity, including measures such as liquidity fees, redemption limits, and suspension of redemptions. Singapore will mandate that issuers hold sufficient liquid assets to support recovery or orderly wind-down and requires independent verification of the amounts needed. In the Bahamas, stablecoin issuers are required to prepare a plan with procedures for their recovery and wind down, including the steps it will take to cease operations and procedures to ensure that reserve assets shall at all times be separate and insulated from the issuer's estate. In Hong Kong, licensees must have systems in place to ensure a timely recovery from significant operational disruptions and an orderly wind-down of stablecoin activities if necessary.

In the US, while the GENIUS Act does not mandate plans for the payment stablecoin issuers' recovery, resolution or insolvency, the Act establishes a rule that the claims of holders of payment stablecoins to reserves backing those stablecoins have priority over all other claims in bankruptcy proceedings. The Act also mandates the primary federal payment stablecoin regulators to perform a study of the potential insolvency proceedings of permitted payment stablecoin issuers, including an examination of, among other things, whether additional legislative or regulatory authorities are needed to implement orderly insolvency administration regimes. In addition, insolvency plans may be required under ongoing rulemaking by US authorities.

In contrast, some jurisdictions, such as Bermuda, Chile, and Japan, do not currently include provisions that require stablecoin issuers to develop plans for recovery, resolution, or wind-down

procedures. Bermuda's principles-based regime does not explicitly address recovery or wind-down procedures, but BMA's proposed amendments to the Digital Asset Business Act would grant BMA the powers to require stablecoin issuers (and other DABs) to prepare and maintain a wind-down plan. The absence of recovery and resolution plans for stablecoin issuers is not aligned with GSC Recommendation 7, which recommends that authorities require GSC arrangements to have such plans.

These differences highlight a spectrum of regulatory approaches, ranging from jurisdictions with robust recovery and resolution frameworks to those still in the process of developing or considering such measures. This divergence underscores the different level of maturity of the regulatory process at the jurisdictional level but also highlights that risks to financial stability may be amplified in jurisdictions without recovery and resolution arrangements. In particular, the absence of adequate crisis management tools could result in the spillover of shocks from stablecoin arrangements to the traditional financial sector.

3.4. Examinations and inspections

GSC recommendations 1 and 2 recommend authorities have the powers, tools and resources to apply comprehensive supervisory requirements to GSC arrangements on a functional basis and proportionate to their risks. Supervisory requirements, such as examination, inspections, and the ability to require correction actives, are critical tools to ensure stablecoin issuers are managed in a safe and sound manner.

Supervisory frameworks for stablecoins remain at an early stage and reflect differing priorities and levels of implementation. Jurisdictions can be grouped into three categories: those with comprehensive supervision, those focused on non-financial stability risks (e.g. AML/market integrity), and those where frameworks are still under development. While some jurisdictions have implemented broad oversight frameworks, most supervisory exams to date have limited focus on financial stability risks, such as liquidity and reserve adequacy. Instead, authorities have prioritised addressing financial crime risks, operational soundness, and governance. This reflects current concerns but also highlights the need for further progress to fully address the liquidity risk of stablecoin issuers which appear the most relevant driver for financial instability.

In the EU, the supervisory regime for stablecoin issuers is differentiated for significant and non-significant issuers. Significant issuers are subject to EU level supervision conducted by the European Banking Authority (EBA) and supported by colleges of relevant EU national supervisors; non-significant issuers remain under the responsibility of national supervisors. Since issuers of stablecoins are usually at the centre of a network of entities that ensure the issuance, transfer and distribution of such crypto-assets, the members of the college of supervisors for each issuer must therefore include, amongst others, the competent authorities of the most relevant trading platforms for crypto-assets, in cases where the significant stablecoins are admitted to trading, and the competent authorities of the most relevant entities and CASPs ensuring the custody and administration of the significant stablecoins on behalf of holders.

At the moment there is no significant issuer in the EU and therefore the EBA does not conduct any direct supervision. However, the EBA has been working to foster convergence of supervisory practices among national competent authorities with respect to non-significant issuers.

Bermuda has established a comprehensive supervisory framework for stablecoins. The BMA supervises stablecoin issuers with a focus on financial stability risks, including credit, market, liquidity, operational, and systemic risks. Stablecoin issuers are required to provide annual audited financial statements and risk assessments, ensuring transparency and accountability. The BMA conducts on-site reviews based on risk ratings, thematic studies, and off-site monitoring.

3.5. GSC implementation progress: overall findings

The examination of the implementation progress of regulatory frameworks for global stablecoins reveals a fragmented and uneven landscape. While some jurisdictions have made notable advancements, the overall pace of implementation is slow, and significant gaps remain in aligning with the GSC recommendations. Regulatory approaches are increasingly moving away from applying existing securities or payment frameworks to stablecoins, acknowledging their limitations, and instead converging toward treating stablecoins as a new type of payment instrument through tailored rules that address their unique risks and business models.

While several jurisdictions have a regulatory framework in place or near finalisation, few jurisdictions are fully aligned with the GSC recommendations. The EU and Hong Kong have regulatory frameworks aligned with each GSC recommendation, while the frameworks in Armenia, Bermuda, and Japan require further work to reach full alignment. Critical gaps include insufficient requirements for robust risk management practices, such as stress testing and contingency funding and business continuity plans, capital requirements (in particular that are sensitive to the GSC's size and risk profile), stabilisation mechanisms, as well as gaps in recovery and resolution planning (which are critical to ensuring operational continuity in times of distress). In the US, implementation of the framework required under the GENIUS Act remains ongoing.

Stablecoin arrangements that operate across multiple jurisdictions pose particular regulatory and supervisory challenges. Differences in redemption and custody requirements, the timing and details of disclosures, as well as reserve collateralisation frameworks presents higher liquidity and operational risks for stablecoins that are fungible across borders. Furthermore, authorities would be very likely to benefit from cross-border cooperation and information sharing to comprehensively oversee the activities of these stablecoins arrangements

The limited number of licenses and authorisations granted, despite the growing size of and new entrants into the stablecoin market, underscores a lag between regulatory implementation and market developments and benefits the dominant position of incumbents operating from jurisdictions that have not fully implemented the GSC recommendations. This fragmented approach not only creates risks of regulatory arbitrage but also undermines the stability and potential benefits of stablecoins as a viable financial product. Achieving alignment with the GSC recommendations is critical to safeguarding financial stability and fostering trust in this rapidly evolving market.

4. Implementation progress of data, disclosure, and regulatory reporting requirements

The FSB Crypto Framework includes several recommendations for authorities to collect, and for CASPs and issuers to report data and information relevant to financial stability. These include CA recommendations 6 (data management), 7 (disclosures), and 8 (monitoring interconnectedness), and GSC recommendations 6 (data storage and access) and 8 (disclosures).

Significant gaps and challenges persist for authorities to obtain the data necessary to effectively monitor financial stability risks associated with crypto-asset markets and activities. Regulatory data sources remain limited, prompting authorities to rely heavily on commercial data providers, surveys, and other incomplete or fragmented data sources. These approaches often present challenges related to accuracy, consistency, and comprehensiveness, further complicating efforts to assess and address risks in this rapidly evolving sector.

The implementation of data and reporting requirements for CASPs and stablecoin issuers lags significantly behind other elements of crypto-asset regulatory frameworks. While many jurisdictions have established licensing and authorisation frameworks and begun granting licenses, these efforts are not accompanied by comprehensive reporting requirements. This gap exacerbates data deficiencies, limiting authorities' ability to monitor risks and assess the activities of licensed CASPs effectively. Comprehensive data and reporting frameworks are essential to closing data gaps, enhancing transparency, and enabling effective regulatory oversight.

4.1. CASP reporting frameworks

CA Recommendation 6 calls on authorities to ensure CASPs have robust systems and processes in place to collect, record and report data. Reporting should be proportionate to the risk, size, complexity, and systemic importance of CASPs, and supervisory authorities should be able to access the data as necessary and appropriate to fulfil their regulatory, supervisory and oversight mandates. Reporting should extend beyond AML/CFT and consumer protection, offering data that enables authorities to monitor and address financial stability risks effectively.

Jurisdictions have generally taken a slower approach to implement regulatory reporting requirements for CASPs than they have in introducing other aspects of their regulatory frameworks. This is concerning where jurisdictions have begun licensing CASPs but are not yet receiving relevant data to monitor their risks and compliance with relevant regulations. While 19 jurisdictions have finalised a comprehensive regulatory framework for CASPs,[79] only 11 jurisdictions have comprehensive reporting requirements in place to ensure authorities can effectively monitor the financial stability implications of CASP activities.[80] A further five jurisdictions[81] have some financial stability-related reporting requirements in place while 13

[79] This includes the 11 jurisdictions identified in “Stage 5” implementation of the CA recommendations in Table 1 and the 8 EU national authorities included in this peer review (Germany, France, Hungary, Ireland, Italy, Netherlands, Poland, and Spain).

[80] These are Bermuda, Canada, Chile, Hong Kong, Hungary, Indonesia, Japan, Philippines, Singapore, Thailand, and Türkiye.

[81] These are Argentina, The Bahamas, Korea, Nigeria, and Switzerland.

jurisdictions[82] do not have regulatory reporting requirements from a financial stability perspective in place, or they are under development.

Monitoring the financial stability implications of CASP activities requires CASPs to submit relevant data and reports to their supervisor. Jurisdictions that have implemented more comprehensive regulatory reporting frameworks require CASPs to submit data on their financial condition, financial and non-financial risks, compliance with prudential and other regulations, as well as incident related information (see Table 7 below).

Bermuda, the Philippines, and Thailand have implemented reporting requirements with standardised templates, disclosure obligations, and mechanisms to request data ad hoc from CASPs or third parties. Similarly, Japan, Singapore and Hungary have comprehensive reporting requirements, though non-financial risks are collected on an ad hoc basis. Japan is also able to request data ad hoc from CASPs and third parties.

Table 7: Contents and frequency of CASP reporting requirements, by jurisdiction

Jurisdiction[83]	Assessment category[84]	Financial statements and condition	Financial risks	Non-financial risks	Regulatory compliance	Other reporting
Argentina	Some reporting	Annual	None	Monthly & Annual	None	None
Armenia	Under development	Under development	Under development	Under development	Under development	Under development
Australia	None required	None	None	None	None	None
The Bahamas	Some reporting	Annual	Upon material changes	None	Annual	Annual
Bermuda	Comprehensive	Annual	Annual	Annual	Annual	Annual
Brazil	None required	Under development	Under development	Under development	Under development	Under development
Canada	Comprehensive	Quarterly, Annual	None	Quarterly, Ad hoc	Quarterly, Annual	Monthly, Quarterly, Annual
Chile	Comprehensive	Quarterly	Monthly	Triggered by events, Semi-annually, Monthly	Annually / Monthly	Monthly, Quarterly

82 These are Armenia, Australia, Brazil, France, Germany, Ireland, Italy, Netherlands, Poland, South Africa, Spain, UK and Uruguay.

83 Jurisdictions in group 1 of Table 1 are not included here as they do not have or have not proposed a regulatory framework for CASPs.

84 The categories are comprehensive reporting framework; some reporting in place; none required and requirements under development.

Jurisdiction[83]	Assessment category[84]	Financial statements and condition	Financial risks	Non-financial risks	Regulatory compliance	Other reporting
France[85]	None required	None	None	None	As necessary	None
Germany[86]	Under development	Under development	Under development	Under development	Under development	Annual
Hong Kong	Comprehensive	Monthly	None	Ad-hoc	Monthly / Annual	Annual
Hungary	Comprehensive	Annual	Upon request	Ad-hoc	Upon request	
Indonesia	Comprehensive	Monthly & Annual	Quarterly	Quarterly	None	Supervisory rules
Ireland	None required	None	None	None	None	None
Italy	None required	None	None	None	As necessary	Quarterly
Japan	Comprehensive	Quarterly	Monthly	Ad-hoc	Quarterly	Ad-hoc
Korea	Some reporting	None	None	None	None	Quarterly / Ad hoc
Netherlands	None required	None	None	None	None	Supervisory rules
Nigeria	Some reporting	Under development	Under development	Under development	Under development	Weekly
Philippines	Comprehensive	Annual	Annual	None	Annual	Supervisory rules
Poland	None required	None	None	None	None	None
Singapore	Comprehensive	Annual	Monthly & Semi-annual	Ad-hoc	Annual	None
Spain	None required	None	None	None	None	None
South Africa	None required	None	None	None	None	None
Switzerland[87]	Some reporting	Annual	Annual	Annual	Annual	Quarterly

85 France notes that reports are required for IT incidents.

86 Germany notes that while certain reporting requirements under national law are already applicable, the delegated act defining the full scope of regulatory reporting is still under development.

87 Switzerland has a partial framework in place and therefore does not require reports of all CASPs that might be operating in the jurisdiction. However, where they fall under existing regulation, they are subject to reporting requirements.

Jurisdiction[83]	Assessment category[84]	Financial statements and condition	Financial risks	Non-financial risks	Regulatory compliance	Other reporting
Thailand	Comprehensive	Annual	Daily or Monthly	Annual	Daily or Monthly	None
Türkiye	Comprehensive	Annual	Weekly	Annual	Weekly	Quarterly
UK	Under development	Under development	Under development	Under development	Under development	Under development
Uruguay	Under development	Under development	Under development	Under development	Under development	Under development

The frequency of reporting varies significantly across jurisdictions. For example, Bermuda collects financial statements, financial risk reports, non-financial risk reports, and compliance reports annually.[88] The Philippines follows a similar annual schedule but collects non-financial risk reports only on an ad hoc or event driven basis. Thailand requires annual submissions of financial and compliance reports but does not request non-financial risk reports. Türkiye mandates annual reporting for financial statements and non-financial risks, while financial risk and compliance reports are submitted weekly. Hong Kong requires regular submissions of independent attestation and audit of its reserve assets and annual submissions of financial statements, with non-financial risks collected on an ad hoc basis. Despite these variations, jurisdictions like Bermuda and Türkiye stand out for their frequent and standardised reporting frameworks.

Box 8: Good practices for regulatory reporting

FSB CA Recommendation 6 sets out the importance of authorities having access to full, timely, and ongoing access to relevant data wherever it is located. Bermuda combines both mandatory and voluntary reporting for CASPs and relevant third parties to get a comprehensive understanding of activities and emerging risks. CASPs are expected to submit annual reports through a standardised template, in line with expectations on wider financial services firms conducting similar activities. Authorities in Bermuda can also request data from firms providing services to CASPs, as well as incumbent financial sector institutions that are conducting crypto asset activities. Through onsite inspections, authorities cross verify the accuracy of the data that has been provided and can also share information with other relevant domestic authorities and have taken steps to share and request data from foreign authorities.

Thailand has many similar requirements, although for certain reports, like financial risks, there is an expectation that reports are submitted more frequently, and potentially daily depending on the nature of the risk. Likewise, the Philippines can request data on non-financial risks on an ad-hoc basis while also having the powers to request data from CASPs and relevant third parties. Much like Bermuda and Japan, the Philippines requires common templates across financial risk reporting, non-financial risk reporting, compliance reporting, and the submission of financial statements. However, unlike Bermuda and Japan, which has different requirements for different licenses classes that CASPs might hold, the Philippines has the same reporting requirements regardless of the class of license, although this is in line with their expectations of firms in wider financial markets. These three jurisdictions are also the only ones that set out their powers to verify data provided by third parties as well as CASPs.

88 Entities participating in BMA's regulatory sandbox are subject to different reporting frequencies, with submissions typically required on a monthly basis.

Seven jurisdictions (Argentina, The Bahamas, Kazakhstan, Korea, Netherlands, Nigeria, and Switzerland) have implemented some requirements for data collection and regulatory reporting, though these frameworks are less extensive and often omit critical elements for financial stability. Switzerland has reporting requirements for traditional financial institutions, such as banks and securities firms engaged in crypto asset activities, but these requirements do not extend to all CASPs operating outside existing regulatory frameworks. Argentina has reporting obligations for CASPs but lacks standardised templates, the authority to request data from third parties, or mechanisms to verify submitted data. Similarly, the Netherlands, France, Spain, and Italy mandate incident reporting from CASPs but do not require submissions of financial statements or financial risk reports. Canada collects various reports either annually, quarterly, or ad hoc, but does not include financial risk reporting in its framework.[89] Indonesia collects financial statements monthly but does not require regulatory compliance reports or financial risk reporting. Nigeria highlighted the use of automated API connections with CASPs for reporting, while The Bahamas, Korea, and the Netherlands rely on supervisory meetings or onsite inspections to verify reporting accuracy. These jurisdictions exhibit a more limited scope of reporting, focusing on selected aspects of CASP activities rather than a comprehensive approach.

The frequency of reporting in these jurisdictions is generally less structured and varies depending on the regulatory framework in place. For example, Switzerland's reporting requirements align with traditional financial institutions and are not specific to CASPs, resulting in inconsistent reporting coverage. Argentina does not have standardised reporting intervals, and its framework lacks the capacity to request data ad hoc. Canada collects reports at varying intervals – annually, quarterly, or ad-hoc – depending on the type of report, while Indonesia collects financial statements monthly but does not mandate other critical reports. Nigeria uses automated API connections to facilitate ongoing reporting, though the frequency of data submissions was not detailed. The Bahamas and Korea conduct reporting accuracy checks primarily through supervisory meetings or inspections, suggesting a more reactive approach to data collection. Overall, the reporting schedules in these jurisdictions lack the consistency and granularity seen in jurisdictions with more comprehensive frameworks.

Thirteen jurisdictions (Armenia, Australia, Brazil, France, Germany, Ireland, Italy, Netherlands, Poland, South Africa, Spain, UK[90] and Uruguay) lack regulatory reporting requirements for CASPs from a financial stability perspective. In the EU, where several of these jurisdictions are located, CASPs are required to report to their NCA all necessary information to assess compliance with governance requirements including changes in the management body or shareholders with qualified holdings, ICT-related incidents, including cyber threats and disruptions, suspicious transactions or orders (to counter market abuse). However, the implementation of all other reporting obligations, including financial condition and risks, is delegated to NCAs, and progress varies significantly across EU member states. Notably, France and the Netherlands do not have comprehensive CASP reporting requirements relevant for financial stability despite these jurisdictions authorising 18 CASPs. These jurisdictions are not aligned with CA Recommendation

89 While Canada does not have a separate reporting system specifically for financial risks, its financial reporting does include the amount of excess working capital, and firms are required to immediately notify regulators if the capital falls below a certain proportional threshold.

90 CASPs that are designated as systemic would fall under the remit of the Bank of England and its powers to impose requirements and enforce against them. CASPs would be expected to provide regulatory reporting to the Bank under its safeguarding regime. No systemic CASPs have been identified in the UK.

6 and highlight a significant gap in financial stability monitoring, with little to no data collection or monitoring of CASP activities to address financial stability risks. Finally, China, and Saudi Arabia have imposed a prohibition on crypto-asset activities.

4.2. Stablecoin reporting frameworks

The GSC recommendations on data, reporting, and disclosures prioritise accurate and timely reporting to authorities, aiming to ensure they have full access to relevant data, including on-chain and off-chain information, to fulfil their regulatory, supervisory, and oversight mandates. GSC issuers should make disclosures to users and stakeholders that provide transparent information on key aspects such as governance structures, redemption rights and processes, and the composition and value of reserve assets, supported by regular independent audits.

Stablecoin reporting and disclosure practices vary significantly across jurisdictions, reflecting differing regulatory priorities and levels of maturity (see Table 8). Public disclosures often focus on reserve asset transparency, governance structures, and redemption rights. The Bahamas, Bermuda, Canada, the EU, Hong Kong, Singapore, and the US require, or will require, regular public updates on reserve assets, with frequencies ranging from monthly attestations to annual financial reports. In contrast, Japan and the Philippines either lack clear requirements for public reserve disclosures or do not specify the frequency of such updates. Differences in the extent and frequency of reserve asset disclosures, especially for the same stablecoin issued from multiple jurisdictions, could lead to financial stability risks if stablecoin holders lack sufficient information to determine the financial soundness of the issuer during periods of stress. Beyond reserves, public disclosures in certain jurisdictions (the EU, Hong Kong, Singapore, the UK and the US) extend, or will extend, to governance structures, risks, and redemption policies, often requiring detailed white papers.

Table 8: Disclosure and supervisory reporting requirements for stablecoin issuers

Jurisdiction[91]	Public Disclosure Requirements	Supervisory Reporting Requirements
Armenia	Public disclosure requirements will be introduced in 2026.	Internal reporting requirements under development; details not yet specified.
Australia	There are no specific disclosure requirements for stablecoin issuers.	There are no specific supervisory reporting requirements for stablecoin issuers.
The Bahamas	Offering memorandum must include reserve asset details and be updated promptly.	Quarterly proof of reserves with independent audits submitted to the regulator.
Bermuda	Public disclosures required under Stablecoin Guidance, including monthly reserve asset attestations, custodial arrangements, and overview of risks.	For sandbox entities, monthly reporting of key indicators tailored to the risks of the issuer's business.

[91] Jurisdictions included in this table are those in implementation stages 2, 4 and 5.

Jurisdiction[91]	Public Disclosure Requirements	Supervisory Reporting Requirements
Canada	Redemption policies, fees, rights of stablecoin holders, monthly reserve attestations, annual audited financial statements, and significant events disclosed publicly.	Existing securities law reporting requirements as applicable.
EU (MiCAR)	Monthly updates on reserve size, composition, and value; summaries of audit reports; significant events disclosed.	Quarterly reports on reserve size, composition, token circulation, and systemic use to supervisors.
Hong Kong	Reserve composition and redemption rights must be disclosed; white papers required.	Governance details, reserve updates, and breach of internal credit, liquidity and market risk indicators submitted to the supervisor.
Japan	Governance attributes and redemption rights are disclosed but reserve asset composition is not specified.	Reserve asset composition is reported to FSA.
Singapore	Monthly attestation of reserve compliance and white papers detailing governance, risks, and redemption rights.	Monthly and annual reports on reserve compliance to MAS; annual audits of reserve assets.
Switzerland	No stablecoin issuers in Switzerland are currently subject to FINMA oversight and therefore not subject to disclosure requirements.	No stablecoin issuers in Switzerland are currently subject to FINMA oversight and therefore not subject to supervisory reporting.
UK	Governance structures, redemption policies, and reserve details expected to be disclosed (under development).	Likely to require internal audits of reserve assets in the upcoming framework (under development).
US	Redemption policies and fees, monthly reporting of number of outstanding stablecoins issued and reserve portfolio composition (to be examined by public accounting firm and attested to by issuer CEO and CFO), annual audited financial statements (for larger issuers)	Reports, on request of supervisor, covering financial condition, systems for monitoring and controlling risk, and compliance with laws and regulations.

4.2.1. Public disclosures

Public disclosure requirements for stablecoin issuers vary across jurisdictions, with most focusing on transparency for consumers and market participants. Commonly disclosed information includes reserve asset details, governance structures, and redemption rights. However, some jurisdictions do not specify public disclosure requirements for stablecoins, reflecting differences in regulatory maturity. Furthermore, while some jurisdictions such as EU, Hong Kong and the US require, or will require, audit verifications others set a lower standard by mandating independent ‘attestation’ or ‘proof of reserve’ (e.g. Bermuda; Singapore requires monthly attestation, with annual audit). In some cases, it is not clear what the required assurance

standard is; for instance, one jurisdiction reported that issuers must appoint 'an approved auditor to conduct an examination of the issuer's reserve assets on a quarterly basis and provide a proof of reserve report by an independent auditor.'

Many jurisdictions mandate regular public updates on reserve assets, but some jurisdictions have not specified the details or the frequency. In the EU, under MiCAR, stablecoin issuers must publish on a monthly basis, updates on the size, composition, and value of reserve assets. Similarly, Singapore will require monthly independent attestations of reserve compliance to be published, along with white papers that include detailed information on governance, risks, and redemption rights. Canada also mandates monthly reserve attestations to be made publicly available. The Bahamas requires issuers to maintain an offering memorandum that includes reserve asset details, which must be updated promptly following any significant changes. In Hong Kong, licensed stablecoin issuers are required to engage qualified and independent auditors to perform attestation on a regular basis at a frequency that is acceptable to the supervisory authority, on the market value and composition of reserve assets. In Japan, the disclosure of reserve composition is not specified. In the US, stablecoin issuers will be required to disclose monthly the total outstanding number of stablecoins in circulation and the amount and composition of reserves, including the geographic location and tenor of assets. Issuers with more than USD 50 billion in total consolidated issuance will be required to disclose audited annual financial statements.

Bermuda includes public disclosure requirements in its Stablecoin Guidance, including monthly attestations on the nature and quantity of reserve assets, custodial arrangements, and risk overviews. In the Philippines, disclosures are tied to the sandbox application process, which may include reserve details, but there are no explicit ongoing public disclosure mandates.

Verifications (in some jurisdictions, audits) of reserve assets are increasingly becoming a standard requirement for stablecoin issuers, with many jurisdictions already implementing such measures or developing regulations to include them. Jurisdictions such as The Bahamas, Bermuda, Canada, Hong Kong and Singapore require independent audits of reserve assets, with varying frequencies. The Bahamas mandates quarterly audits, while Singapore requires annual audits to ensure compliance with reserve requirements. Canada and Hong Kong require annual audited financial statements. In the EU, issuers of EMTs must provide bi-annual independent audits of their reserve assets, with findings reported to management and regulators. Japan requires regular internal audits, though specific timelines are not outlined. Among jurisdictions developing their frameworks, the UK is likely to include audit requirements, while Armenia and Chile remain in the early stages of regulatory development.

In addition to reserves, public disclosure requirements often include white papers or other publications that cover other critical areas such as governance arrangements, conflicts of interest, the issuer's risks, and redemption rights.

- Examples of white paper requirements: In the EU, stablecoin issuers must publish a white paper before the issuance is undertaken (and the white paper must then be maintained and updated), providing relevant information to the public such as protocols for validating transactions, functioning of the distributed ledger technology mechanisms to manage liquidity risk, rights and conditions of redemption, arrangements with third parties, complaint handling procedure and assessment of ML/TF. In Singapore, issuers will be required to publish white papers that include detailed descriptions of governance

structures, risks affecting token price stability, and obligations to stablecoin holders. Similarly, Hong Kong mandates the publication of white papers that detail conflicts of interest, operational mechanisms, and risks associated with stablecoins.

- Examples of other publications: In the US, payment stablecoin issuers will be required to disclose redemption policies, including procedures for timely redemption and fees associated with redemption. The UK is proposing to require issuers to disclose governance structures and redemption policies to ensure consumer understanding and confidence. In Japan, disclosures include the timing and procedures for redemption, as well as issuer obligations. Bermuda and The Bahamas include governance and risk-related disclosures as part of their broader frameworks, while the EU requires issuers to publish summaries of audit reports, alongside any significant events likely to affect the token's value.

4.2.2. Supervisory reporting

Supervisory reporting for stablecoin issuers is typically aimed at providing authorities with detailed, non-public information for supervisory purposes. Most jurisdictions focus on detailed data of reserve assets, governance updates, and systemic risk monitoring. However, some jurisdictions do not yet have specific internal reporting requirements for stablecoins.[92]

Regular reserve asset reporting is a cornerstone of internal regulatory reporting in many jurisdictions.

- In the EU, issuers must submit quarterly reports to supervisors, detailing reserve asset size, composition, and the number of tokens in circulation.[93] Furthermore, issuers of ART and EMT denominated in currency of a country that is not a member of the EU must report to competent authorities on a quarterly basis the average number and average aggregate value of transactions per day during the relevant quarter.

- In the US, payment stablecoin issuers will be required to submit reports upon the request of their primary regulator, covering financial condition, systems for monitoring and controlling risk, and compliance with laws and regulations. The specific details of disclosure and regulatory reporting obligations have yet to be determined.

- Singapore will require stablecoin issuers to submit monthly and annual reports on reserve compliance to MAS. In The Bahamas, issuers must provide quarterly proof of reserves, including independent audits of reserve assets. Canada also requires monthly reserve attestations and audited annual financial statements be made publicly available. In Switzerland, quarterly crypto-specific reporting is required, covering both financial and non-financial risks, including reserve asset details. In Hong Kong, issuers are required to prepare statements on the market value and composition of reserve assets on a daily basis and report to the HKMA on a weekly basis.

Governance and operational updates are another common focus. In Japan, issuers must notify regulators of any changes to governance structures, reserve management policies, or other

---

92 For example, Switzerland for those stablecoin issuers under the default guarantee exemption scheme.

93 Issuers of EMT are bound also by the reporting obligations that are set by the Payment services directive which, inter alia, requires reporting on fraud events.

critical aspects. Similarly, Hong Kong requires issuers to submit governance details and reserve management updates to regulators and has published supervisory guidelines setting out such requirements. The UK is proposing that regulatory reporting of reserve assets shall be reported to the Bank of England and FCA, along with governance updates as part of broader regulatory reporting.

Some jurisdictions implement proportional or risk-based reporting frameworks. In the Philippines, quarterly transaction reports and additional regulatory submissions are required, with the scope determined by the issuer's business model and risk profile. In Switzerland, internal reporting frameworks include both traditional financial risks and crypto-specific risks, such as operational resilience and anti-money laundering compliance, however, this obligation does not apply to issuers using the 'default guarantees from banks'.

4.3. Monitoring financial stability risks

While financial stability risks from crypto-assets appear limited at present, monitoring financial stability risks in crypto asset markets, including specific use cases and interconnections, is critical for authorities to fulfil their financial stability mandates. CA Recommendation 8 notes that jurisdictions should identify and monitor interconnections both within the crypto asset ecosystem and between the crypto asset ecosystem and the broader financial system.

Jurisdictions have made varying levels of progress in monitoring financial stability risks. Fourteen jurisdictions have adopted a proactive approach, establishing infrastructures that enable monitoring of financial stability risks.[94] Their efforts often involve regulatory reporting, data analysis, and other structured approaches to assess risks. In contrast, eleven jurisdictions are conducting limited monitoring of developments and activities that may not fully encompass financial stability risks.[95] These jurisdictions have implemented partial measures but lack comprehensive monitoring frameworks. A further seven jurisdictions, reported no active monitoring of financial stability risks in crypto asset markets.[96]

Some jurisdictions have adopted notable practices to address financial stability risks. Regulatory reporting from CASPs or incumbent financial institutions is a key source used by several authorities, including Bermuda, Canada, Hong Kong, Indonesia, Singapore, Switzerland, Thailand, and the UK. For example, Thailand uses regulatory reporting to understand market movements and the custody of client assets, while Switzerland and the UK focus on data from traditional financial institutions. In addition to regulatory reporting, jurisdictions such as Bermuda, France, Hong Kong, Hungary, Italy, Netherlands, Philippines, Thailand, and the UK use public and commercial data tools, including blockchain analytics providers, to monitor risks. The EU has highlighted the use of metrics such as market capitalisation, trading volumes, and concentration risks to identify potential vulnerabilities. Surveys have also proven effective in some jurisdictions, such as France, Germany, and Switzerland, where authorities have gathered data on crypto adoption and activities. Switzerland, for instance, has been conducting detailed

---

94 Bermuda, The Bahamas, Canada, France, Germany, Hong Kong, Hungary, Indonesia, Korea, Philippines, Singapore, Switzerland, Thailand, and the UK.

95 Argentina, Australia, Brazil, India, Italy, Japan, Netherlands, Saudi Arabia, Spain, Türkiye and Uruguay.

96 Armenia, Chile, China, Kazakhstan, Nigeria, Poland and South Africa.

surveys since 2023 to collect granular information on crypto-related activities. Cross-border collaboration has also emerged as a best practice, with jurisdictions such as Germany, the Netherlands, Singapore, Spain, and the UK working with international organisations and peers to enhance their financial stability risk monitoring capabilities.

In addition to these efforts, some jurisdictions have begun exploring methods to integrate crypto-asset transaction monitoring into broader capital flow management systems. These approaches are particularly relevant in jurisdictions seeking to understand the role of crypto assets in cross-border financial flows and their potential implications for financial stability (see Box 9).

Box 9: Approaches to monitor crypto-asset transactions within capital flow management systems

Crypto-assets pose significant challenges for jurisdictions with capital flow management systems due to their borderless and pseudonymous nature. These characteristics enable transactions to occur outside traditional financial systems, complicating the monitoring and enforcement of foreign exchange (FX) regulations and creating risks of regulatory arbitrage. For jurisdictions with capital controls, such as India, South Africa, and Indonesia, the growing use of crypto-assets raises concerns about financial stability, regulatory sovereignty, and the ability to monitor cross-border flows effectively.

Crypto-assets also create specific obstacles for the implementation of key FSB recommendations, further complicating efforts to manage capital flows effectively. The borderless nature of these assets raises challenges to implement CA Recommendation 3, which emphasises the potential benefits of cross-border regulatory cooperation and supervision, particularly when CASPs operate in offshore jurisdictions outside the reach of domestic authorities. The pseudonymous nature of transactions, combined with technologies such as mixers and tumblers, presents additional challenges to fulfilling CA Recommendation 6, which calls for comprehensive and ongoing access to relevant data. Specifically, authorities require granular data on transaction volumes, counterparties, geographic flows, and the timing of transactions to monitor compliance with capital flow measures and detect potential circumvention. South Africa and India highlight that CASPs are not yet required to report crypto-asset transactions, leaving critical data gaps that hinder effective oversight. Furthermore, foreign currency-pegged stablecoins present unique challenges, as they can facilitate cross-border payments outside regulated banking channels, undermining compliance with capital flow measures and potentially destabilizing monetary systems. Ensuring that stablecoin activity occurs within the regulatory perimeter is critical to maintaining oversight, enforcing capital controls, and safeguarding financial stability.

To address these challenges, jurisdictions are employing a variety of approaches. Brazil is proactively integrating crypto-asset oversight into its FX framework by requiring CASPs to report customer transactions to the Central Bank of Brazil, enhancing transparency and regulatory reach. Similarly, South Africa is conducting a policy review to refine its exchange control regulations, with a focus on bringing CASPs within its reporting and supervisory scope. India and Indonesia emphasise the importance of cross-border collaboration to mitigate risks of regulatory arbitrage and enhance monitoring of crypto-asset activities. Thailand is addressing challenges in FX monitoring through collaboration between the Bank of Thailand and the Thai SEC, which involves sharing aggregate data on regulated crypto-asset activities, though efforts are ongoing to improve data granularity and address peer-to-peer transfers outside regulated intermediaries.

Despite these efforts, significant gaps remain in the monitoring of financial stability risks. A critical shortcoming is the lack of comprehensive monitoring of interconnection risks, both within crypto asset markets and between crypto markets and the traditional financial system. Many jurisdictions have not yet developed robust frameworks to assess these interconnected risks, which represent a potential vector for systemic financial stability concerns. Another key challenge is data quality and availability. Authorities in France, Nigeria, Singapore, Spain, and the UK have highlighted limitations in data provided by blockchain analytics firms, as well as an

over-reliance on a small number of vendors. Furthermore, the limited use of regulatory reporting from CASPs is a notable gap. While some jurisdictions, such as Canada and Indonesia, rely on CASP reporting to monitor risks, others do not have similar requirements, which restricts their ability to gather critical data on activities that could pose financial stability risks.

4.4. Data related implementation progress: overall findings

The limited implementation progress highlights significant gaps and inconsistencies in regulatory reporting frameworks for CASPs and stablecoin issuers, which undermine authorities' ability to monitor and address financial stability risks effectively. Many jurisdictions lack comprehensive requirements for CASPs, particularly for financial and non-financial risks, while reporting frequency varies widely, with few jurisdictions mandating timely and frequent submissions. For stablecoin issuers, inconsistent reporting requirements – particularly regarding reserve transparency, governance disclosures, and audit obligations – risk undermining the consistency of GSC recommendations and creating an uneven playing field across jurisdictions. The limited use of regulatory and supervisory data for financial stability monitoring and challenges in data quality, such as reliance on third-party providers and lack of standardised templates, further hinder risk oversight. Additionally, insufficient monitoring of interconnections within crypto markets and between these markets and traditional financial systems can delay timely recognition of systemic risks as crypto adoption grows.

5. Implementation of cross-border cooperation and coordination recommendations

Cross-border regulatory and supervisory cooperation and coordination relating to crypto-asset markets is still developing but faces significant challenges and gaps, hindering effective oversight. Authorities are leveraging existing mechanisms in place to permit a degree of information sharing across jurisdictions. However, these existing mechanisms are often limited as to which authority is able to make use of them and are primarily used for investigations and enforcement (such as the IOSCO MMoU), and to a lesser extent licensing and supervision. Very few of the existing mechanisms have a purpose to facilitate monitoring and sharing information relevant to financial stability. Furthermore, there is a widespread view that greater levels of cooperation may be needed for crypto-asset markets than for traditional finance due to the current relative ease of cross-border activity and rapid developments in crypto-asset markets.

One of the key challenges to effective cooperation and information sharing is the early-stage nature of crypto-asset and stablecoin regulatory developments in most jurisdictions. Given this, there are challenges relating to fragmented responsibilities across domestic authorities that appear to be emerging in the evolving structure of regulatory responsibilities assigned to different domestic authorities. Such fragmentation can also lead to inconsistent definitions of crypto-assets between jurisdictions, inconsistent scope of crypto-asset activities covered by regulatory frameworks and legal barriers such as secrecy or data privacy laws, which can prevent, delay or hinder information sharing. Additionally, as set out earlier in this report, many jurisdictions do not have frameworks in place to collect the data necessary to monitor levels of adoption, systemic risks or address regulatory arbitrage effectively. While some jurisdictions are leveraging existing arrangements, such as regional frameworks and expanded cooperation between certain jurisdictions, to address cross-border cooperation challenges, more efforts are

likely to be needed to strengthen cross-border cooperation and respond to the rapid evolution and global nature of crypto-asset activities.

5.1. The global nature of crypto-asset activities

CASPs and stablecoins arrangements often have a global footprint, being headquartered in one jurisdiction and establishing branches in or operating from various jurisdictions around the world. They interact with many customers in various different jurisdictions. The FSB recommendations set out that jurisdictions should cooperate and coordinate with each other to share information and support consistent regulatory and supervisory outcomes. Similarly, IOSCO's crypto and digital assets recommendations cover the importance of information sharing in relation to investor protection and market integrity risks. FATF's recommendations cover similar topics in relation to money laundering and financial crime risks. Together, these recommendations reinforce that cooperation and coordination is likely to prove important to the regulation of CASPs and stablecoin arrangements and is, therefore, likely to prove important to managing any financial stability risks from crypto assets which may emerge.

Cooperation starts with mutual assistance and learning. As jurisdictions are implementing global standards in their domestic regulatory frameworks at different speeds, cross-border cooperation is likely to prove beneficial across all stages of the regulatory and supervisory journey. Conventional cooperation arrangements focus on a particular part of regulation such as licensing, investigation or enforcement. However, the present extent of these conventional arrangements may be unlikely to address the financial stability risks which may arise in this sector given the character of its global operations. Effective and efficient cooperation and information exchange during regulatory development phases can also support EMDEs which may not only face challenges with mitigating risks stemming from crypto-assets, but challenges with resourcing and expertise.

Similarly, supervisors should be aware of where, and how, each CASP operates. They also should consider the risks posed by their operations, both individually and collectively within their jurisdiction, as well as more broadly across jurisdictions. Supervisory authorities cannot address these questions alone. They should cooperate and coordinate with each other, as appropriate, both domestically and internationally. Otherwise, some CASPs may seek to operate out of jurisdictions with less stringent legal and regulatory requirements or set up their higher-risk products and services in jurisdictions with less robust supervision or legislation which stops or hinders effective information sharing with other jurisdictions. Bad actors may also leverage these CASPs' business models to obfuscate their locations of fraudulent activities. Equally, risks, including financial stability risks, becoming apparent in one jurisdiction, may not be so apparent in other jurisdictions – amplifying the risk if it is not addressed holistically

Jurisdictions should also cooperate and coordinate on how CASPs' activities and products interact with other parts of the crypto-asset ecosystem as well as traditional finance. Lack of efficient and effective cross-border cooperation, such as information sharing, may hamper the ability of jurisdictions to monitor potentially systemic exposures, trends, risks, or shocks originating in crypto-asset markets, especially if these markets become more integrated with the wider financial system. The IMF-FSB's 2023 paper on crypto-asset notes the potential for

amplifying contagion when cooperation arrangements have not effectively captured all aspects of crypto-asset activities.[97]

Given this, it is all the more important for jurisdictions to embed a culture of cooperation throughout the regulatory and supervisory lifecycle, and look to coordinate and cooperate closely, both across domestic and international authorities, to share information as appropriate, in particular around actual or potential risks as well as firm specific issues, ensuring that CASPs and stablecoins arrangements are effectively regulated given their global business models, and to support supervisory and enforcement actions in a regular, constructive, and timely manner. Where existing arrangements do not presently support this, or where it is not possible because of either regulatory or legislative barriers, this should be addressed as regulatory frameworks are developed and implemented.

5.2. Progress in cross-border cooperation

To coordinate across borders, most jurisdictions reported relying on MoUs which establish terms under which signatory authorities agree to share information and coordinate regulatory responses with other authorities, both domestically and internationally (see Annex 4). Although some jurisdictions have bilateral or regional MoUs with other jurisdictions, the most common MoU referenced by jurisdictions' responses is the IOSCO Multilateral MoU (MMoU) and related Enhanced MMoU (EMMoU). These arrangements were produced by IOSCO and the 130 IOSCO ordinary member authorities are signatories. Some, but not all, of these jurisdictions are also a signatory to the EMMoU. The IOSCO MMoUs and EMMoU provide a mechanism for signatories to exchange information in securities-related enforcement investigations and proceedings. They are structured as broadly applicable to capital markets activities and products and were not designed specifically for the purposes of regulating crypto-assets, and there are limits to relying on these arrangements entirely to provide a comprehensive framework for cross border cooperation.

Potential gaps in utilising existing arrangements for cooperation and coordination arise when authorities regulate crypto-asset activity in a certain jurisdiction which are not themselves IOSCO members. For example, a jurisdiction may regulate crypto-asset-related activity using its banking regulator, which is not a party to the IOSCO MMoU. The banking regulator, or regulator responsible for financial stability (which is not a party to the MMoU) may encounter challenges receiving or requesting information from another jurisdiction's securities regulator (which is a party to the MMoU).

As set out in the IOSCO Thematic Review Assessing the Implementation of Recommendations for Crypto and Digital Asset Markets there are different uses of the MMoU across jurisdictions. The MMoU focusses on enforcement related issues, however a small number of jurisdictions have used it to request information related to fitness and propriety assessments as part of an authorisation process. Although the MMoU does not preclude any signatory from sharing information as part of on-going supervision, in practice it is mainly used for enforcement

[97] IMF-FSB (2023), *IMF-FSB Synthesis Paper: Policies for Crypto-assets*, September.

purposes and authorisation purposes to some extent. Its use does not currently extend to financial stability risks, either in traditional finance or crypto and digital asset markets.

5.2.1. Challenges

Some jurisdictions noted it can be challenging to identify the appropriate authority in a foreign jurisdiction when seeking to coordinate. Additionally, MoUs, bilateral or regional, can often be set up for specific investigation or enforcement purposes and so may not meet the need of authorities to exchange information on day-to-day regulatory or risk-related matters.

These challenges in cross-border coordination could enable crypto-asset activities, or broader market trends, that pose potential financial stability risks to remain unmonitored or unaddressed in some jurisdictions. Crypto-asset-related entities, including large stablecoin issuers or CASPs, can participate in markets across jurisdictions and may conduct most of their activities outside of the jurisdiction in which they are officially domiciled. The regulatory authorities of those home jurisdictions may lack tools to provide or receive information needed for comprehensive monitoring of that CASP's activities. This could be exacerbated by existing cross-border cooperation arrangements and tools not being intended to exchange information on financial stability-related matters.

Financial stability monitoring and regulation could require greater focus on linkages between systemically important financial institutions and participants in crypto-asset markets. This could reduce the risk that distress in one crypto-asset market participant or sector spills over to other financial intermediaries or jurisdictions.

5.3. Tools for cross-border cooperation

At present, jurisdictions generally leverage a range of existing cross-border cooperation mechanisms, with a small number of them also exploring or establishing new mechanisms. To date, jurisdictions generally have not established a consistent or regular model for cooperation, although we note that jurisdictions are still at the stage of developing their regimes. Consequently, this review found no evidence that currently available cooperation mechanisms adequately cater to sharing information and risks relating to financial stability either in developing or established regimes. In addition, in some cases there are legal impediments to sharing personal or confidential information. In light of the limited and nascent usage of these mechanisms, it remains too early to assess whether cooperation mechanisms are effective, or whether there are fundamental barriers (such as legal or operational) limiting such use. At this stage, the absence of financial stability coverage and lack of data collection, appears to be a hurdle to cooperation.

The use of cross-border cooperation arrangements and tools appears limited and to occur on an ad-hoc basis, where appropriate. As is the case for traditional financial markets, cooperation arrangements and MoUs which are in place seem to be primarily used for authorisation, licensing or registration purposes (e.g. to exchange information on firms operating in multiple jurisdictions), investigations, and to a lesser extent for supervision-related matters (also covering AML/CTF). It is not clear to what extent these cooperation arrangements have been used to cover financial stability matters. In addition, it is also not clear that cooperation arrangements have been used extensively for enforcement related to crypto-asset activities, bearing in mind

that the regulation of crypto-assets is still relatively new in most jurisdictions and regulatory frameworks are under development. Notwithstanding, a small number of jurisdictions have started to expand existing cooperation arrangements for broader usage albeit focussing on general crypto-asset regulation and not financial stability. For instance, Bermuda intends to expand arrangements from licensing to enforcement purposes, and Chile established where relevant, bilateral engagements that might cover both traditional and innovative entities, the possibility to enable cross-border on-site inspections.

5.3.1. Leveraging non-financial stability international cooperation frameworks

A majority of jurisdictions participating in this review reported that their work on cross-border cooperation primarily relies on the IOSCO MMoU and/or EMMoU, which were not designed for financial stability purposes. Currently, all FSB member jurisdictions are MMoU signatories, and most of them naturally leverage on IOSCO MMoU or EMMoU as a common cooperation channel. Nonetheless, many of them did not indicate that they are actively using the MMoU or EMMoU for crypto-asset activities. These findings reflect the limited applicability of the IOSCO MMoU/EMMoU to cross-border cooperation on financial stability risks associated with crypto-asset activities.

A small number of jurisdictions including India, Korea, and Türkiye reference financial crime cooperation frameworks under FATF or the Egmont Group as the basis for their cooperation. The Egmont Group is an international organisation which provides secure platforms for national Financial Intelligence Units (FIUs) to exchange information and expertise to counter money laundering and terrorist financing, facilitating cross-border cooperation between approximately 177 FIUs.

5.3.2. Use of regional cooperation frameworks

Jurisdictions have also entered into regional MoUs and cooperation arrangements. Several Latin American jurisdictions, such as Chile, have highlighted their membership in Pacific Alliance MoUs, the Ibero-American Securities Markets Institute (IIMV) FinTech MoU, and the Association of Insurance Supervisors of Latin America (ASSAL). Some members of the IOSCO Asia-Pacific Regional Committee (APRC) have developed a regional supervisory MMoU, including Australia, Hong Kong, Japan, Korea, Singapore, and Thailand which facilitates signatories to exchange supervisory information to the fullest extent permissible, in accordance with their domestic laws and regulations. This supervisory MMoU covers the relevant regulatory activities for authorisation and ongoing supervision and offers a framework to exchange information on emerging or potential risks and issues of common interest. In the EU, sharing of information among NCAs which are members of ESMA takes place under the ESMA MMoU on information and cooperation exchange, which allows for the sharing of confidential information between European authorities on matters of authorisation, supervision or enforcement.

Some authorities choose to use public blacklists or warning lists of non-compliant firms published by overseas authorities to cross-reference firms which may be seeking to conduct crypto-asset or stablecoin related activities in their jurisdictions. Canadian provincial authorities, such as those in Alberta, Quebec, and Ontario, maintain such blacklists, in particular targeting offshore CTPs for enforcement actions. Although these blacklists may be informed by data or input received through cross-border cooperation mechanisms, it is not clear the extent to which they

are considered by other jurisdictions in their regulatory, supervisory, or enforcement actions. Internationally, IOSCO maintains a list of alerts and warnings voluntarily submitted by member authorities regarding unauthorised or noncompliant firms through its International Securities and Commodities Alerts Network (I-SCAN). While the list is not specific to crypto-asset firms, it can include alerts and warnings related to unauthorised or noncompliant firms offering crypto-asset services.

5.3.3. How international and regional cooperation frameworks are being used

Jurisdictions where crypto-assets fall under the purview of the securities or markets regulator are more likely to rely on IOSCO's MMoU or EMMoU as an available mechanism for information sharing. In contrast, jurisdictions lacking clarity on the asset categorisation of crypto-assets or those without established regulatory frameworks or designated market regulators for this purpose may rely less on these mechanisms, or be less familiar with their use, despite in some cases being signatories to the IOSCO arrangements.

Beyond securities regulators, in some cases, central banks are taking the lead in cross-border coordination. For instance, the Saudi Central Bank's bilateral communication with overseas central banks has reportedly been effective in addressing issues related to offshore crypto-asset service providers.

Crypto-assets are rapidly evolving and sharing appropriate information about risks may support improved oversight of firms operating internationally. From a financial stability perspective, the role of nonbank financial intermediation (NBFI) and the exposure of banks to NBFIs further adds a layer of uncertainty.[98] If the linkages between NBFIs and the crypto-asset ecosystem also grow, we may see growing interconnections that can influence system-wide financial stability. Data gaps can limit a complete and timely assessment of vulnerabilities.

From the responses, it is evident that a certain amount of cross-border cooperation is being carried out through multiple mechanisms and across different types of regulators. However, these tools are still infrequently used as regulatory frameworks continue to develop, and appear at present to be neither sufficient to address the risks posed by the crypto-asset sector, nor suitable for financial stability purposes. Jurisdictions and the FSB may consider further efforts to make the FSB recommendations more effective.

5.4. Challenges in cross-border cooperation

Jurisdictions have identified several recurring challenges related to cross-border cooperation in the regulation, supervision, and oversight of crypto-assets. First, responsibilities within a jurisdiction are often divided among multiple authorities (see section 2.2), making it difficult for external jurisdictions to identify the appropriate authority when seeking assistance. With regimes still coming online and clarity across division of responsibilities among authorities still coming into focus, this can result in delays in processing cooperation requests, which is likely to be problematic given the speed at which crypto-asset activities occur across borders. Timeliness is

98 IMF (2025), *Global Financial Stability Report: Enhancing Resilience amid Uncertainty*, April.

critical, especially when legal deadlines apply to certain procedures. The division of responsibilities suggests the benefits of clear points of contact for cross-border cooperation.

Second, the scope of existing cooperation arrangements can limit their effectiveness. Two key limitations have been highlighted. One is that (as mentioned earlier) not all responsible authorities may fall within the scope of international agreements. For example, most signatories to the IOSCO MMoU are securities regulators, leaving out central banks or other authorities that may oversee crypto-asset or stablecoin activities. This gap emphasises the importance of robust domestic cooperation frameworks to ensure information sharing even when certain authorities are not part of international arrangements. On the other hand, some jurisdictions with cross-sectoral authorities benefit from broader remits that allow easier collaboration across sectors. Another limitation is the divergence in definitions of crypto-assets. If jurisdictions define crypto-assets differently, it can hinder the use of cooperation tools that rely on consistent definitions. For instance, jurisdictions that do not classify crypto-assets as securities may face challenges leveraging the IOSCO MMoU, which focuses on enforcing securities and derivatives laws.

Finally, secrecy or data privacy laws may pose significant barriers to cooperation. Some jurisdictions restrict the ability of firms in their jurisdiction to share information with regulators in other jurisdictions. In addition, some are hesitant to share sensitive information due to fears about confidentiality breaches or the lack of guaranteed reciprocity. These concerns lead to delays in addressing cooperation requests where they are made and, in some cases, may prohibit or discourage participation in cooperation arrangements altogether. Additionally, differing confidentiality and data protection legislation across jurisdictions can further complicate legal processes, as additional time may be needed to demonstrate compliance with these standards. Addressing these challenges is likely to foster more effective and efficient cross-border cooperation in the rapidly evolving crypto-asset landscape.

Box 10: Good practices - Legislative empowerment for cooperation

Domestic legislation can enable authorities to cooperate with overseas authorities on issues relevant to their mandates and remits. Clear legal frameworks where authorities understand when and how they can cooperate with overseas authorities can help narrow gaps where cooperation requests fall outside the scope of existing arrangements. Similar measures can also be in place for domestic authorities to cooperate with each other – for example, MoUs between the HKMA and the SFC to exchange information domestically in Hong Kong.

Several examples of legislative empowerments for domestic and cross-border cooperation from surveyed jurisdictions exist. The Bahamas' Digital Assets and Registered Exchanges (DARE) Act appears to provide greater clarity and flexibility, as it empowers its Securities Commission to cooperate internationally on supervisory, investigative, and enforcement matters with any relevant regulator in a foreign jurisdiction, even where multiple regulators are involved. Additionally, the DARE Act enables the Securities Commission to cooperate with any relevant domestic authority.

Likewise, the Monetary Authority of Singapore, South African Financial Sector Conduct Authority (FSCA), Switzerland's FINMA, and some Canadian provincial authorities have been empowered to enter into MoUs with overseas regulators and law enforcement agencies for regulatory and enforcement assistance, and to engage in formal and informal information exchange with foreign counterparts.

In the EU, the MiCAR sets out requirements for national authorities, the EBA, and ESMA to cooperate with each other through exchanging and requesting information to facilitate carrying out their legal duties. MiCAR also enables national authorities to conclude cooperation arrangements with jurisdictions outside the EU, with the EBA and ESMA currently developing templates for such cooperation arrangements. Further, the sharing of information among NCAs which are members of ESMA takes

place under the ESMA Multilateral Memorandum of Understanding (MMoU) on information and cooperation exchange, which allows for the sharing of confidential information between European authorities on matters of authorisation, supervision or enforcement. Using common templates can help create consistency and legal certainty across cooperation arrangements and can help speed up discussions on entering into arrangements if documents are readily available. None of the EU member states who took part in the review have yet established cooperation arrangements with overseas authorities under MiCAR.

5.5. Cross-border cooperation implementation progress: overall findings

The analysis underscores that cross-border cooperation and coordination in crypto-asset markets at present are fragmented, inconsistent, and insufficient to address the global and rapidly evolving nature of these markets. Existing mechanisms, such as MoUs, are predominantly used for enforcement and licensing purposes and in only limited occasions extend to financial stability monitoring or broader supervisory objectives. Key challenges include fragmented responsibilities among domestic authorities, divergent definitions of crypto-assets, inconsistencies in regulatory scope, and barriers such as secrecy or data privacy laws. Some of these challenges are due in part to the early stage of regulatory frameworks in many jurisdictions. Nonetheless, all of these impede effective information sharing. These shortcomings may create opportunities for regulatory arbitrage, constrain the oversight of systemic risks, and delay coordinated enforcement responses. While some jurisdictions have made progress through regional frameworks and expanded cooperation, these efforts remain ad hoc and lack the uniformity required to address the interconnected risks posed by crypto-asset activities across jurisdictions. Enhancing cross-border cooperation frameworks, embedding financial stability considerations, and fostering trust and reciprocity in information-sharing arrangements will strengthen effective global oversight and mitigating the risks associated with regulatory fragmentation.

Annex 1: Definitions of implementation stages

In assessing jurisdictions' progress in implementing the FSB's Global Regulatory Framework for crypto-assets, the report focused primarily on the establishment of jurisdictional regulatory, supervisory and oversight frameworks. This assessment does not indicate whether a jurisdiction's framework fully addresses all elements of each CA and GSC recommendation. In this report, the following definitions are used for the implementation assessment stages:

- **1 - No framework in place** means a jurisdiction has not developed, or disclosed plans to develop, a regulatory, supervisory and oversight framework for crypto-asset or stablecoin activities, that aims to address financial stability risks. This category includes jurisdictions with comprehensive bans or prohibitions on the use of crypto-assets, and those with regulatory frameworks that are limited to AML/CFT related registration and transaction reporting requirements.[99]

- **2 - Partial framework in place** means a jurisdiction's existing regulations apply only to some crypto-asset or stablecoin activities, or its regulations apply to all crypto-asset activities but only cover very limited financial stability risks as highlighted by the FSB's CA and GSC recommendations. For example, this category would include (i) a jurisdiction that applies existing financial regulations on a subset of crypto-asset and stablecoin activities that meet the definitions of financial products, payment instruments, or securities (but do not cover activities that do not meet these definitions); and (ii) a jurisdiction that has some form of licensing and oversight framework for CASPs and stablecoins, but such framework does not contain key financial stability requirements as recommended by the FSB, such as financial risk management, prudential buffers, and risk reporting.

- **3 - Plans for framework under public discussion** means a jurisdiction, or its relevant authorities, have made public plans to establish a comprehensive regulatory framework for crypto-asset or stablecoin activities, that aims to address financial stability risks. This includes (i) jurisdictions where legislatures have proposed or already granted powers to regulatory or supervisory authorities, but the details of the framework are not yet public and clearly defined; as well as (ii) jurisdictions where authorities have publicly initiated a policy development process, but the details of a proposed framework are not yet clear or fully defined. This definition does not indicate whether a jurisdiction's planned framework fully addresses all considerations under each CA and GSC recommendation.

- **4 - Framework proposed but not finalised** means a jurisdiction, or its relevant authorities, have proposed and made public a comprehensive regulatory framework for crypto-asset or stablecoin activities, that aims to address financial stability risks, but that framework is not yet finalised. This includes jurisdictions where detailed frameworks are proposed but awaiting legislative approval as well as jurisdictions where a clear legislative framework has been enacted but further rulemaking by authorities is

[99] While AML/CFT regulatory frameworks for the crypto-asset sector are critical to mitigate financial integrity risks, these frameworks are not within the mandate or purview of the FSB and this peer review.

not yet proposed or finalised. This definition does not indicate whether a jurisdiction's proposed framework fully addresses all considerations under each CA and GSC recommendation.

- **5 - Regulatory framework finalised** means a regulatory framework that aims to address financial stability risks, among other risks, has been finalised and the details of which are clearly defined and public. This includes jurisdictions where the legislation, rules and relevant guidance is clearly defined. Finalised in this context does not mean the framework is in effect. This definition does not indicate whether a jurisdiction's framework fully addresses all considerations under each CA and GSC recommendation. Jurisdictions may continue to update, modify, or refine their finalised frameworks as the crypto-asset ecosystem continues to develop and evolve.

Annex 2: Coverage of activities in CASP licensing and authorisation framework

Jurisdiction	Custody	Borrowing/Lending	Derivatives Trading	Proprietary Trading	Investment Activities (Yield/Earn/Liquid staking)	Own Issuance
Argentina	Permitted (segregation required)	Not covered by regulatory framework	Not covered by regulatory framework	Not covered by regulatory framework	Not covered by regulatory framework	Permitted for offerings
Armenia	Permitted (regulatory requirements)	Not covered by regulatory framework	Permitted under Securities Market Act	Permitted with regulatory requirements	Not covered by regulatory framework	Permitted (with disclosure requirements)
Australia	Permitted and regulated in certain cases[100]	Permitted (partially regulated[101])	Permitted under Corporations Act of 2001	Partially regulated[102]	Partially regulated[103]	Permitted (if compliant)
The Bahamas	Permitted (segregation required)	Permitted (regulated)	Permitted (regulated)	Does not require separate registration	Permitted (regulated)	Permitted (with approval)
Bermuda	Permitted (segregation required)	Permitted (regulated)	Permitted (regulated)	Permitted (regulated)	Permitted (regulated)	Permitted (with licensing)
Brazil	Permitted	Under development	Under development	Under development	Under development	Under development

[100] Regulated where custody of digital assets is tied to a regulated financial product (e.g., managed investment scheme).

[101] CASPs lending of fiat against crypto-assets (e.g., Bitcoin) is covered as credit activities. CASP lending of crypto-assets is not covered as credit activities.

[102] Regulated if assets used for proprietary trading meet the definition of financial product.

[103] If structured as collective investment schemes then regulation applies. However, some investment activities may be structured to fall outside existing regulation.

Jurisdiction	Custody	Borrowing/Lending	Derivatives Trading	Proprietary Trading	Investment Activities (Yield/Earn/Liquid staking)	Own Issuance
Canada	Permitted	Permitted (if compliant)	Requires approval by self-regulatory agency	Not permitted	Permitted (if compliant)	Prohibited
Chile	Permitted (segregation required)	Not covered by regulatory framework[104]	Permitted	Permitted	Not covered by regulatory framework	Not covered by regulatory framework
EU	Permitted (segregation required)	Not covered by regulatory framework	Permitted under MiFID	Prohibited for trading venues	Not covered by regulatory framework	Regulated under issuer framework
Hong Kong	Permitted (segregation required)	Prohibited for licensed CASPs[105]	Prohibited for licensed CASPs[106]	Prohibited (limited exceptions)	Requires separate approval	Disclosure required for affiliation
Indonesia	Permitted (centralised custodians)	Not covered by regulatory framework	Under development	Permitted, subject to conflicts of interest rules	Under development	Under development
Japan	Permitted (segregation required)	Permitted (partially regulated).[107]	Permitted under Financial Instrument and Exchange Act	Partially regulated[108]	Not covered by regulatory framework	Issuance permitted, offer or sale requires registration

[104] In Chile, although borrowing and lending is not explicitly regulated, according to Fintech Law and regulations, Alternative Trading Systems should have an internal regulation regarding trading and other aspects, and these entities, as well as intermediaries and custodians, should comply with prudential and conduct requirements which includes custody safeguards when applicable.

[105] Hong Kong is considering allowing the provision of crypto-asset borrowing and lending services while imposing robust risk management measures.

[106] Hong Kong is considering allowing the provision of crypto-asset derivatives while imposing robust risk management measures.

[107] Regarding lending, regulations under the Money Lending Business Act may apply for CASP lending activities. Regarding borrowing, if a CASP borrows crypto-assets, it must implement a framework to manage its debt. Regulations also prohibit excessive debt burdens.

[108] Regulations to address conflicts of interest exist.

Jurisdiction	Custody	Borrowing/Lending	Derivatives Trading	Proprietary Trading	Investment Activities (Yield/Earn/Liquid staking)	Own Issuance
Korea	Permitted (segregation required)	Not covered by regulatory framework[109]	Not covered by regulatory framework	Not covered by regulatory framework	Permitted	Not covered by regulatory framework
Philippines	Permitted	Margin trading prohibited, otherwise not covered by regulatory framework	Prohibited under SEC CASP Guidelines	Permitted and supervised under BSP Framework	Not covered by regulatory framework	Regulated under SEC CASP Rules
Singapore	Permitted	Not covered by regulatory framework	Permitted under SFA[110]	Not covered by regulatory framework	Not covered by regulatory framework[111]	Not covered by regulatory framework[112]
South Africa	Permitted (additional requirements)	Not covered by regulatory framework	Permitted under Financial Markets Act	Not covered by regulatory framework	Covered only where CASP is providing investment advice	Not covered by regulatory framework
Switzerland[113]	Permitted (partially regulated)	Permitted (partially regulated)	Permitted under Swiss Financial Market Infrastructure Act	Permitted (partially regulated)	Permitted (partially regulated)	Permitted (partially regulated)
Thailand	Permitted (segregation required)	Prohibited	Not covered by regulatory framework	Prohibited for digital asset exchanges	Not covered by regulatory framework	Regulated separately (SEC approval)

[109] Authorities have issued administrative guidance requesting suspension of crypto-asset lending services.

[110] CASPs must register under the Securities and Futures Act (SFA) for services that meet the definition of "capital markets product," which would include derivatives trading against crypto-asset underlying.

[111] If entities already providing regulated activities such as custody, then that entity is subject to holistic supervision.

[112] If entities already providing regulated activities such as custody, then that entity is subject to holistic supervision.

[113] Partially regulated means specific rules apply where crypto-asset activities qualify as payment or banking activities or the crypto-asset qualifies as a security.

Jurisdiction	Custody	Borrowing/Lending	Derivatives Trading	Proprietary Trading	Investment Activities (Yield/Earn/Liquid staking)	Own Issuance
Türkiye	Permitted (90% in cold wallets)	Prohibited	Prohibited	Permitted	Permitted	Prohibited
UK (proposed)	Consulting on regulation	Under development	Under development	Under development	Under development	Under development
Uruguay	Under development	Under development	Under development	Under development	Under development	Under development

Annex 3: Authorities responsible for the licensing and supervision of crypto-asset activities

Jurisdiction	CASPs		Stablecoin arrangements	
	Licensing	Supervision	Licensing	Supervision
Argentina	CNV	CNV	CNV (only for assets defined as securities)	CNV (only for assets defined as securities)
Armenia	CBA	CBA	CBA	CBA
Australia	ASIC	ASIC	ASIC	ASIC
The Bahamas	SCB	SCB	SCB	SCB
Bermuda	BMA	BMA	BMA	BMA
Brazil	BCB, proposed	BCB, proposed	BCB, proposed	BCB, proposed
Canada	CSA regulators	CSA regulators	CSA regulators (for securities/derivatives)	CSA regulators (for securities/derivatives)
Chile	CMF	CMF	CMF	CMF
China	N/A	N/A	N/A	N/A
EU	NCAs (see below)	NCAs (see below) and ESMA	NCAs (see below)	EBA (for issuers of significant ARTs and certain significant EMTs), NCAs (EMTs and other ARTs)
- **France**	AMF	AMF[114]	ACPR	ACPR
- **Germany**	BaFin, in cooperation with Deutsche Bundesbank	BaFin, in cooperation with Deutsche Bundesbank	BaFin, in cooperation with Deutsche Bundesbank	BaFin, in cooperation with Deutsche Bundesbank

[114] In cooperation with ACPR on AML-CFT.

Jurisdiction	CASPs		Stablecoin arrangements	
	Licensing	Supervision	Licensing	Supervision
- **Hungary**	MNB	MNB	MNB	MNB
- **Ireland**	CBI	CBI	CBI	CBI
- **Italy**	BdI and CONSOB	BdI and CONSOB	BdI and CONSOB	BdI and CONSOB
- **Netherlands**	AFM	AFM and DNB	DNB	DNB
- **Poland**	N/A	N/A	N/A	N/A
- **Spain**	CNMV	CNMV	BdE	BdE
Hong Kong	SFC	SFC and HKMA	HKMA	HKMA
India	N/A	N/A	N/A	N/A
Indonesia	OJK	OJK	N/A	N/A
Japan	FSA	FSA	FSA	FSA
Kazakhstan*	N/A	N/A	N/A	N/A
Korea	FSC	FSC, FSS	FSC, proposed	FSC, FSS, BOK proposed
Lebanon	N/A	N/A	N/A	N/A
Mexico	N/A	N/A	N/A	N/A
Nigeria	SEC	SEC	SEC	SEC
Philippines	BSP	BSP and SEC	N/A	N/A
Saudi Arabia	N/A	N/A	N/A	N/A
Singapore	MAS	MAS	MAS	MAS
South Africa	FSCA	FSCA	N/A	N/A
Switzerland	FINMA	FINMA	FINMA (if stablecoin activity is provided by a bank or	FINMA (if stablecoin activity is provided by a bank or

Jurisdiction	CASPs		Stablecoin arrangements	
	Licensing	Supervision	Licensing	Supervision
			other entity under existing supervision)	other entity under existing supervision)
Thailand	MoF and SEC	SEC	N/A	SEC (when used as investment vehicle)
Türkiye	CMB	CMB	N/A	N/A
UK	FCA, HMT if systemic	FCA, BoE if systemic	FCA, HMT if systemic	FCA, BoE if systemic
Uruguay	BCU, via SSF	BCU, via SSF	BCU, via SSF, proposed	BCU, via SSF, proposed
US	N/A	N/A	OCC (federally qualified payment stablecoin issuers) State regulator (for state qualified payment stablecoin issuer); Primary federal banking regulator (for bank insured depository institutions issuing a payment stablecoin)	Primary federal payment stablecoin regulator (OCC/FDIC/FRB/NCUA) or OCC or State payment stablecoin regulator. In certain cases, the State and Federal regulators will have joint jurisdiction.

* The regulatory framework of the Astana International Financial Centre was not in scope for this review.

Annex 4: Tools for cross-border cooperation

Jurisdiction	Multilateral cooperation frameworks and tools				Bilateral tools			International organisations /fora
	IOSCO MMoU	IOSCO EMMoU	Regional MoUs	Other	Bilateral MoUs	Informal/ad hoc engagement	Other	
Argentina	◉*			◉ (IIMV MoU*)	◉			
Armenia	◉							
Australia	◉	◉	◉ (APRC SMMoU)				◉ (MLATs)	
The Bahamas	◉	◉						
Bermuda	◉			◉ (GIFCS MMoU)	◉			
Brazil	◉*	◉*						
Canada	◉**	◉**		◉ (Blacklists, fraud prevention initiatives)	◉		◉	◉
Chile	◉		◉ (Pacific Alliance, ASSAL)	◉ (IAIS MMoU, IIMV MoU)	◉	◉		◉
China	◉*							
EU/EEA			◉ (through MiCAR/ESMA)					
France	◉				◉			
Germany	◉				◉	◉		
Hungary	◉							◉
Italy	◉				◉	◉		◉
Netherlands	◉*							

Jurisdiction	Multilateral cooperation frameworks and tools				Bilateral tools			International organisations /fora
	IOSCO MMoU	IOSCO EMMoU	Regional MoUs	Other	Bilateral MoUs	Informal/ad hoc engagement	Other	
Poland	◉*							
Spain	◉	◉		◉ (IIMV MoU*)		◉		
Hong Kong	◉	◉	◉ (APRC SMMoU)		◉			
India	◉*	◉		◉ (Egmont Group)				◉ (FATF)
Indonesia	◉				◉	◉		◉
Japan	◉*		◉ (APRC SMMoU)		◉			◉
Kazakhstan* **	◉*							
Korea	◉*	◉*						◉ (FATF)
Lebanon								
Mexico	◉*		◉ (Pacific Alliance*)	◉ (Egmont Group)				
Nigeria	◉*							
Philippines	◉*				◉	◉		
Saudi Arabia	◉*				◉			
Singapore	◉	◉	◉ (APRC SMMoU)		◉			
South Africa	◉	◉	◉ (CISNA MoU)					
Switzerland	◉	◉						
Thailand	◉	◉	◉ (APRC SMMoU)		◉			◉

Jurisdiction	Multilateral cooperation frameworks and tools				Bilateral tools			International organisations /fora
	IOSCO MMoU	IOSCO EMMoU	Regional MoUs	Other	Bilateral MoUs	Informal/ad hoc engagement	Other	
Türkiye	◉			◉ (Egmont Group)				◉
UK	◉	◉		◉ (Domestic BoE and FCA MoU)	◉		◉ (MLATs)	◉
Uruguay	◉				◉			
US	****	****	****	****	****	****	****	****

* This jurisdiction is a signatory or member but has not referenced use of the tool in their questionnaire response. This may indicate they have not used the tool for cooperation on crypto-asset related issues.

** Canadian provincial regulators can independently enter into cooperation agreements. Several provinces' authorities are signatories of the IOSCO MMoU and EMMoU.

*** The regulatory framework of the Astana International Financial Centre was not in scope for this review.

**** The US did not provide a response to the questionnaire.

Annex 5: Summary of high-level implementation survey

Note on the survey and its findings

This annex provides insights on high-level implementation progress, policy considerations, and challenges across FSB and non-FSB jurisdictions. The source of information was a high-level survey used to update progress previously reported by the FSB and IMF.[115] The results presented here are not necessarily comparable to those in the main body of this report because (a) the set of jurisdictions participating in the high-level survey was different (and larger) than those participating in the rest of the report, and (b) responses to the high-level survey were not subject to a rigorous assessment from the peer review team, in particular in cases where AML/CFT regulation is insufficient to meet the CA and GSC recommendations.

Responses to the FSB Survey[116]

Regions	Responding Jurisdictions	Total Responses
Americas	**Argentina,** Bahamas, Bermuda, **Brazil,** British Virgin Islands, **Canada,** Cayman Islands, Chile, Colombia, Guatemala, Jamaica, **Mexico** Panama, Peru, Trinidad and Tobago, Uruguay	16
Asia[117]	**Australia, Hong Kong, India, Indonesia, Japan, Korea,** Malaysia, Pakistan, Philippines, **Singapore,** Sri Lanka, Thailand, Vietnam	13
Commonwealth of Independent States	Armenia, *Georgia*	2
Europe	*Andorra*, Austria, Belgium, Czech Republic, **EU/EA**[118], Finland, **France, Germany,** *Gibraltar*, Greece, Hungary, Ireland, *Isle of Man*, Israel, **Italy,** Luxembourg, **Netherlands,** Norway, Poland, Portugal, Romania, **Spain,** Sweden, **Switzerland, UK,** Ukraine	26
Middle East and North Africa	Bahrain, Egypt, Kuwait, Lebanon, Oman, **Saudi Arabia, Türkiye**	7
Sub-Saharan Africa	BCEAO, Ghana, Mauritius, Namibia, **South Africa,** Zambia, *Zimbabwe*	7
Total Responses		**71**

FSB member jurisdictions are shown in **bold**. Jurisdictions that are not members of an FSB Regional Consultative Group are *italicised*.

[115] FSB and IMF (2024), *G20 Crypto-asset Policy Implementation Roadmap – Status report*, October.

[116] Some jurisdictions reported that their responses to the 2024 survey remain valid, so they are considered as a respondent.

[117] China responded that it has banned all crypto-asset activities and is therefore not placed to provide answers to the survey questions.

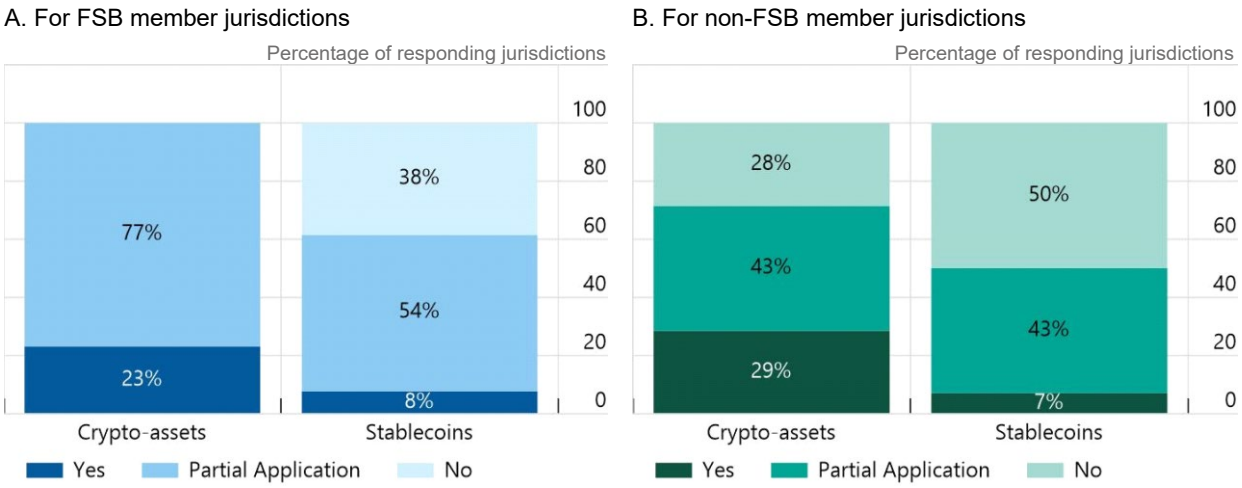
[118] European Commission provided a consolidated answer on EU-level regulatory progress and the European Central Bank provided a consolidated euro area response on specific risks, while EU member countries provided responses reflecting their national frameworks and considerations.

Status of implementation

Both FSB and non-FSB members have made progress in implementing crypto-asset and stablecoin frameworks. All FSB members have some existing laws and regulations for crypto-asset activities, while fewer (only 62%) have some stablecoin frameworks in place (Graph N1A).[119] Meanwhile, only 72% of non-FSB members reported existing laws and regulations covering at least part of crypto-asset activities. The percentage decreases to 48% for stablecoins.

Existing regulations consistent with FSB Framework

For FSB members and non-FSB member jurisdictions **Graph N1**



Source: FSB Survey

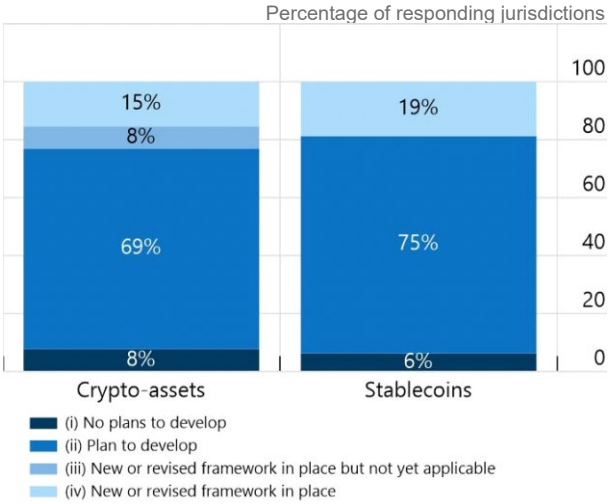
Both FSB and non-FSB members intend to develop new policies to cover the remainder of their partial application of crypto-asset and stablecoin regulations. A vast majority of FSB members have plans to introduce, or are in the process of introducing, new or revised frameworks (see Graph N2A). In comparison, such plans are slightly less common among non-FSB members (see Graph N2B).

[119] As EU member jurisdictions (in both FSB-member and non-FSB member group) will all apply the MiCAR consistently, responses are counted as 1 consolidated answer in Graph N1 and N2.

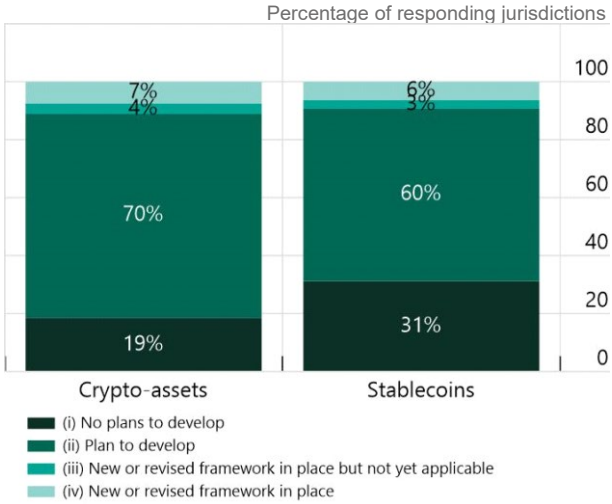
Stage of policy development for new or revised crypto-asset regulations

For FSB members and non-FSB member jurisdictions **Graph N2**

A. FSB member jurisdictions on crypto-asset activities and service providers and stablecoin arrangements



B. Non-FSB member jurisdictions on crypto-asset activities and service providers and stablecoin arrangements



Note: Jurisdictions who have reported "Yes" in Graph N1 are not included in this graph, as there is likely no need for further policy development in those jurisdictions. The detailed descriptions for the four categories are: (i) No plans to develop a new or revised regulatory framework for crypto-assets or plan has not been decided; (ii) Plan to develop a new or revised regulatory framework for crypto-assets, and work on the new or revised regulatory framework has started; (iii) New or revised regulatory framework in place but not yet applicable; and (iv) New or revised regulatory framework in place and applicable.

Source: FSB Survey

By end-2025, a majority of FSB members expect to reach alignment with the CA and GSC recommendations (62% and 50%, respectively); by end-2026, 70% of members expect to align both frameworks (Graph N3A). However, some FSB members that have yet to commit a date to reach alignment with the CA and GSC recommendations (24% and 20% respectively).[120]

Meanwhile non-FSB members generally have slower implementation timelines, with only 49% and 32% of such respondents expecting to reach alignment with CA and GSC recommendations, respectively, by end-2025 (Graph N4A). Nonetheless, they are expecting to catchup largely by end-2026 (when 59% of non-FSB members expect to reach alignment with CA recommendations), and a number of jurisdictions are also in the process of developing their timelines of implementation (at 24% for crypto-asset and 34% for stablecoin respectively).

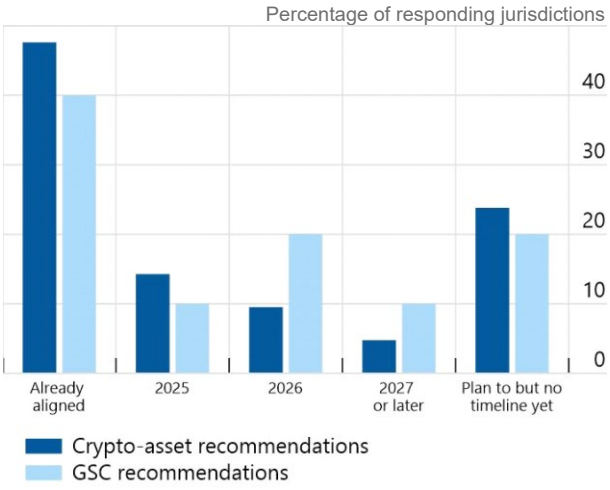
Comparing the responses from 2024 and 2025 surveys, most FSB members have not changed their expected implementation timing. Jurisdictions who had committed to align by end-2024 generally report they implemented their frameworks on time, with only two jurisdictions slightly delaying the expected time frame to end-2025 (Graph N3B). There are more delays reported by non-FSB members (of which 70% of these delays are just for one year), but this is balanced off with various jurisdictions' new commitments to a timeline to develop their regulatory frameworks (Graph N4B). The portion of non-FSB jurisdictions with a concrete implementation timeline is 63% and 51% for crypto-asset and stablecoin frameworks respectively, demonstrating that the FSB's recommendations are being widely recognised and adopted beyond its membership.

[120] Some jurisdictions need new legislation in order to reach alignment with the FSB framework. Typically, the legislation can come into force only after being passed in their legislative body, which is not within the control of the regulatory and supervisory authorities. This may be the reason why many FSB members cannot promise a date of alignment at the current stage.

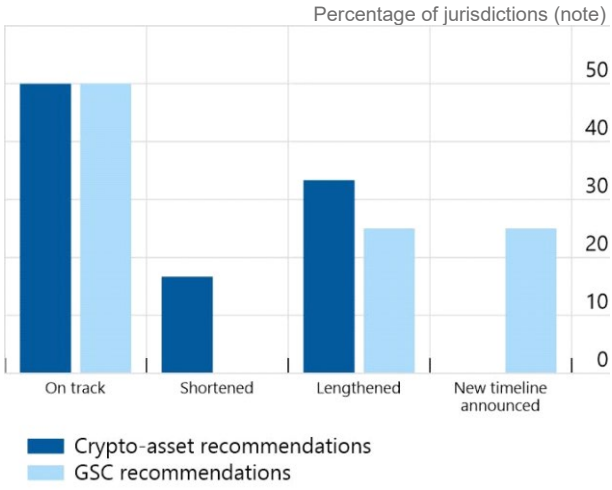
Expected time to reach alignment with FSB Framework

FSB member jurisdictions measured by effective date of rules, at year ends **Graph N3**

A. Expected time to reach alignment with FSB Framework



B. Changes to expected time since last reported in 2024



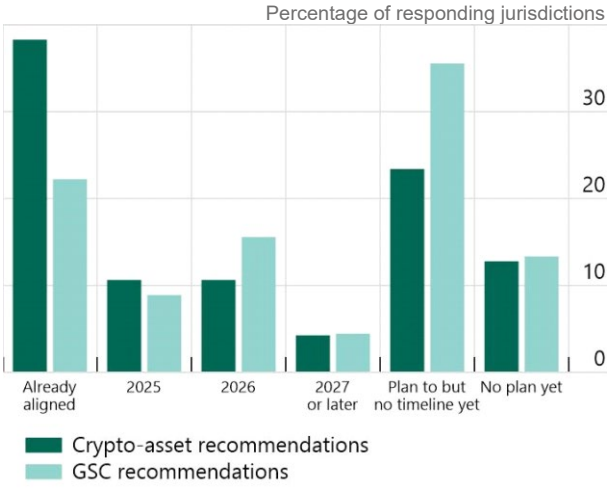
Note: For Graph N3B, only jurisdictions who meet all 3 criteria are represented: (i) reported to both the 2024 and 2025 surveys, (ii) have not reported alignment to FSB recommendations, and (iii) have announced a timeline in 2024 or 2025.

Source: FSB Survey

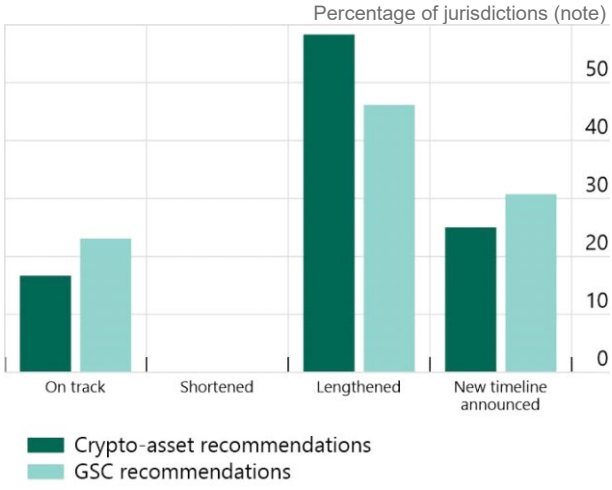
Expected time to reach alignment with FSB Framework

Non-FSB member jurisdictions measured by effective date of rules, at year ends **Graph N4**

A. Expected time to reach alignment with FSB Framework



B. Changes to expected time since last reported in 2024



Note: For Graph N4B, only jurisdictions who meet all 3 criteria are represented: (i) reported to both the 2024 and 2025 surveys, (ii) have not reported alignment to FSB recommendations, and (iii) have announced a timeline in 2024 or 2025.

Source: FSB Survey

Regulatory tools and requirements

In general, there are differences in regulatory tools and requirements applicable to CASPs and stablecoins due to their unique financial stability risk implications. In addition, there are also variations between tools adopted by FSB and non-FSB members, potentially reflecting divergence between policy objectives of advanced economies and EMDEs.[121]

Tools relating to AML/CFT, licensing/registration/authorisation, and fraud are consistently ranked amongst the most common requirements for both FSB and non-FSB members, and across crypto-asset and stablecoin frameworks (see Graphs N5A and N5B). For FSB members, there is a clear emphasis placed on designing requirements on anti-money laundering and consumer protection when compared to other tools, while the mix is more balanced for non-FSB members. These results suggest that there are various areas relating to financial stability in which FSB members still have gaps to reach full alignment with the FSB recommendations.

Comparing the survey results from 2024 surveys, the emphasis for implementing new regulatory requirements have changed over the past year, as implementation stages mature. For FSB members reporting GSC frameworks are partially or fully in place (Graph N5C), there is a clear shift of focus towards new requirements within stablecoin frameworks. Meanwhile, enhancements to crypto-asset frameworks have mainly focused on improving resolution and recovery planning (with 30% more members introducing such requirements over the past year). This is markedly different to non-FSB members (Graph N5D). While non-members continue to combat consumer protection and fraud (both with more than 50% non-FSB members adding to their regulatory frameworks over the past year), attention has also been on designing conduct and disclosure requirements (both with around 60% more non-FSB members adding these to their frameworks).

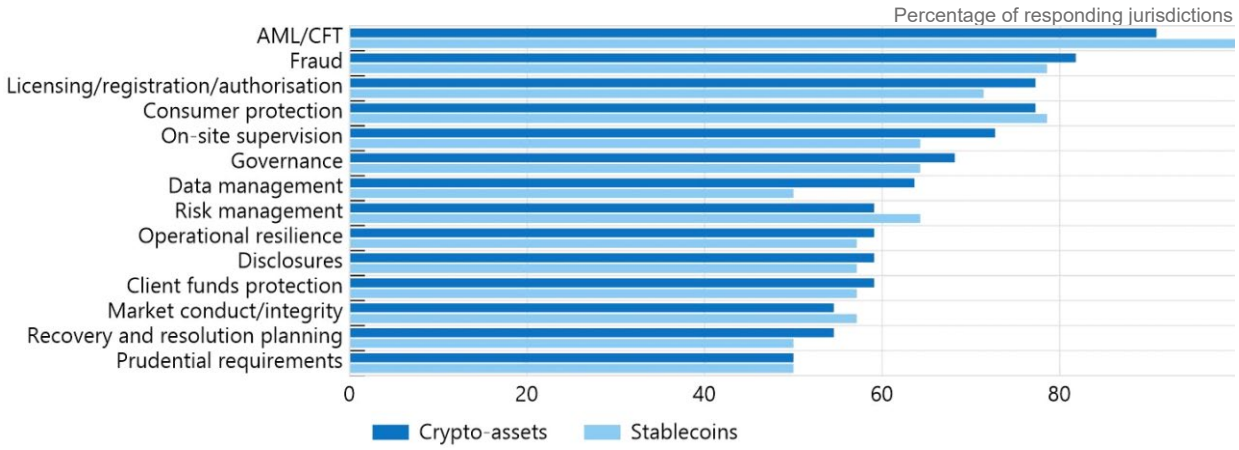
Such difference may be attributed to the varying stages of regulatory requirement developments. As FSB members have already established frameworks around consumer protection and fraud, they are progressing to the implementation of other requirements, while non-FSB members are still at an earlier stage. As the peer review report highlights, it is noteworthy that even for the same regulatory requirements, there are significant differences in the detailed design of the frameworks across jurisdictions, which are not reflected in the below charts.

[121] Based on the survey respondents, a majority of non-FSB members are EMDEs.

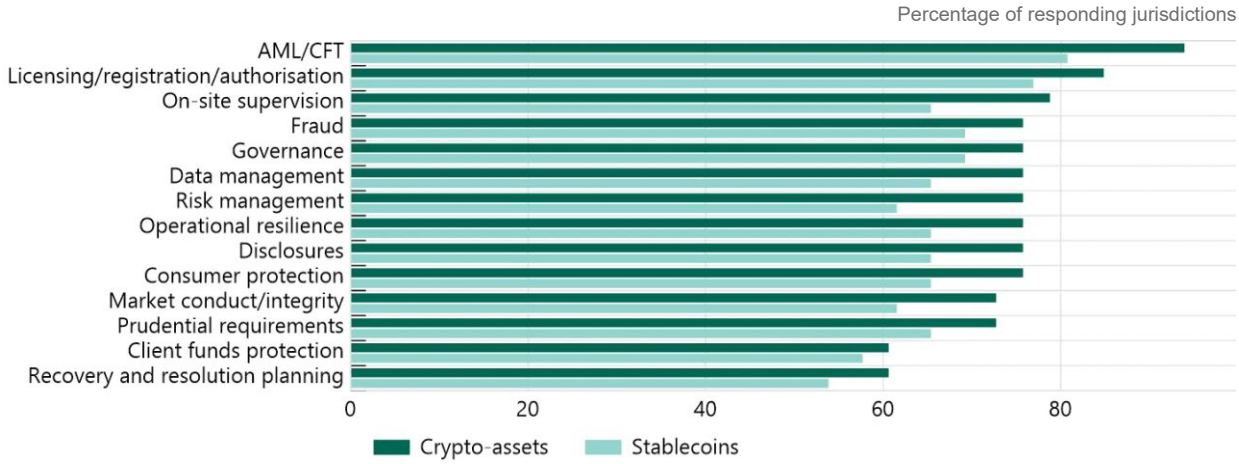
Regulatory requirements currently applied

For FSB and non-FSB member jurisdictions **Graph N5**

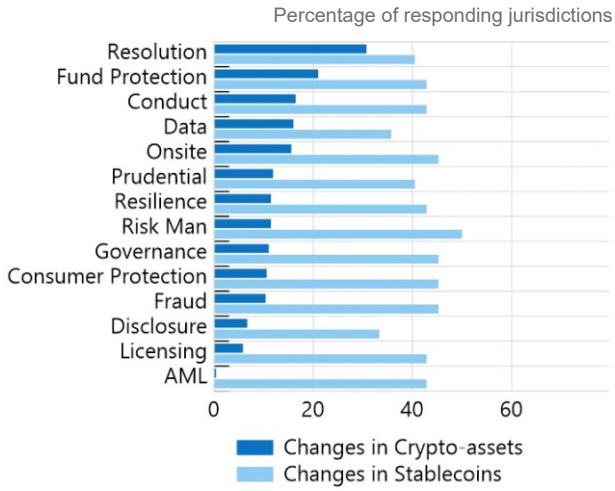
A. For FSB jurisdictions



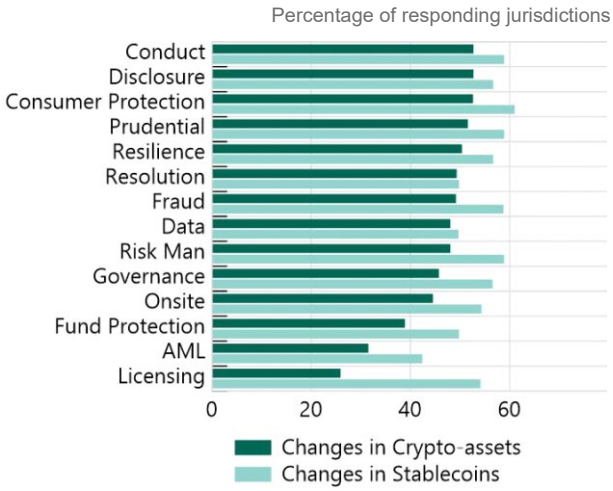
B. For non-FSB jurisdictions



C. Changes since 2024 for FSB jurisdictions



D. Changes since 2024 for non-FSB jurisdictions



Note: The respective percentages are calculated based on the pool of responding jurisdictions who have a partial or full crypto-asset and stablecoin framework in place. For Graphs N5C & N5D, only jurisdictions who (i) reported to both the 2024 and 2025 surveys and (ii) have partial or full implementation of crypto-asset or stablecoin frameworks are included.

Source: FSB Survey

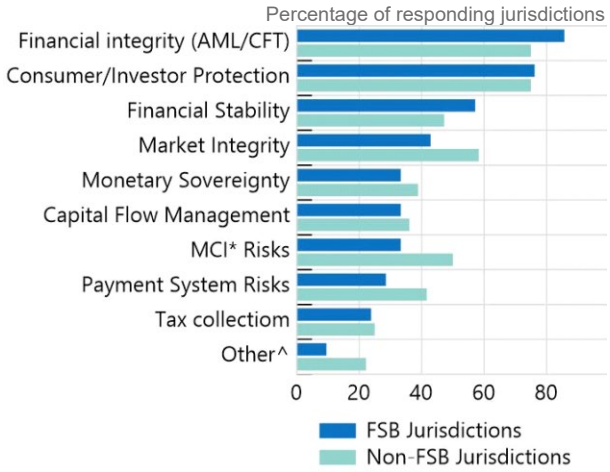
Risks of crypto-asset activities

FSB and non-FSB members continue to converge on the same top two risks - financial integrity and consumer protection, with over 75% of all respondents considering them as “very important”, same as the 2024 survey results (Graph N6A). For FSB members, financial stability risk has risen in importance and emerged as the third most considered risk (57%), while market integrity has become a lesser concern (Graph N6B). There are also shared concerns between FSB and non-FSB members on tax collection issues.

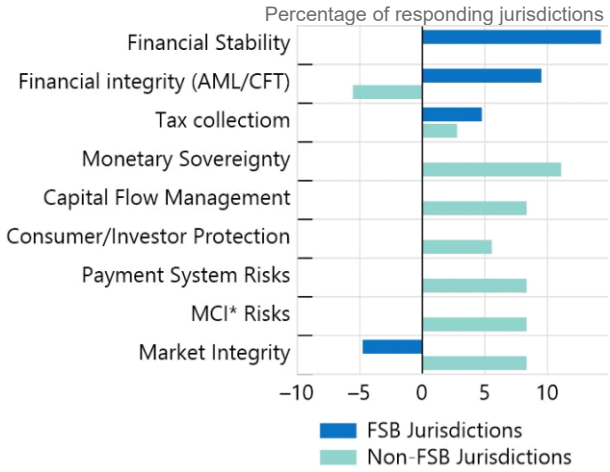
Key risk areas jurisdictions consider in relation to crypto-assets and stablecoins

For FSB members and non-FSB member jurisdictions **Graph N6**

A. Risk areas jurisdictions considered “very important”



B. Changes to risk areas being considered “very important” since last reported in 2024



* “MCIs” refer to Multifunction Crypto-asset Intermediaries.

^ “Other” includes cybersecurity risks and liquidity risks.

Note: Only jurisdictions who responded to both the 2024 and 2025 surveys are included.

Source: FSB Survey

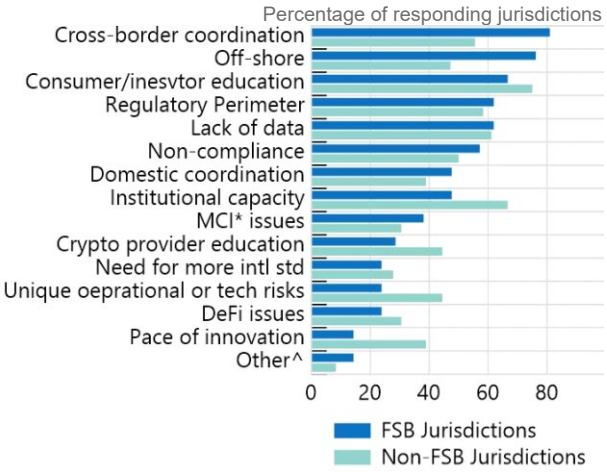
Implementation challenges

Unlike risks, FSB and non-FSB members diverge in their implementation challenges, most likely due to the differences in implementation progress and supervisory maturities. For FSB members with relatively mature frameworks (Graph N7A), their challenges rest in dealing with cross-border coordination (81%) and issues arising from off-shore service providers (76%). Meanwhile, for non-FSB members, their main challenges are on consumer education and institutional capacity (71% and 63% respectively), reflecting that EMDE generally face capacity constraints in monitoring and supervising crypto-asset firms and stablecoin issuers. There is a consensus between FSB and non-FSB members that data issues are gradually alleviated and that there is a markedly reduced need for more international standards, as the FSB recommendations are implemented by more jurisdictions globally (Graph N7B).

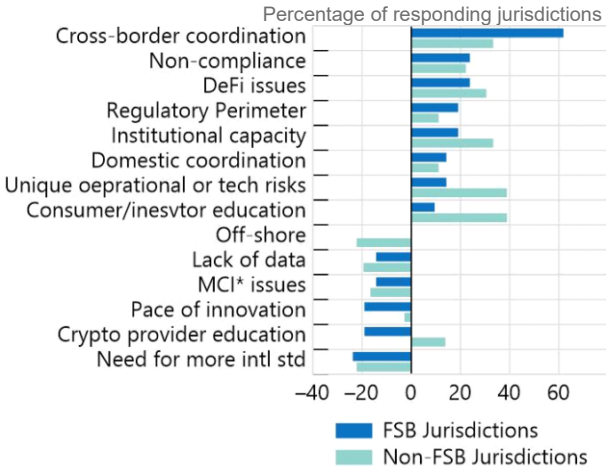
Key challenges jurisdictions consider in implementation of FSB Framework

For FSB members and non-FSB member jurisdictions **Graph N7**

A. Challenges jurisdictions considered "very important"



B. Changes to challenges being considered "very important" since last reported in 2024



* "MCIs" refer to Multifunction Crypto-asset Intermediaries.

^ "Other" includes challenges in processing on-chain data and potential interlinkages with regulated financial institutions.

Note: Only jurisdictions who responded to both the 2024 and 2025 surveys are included.

Source: FSB Survey

Annex 6: Summary of public feedback

The FSB invited feedback from the public on the areas covered by the peer review. 10 written responses were received. The main points raised in the written public feedback are summarised below, together with the highlights of a roundtable organised in London in July 2025.

Impact of Jurisdictional Regulatory Frameworks on Business Decisions

- Public feedback responses indicate that jurisdictional regulatory frameworks play a decisive role in shaping the location and structure of crypto-asset issuers and service providers, including stablecoin arrangements. Respondents emphasised that inconsistent and fragmented regulations create significant operational inefficiencies and compliance burdens, which deter innovation and investment. One respondent highlighted the challenges posed by wide variations in stablecoin reserve requirements. Jurisdictions mandating local reserve holdings or imposing rigid redemption timelines complicate cross-border operations, threatening the interoperability of stablecoins as global settlement assets. Another respondent echoed this concern, explaining that fragmented reserve requirements force issuers to fragment liquidity, creating localised variants of what are intended to be borderless payment instruments like USDC and EURC.

- The lack of harmonisation in how jurisdictions classify digital assets – as securities, commodities, or payment instruments – was seen as a major barrier to global operations from one respondent. They noted that this inconsistency not only increases compliance costs but also incentivises regulatory arbitrage, where businesses relocate to jurisdictions with less stringent requirements. For instance, a jurisdiction that classifies stablecoins as securities may impose disclosure and reporting requirements that differ significantly from a jurisdiction treating them as payment instruments, creating legal uncertainty for issuers. Another respondent added that jurisdictions with unclear or overly restrictive regulations risk deterring innovation, pushing crypto-asset activities to less-regulated markets, which could undermine consumer protection and systemic stability.

- Stakeholders advocated for globally coordinated, technology-neutral, and risk-based regulatory frameworks to address these challenges. Mutual recognition frameworks and passporting regimes, such as those under the EU's MiCAR framework, are widely supported as mechanisms to reduce compliance burdens and enable seamless cross-border operations. For example, MiCAR allows a single regulatory approval to facilitate access across all EU member states, providing a model for other jurisdictions to emulate. One stakeholder emphasised that jurisdictions with clear, proportionate regulations attract long-term investment and innovation while ensuring consumer protection. The submissions collectively argued that regulatory harmonisation is essential to fostering a level playing field in the inherently global crypto-asset ecosystem.

- Participants in the public outreach event highlighted the persistent challenge of regulatory fragmentation, with significant variations in frameworks across jurisdictions.

While frameworks like the EU's MiCAR are seen as comprehensive, stakeholders expressed concerns about their adaptability and the lack of mutual recognition mechanisms. EMDEs were noted to have differing risk priorities, necessitating tailored yet coordinated approaches. Stakeholders advocated for passporting regimes and reciprocity agreements to reduce compliance burdens and facilitate cross-border operations.

Experiences and Challenges Faced by Market Participants

- Crypto-asset market participants cited numerous challenges stemming from the fragmentation and inconsistency of global regulatory frameworks. Compliance costs, varied implementation of AML/KYC requirements, and cybersecurity concerns are among the most common hurdles identified by stakeholders. One respondent highlighted the inefficiencies introduced by jurisdiction-specific reserve mandates, which require stablecoin issuers to rebalance fiat-based reserves frequently across multiple jurisdictions, increasing operational risks and costs. Similarly, another pointed to vulnerabilities in custody practices, such as the lack of clear standards for key management and cybersecurity, which jeopardise the safety of client assets.

- One respondent identified specific operational challenges, including transaction monitoring, identity verification, and cross-chain risk management. It also raised concerns with different reporting requirements across jurisdictions, noting this can result in inefficiencies and increased costs for market participants. For example, firms operating in both the EU and the US must navigate differing AML/CFT thresholds and reporting obligations. Additionally, the same respondent critiqued certain regulatory treatments, such as the BCBS' 1250% risk-weighting for unbacked crypto-assets, as a significant deterrent to institutional participation in the crypto ecosystem. They noted that this treatment, which imposes high capital requirements on banks holding crypto-assets, discourages traditional financial institutions from engaging with the sector, limiting its scalability and stability.

- One respondent highlighted the need for a flexible, principles-based regulatory approach that accommodates rapidly evolving technologies. It noted challenges related to custody, reporting, and record-keeping requirements, particularly for tokenised assets, which often do not align with traditional prudential reporting frameworks. For instance, regulated financial institutions may face additional regulatory scrutiny for using blockchain based technologies for record keeping or other non-transaction, non-client facing activities. Another respondent added that emerging markets face additional challenges, such as limited access to technical infrastructure and banking facilities, which further complicate compliance efforts. All respondents stressed the importance of clear and consistent definitions for digital assets to mitigate these challenges and reduce compliance burdens.

- Licensing and registration processes in some jurisdictions were highlighted as overly complex, particularly for banks. Stakeholders noted that existing risk management frameworks are often sufficient for most digital asset risks, but regulators still require extensive, crypto-specific tailoring. This was seen as introducing unnecessary delays and costs, particularly for institutions already operating within established frameworks.

Financial Stability Vulnerabilities Across Jurisdictions

- Stakeholders highlight that financial stability vulnerabilities associated with crypto-asset activities, including stablecoins, vary significantly across jurisdictions based on the scale and materiality of adoption. In jurisdictions where stablecoins are more widely used for retail payments or remittances, disruptions could pose systemic risks, particularly during stress events such as a de-pegging or liquidity crisis. One respondent warned that local reserve mandates and jurisdiction-specific requirements could fragment stablecoin fungibility, undermining their role as global payment instruments. For example, a stablecoin issuer required to hold reserves in local currency across multiple jurisdictions may struggle to meet redemption demands during periods of market volatility, exposing holders to liquidity risks.

- Other respondents noted that inadequate reserve management standards in some jurisdictions could exacerbate vulnerabilities, particularly if reserves are not held in high-quality liquid assets. For instance, jurisdictions allowing stablecoin issuers to back their tokens with less liquid or riskier assets may increase the likelihood of redemption delays or de-pegging events. Respondents emphasised the importance of harmonised standards for reserve management and redemption timelines to ensure stablecoin liquidity and reliability.

- Respondents noted that current financial stability risks from crypto-assets remain limited due to the relatively small scale and lack of interconnectedness with traditional financial systems. One response highlighted additional risks, such as geographical concentration of crypto activity, lack of transparency in institutional exposures, and collateral practices, which could amplify vulnerabilities as the market grows. For example, the concentration of global crypto activity in a few jurisdictions with regulatory clarity could create single points of failure if those jurisdictions experience sudden policy changes or financial crises. All stakeholders emphasised the need for proactive risk monitoring as adoption increases, particularly in areas like leverage, collateral rehypothecation, and cyber threats to client assets.

- Stakeholders emphasised the critical role banks can play in ensuring the safety and stability of stablecoins. Suggestions included the formation of bank consortia to jointly issue stablecoins and the eligibility of stablecoins as collateral at central banks to enhance their utility during times of stress. Diverging reserve and redemption requirements across jurisdictions were identified as key challenges, with calls for harmonised standards to prevent fragmentation of global liquidity.

Market Practices and Trends That Pose Financial Stability Risks

- Specific market practices and trends in certain geographies and segments are identified as potential threats to financial stability. Respondents highlighted the rapid growth of DeFi as an area requiring close monitoring of market developments. Others pointed to vulnerabilities such as smart contract risks, market manipulation, and operational failures, which could become systemic as DeFi continues to scale.

- One respondent added that the absence of central intermediaries in DeFi platforms poses unique regulatory challenges, particularly in enforcing accountability and ensuring consumer protection. At the same time, some warned about the concentration of liquidity and trading activity on a small number of centralised exchanges, which could amplify systemic risks in the event of operational or cybersecurity failures. For instance, the collapse of a major exchange due to a cyberattack or insolvency could disrupt market liquidity and erode investor confidence.

- Regional "hot spots," where jurisdictions position themselves as crypto hubs with minimal oversight, were highlighted as another area of concern as these hubs may enable excessive leverage and opaque cross-entity exposures, increasing systemic vulnerabilities. Suggestions to addressing these risks included targeted supervisory cooperation and early-warning systems, leveraging supervisory technology and blockchain analytics to enhance market oversight, and for regulators to adopt new technologies, such as hosting blockchain nodes to extract trade reporting data directly, reducing reliance on outdated systems and improving oversight.

- DeFi was recognised as a rapidly growing area requiring close monitoring of market developments. Stakeholders called for regulatory approaches that address risks such as smart contract vulnerabilities and market manipulation without stifling innovation. Distributed key management and multi-jurisdictional custody arrangements were identified as safer alternatives to localised custody, underscoring the benefits of clearer standards in this area.

Abbreviations

ACPR	Autorité de Contrôle Prudentiel et de Résolution (France)
AFM	Authority for the Financial Markets (Netherlands)
AMF	Autorité des marchés financiers (France)
AML/CFT	Anti-money laundering and counter-terrorist financing
APRA	Australian Prudential Regulation Authority
APRC	Asia-Pacific Regional Committee (IOSCO)
ARTs	Asset-referenced tokens (MiCAR)
ASIC	Australian Securities and Investments Commission
ASSAL	Association of Insurance Supervisors of Latin America
BaFin	Federal Financial Supervisory Authority
BdE	Banco de España
BdI	Banca d'Italia
BCB	Banco Central do Brasil
BCBS	Basel Committee for Banking Supervision
BCCh	Central Bank of Chile
BCU	Banco Central del Uruguay
BMA	Bermuda Monetary Authority
BoE	Bank of England
BOK	Bank of Korea
BSP	Bangko Sentral ng Pilipinas
CA recommendations	High-level recommendations for the regulation, supervision and oversight of crypto-asset activities and markets (FSB)
CASP	Crypto-asset service provider
CBA	Central Bank of Armenia
CBI	Central Bank of Ireland
CMB	Capital Markets Board (Türkiye)
CMF	Comisión para el Mercado Financiero (Financial Market Commission) (Chile)
CNMV	Comisión Nacional del Mercado de Valores (Spain)
CNV	National Securities and Exchange Commission (Argentina)
CONSOB	Commissione Nazionale per le Società e la Borsa (Italy)
CSA	Canadian Securities Administrators
DeFi	Decentralised finance
DNB	De Nederlandsche Bank

EBA	European Banking Authority (EU)
ECB	European Central Bank
EMMoU	Enhanced MMoU (IOSCO)
EMT	Electronic money token (MiCAR)
ESMA	European Securities and Markets Authority (EU)
ETPs	Exchange-traded products
EU	European Union
FATF	Financial Action Task Force
FCA	Financial Conduct Authority (UK)
FDIC	Federal Deposit Insurance Corporation (US)
FINMA	Swiss Financial Market Supervisory Authority
FRB	Federal Reserve Board (US)
FSA	Financial Services Agency (Japan)
FSB	Financial Stability Board
FSC	Financial Services Commission (Korea)
FSCA	Financial Sector Conduct Authority (South Africa)
FSS	Financial Supervisory Service (Korea)
GSC	Global stablecoin
GSC recommendations	High-level recommendations for the regulation, supervision and oversight of global stablecoin arrangements (FSB)
HKMA	Hong Kong Monetary Authority
HMT	His Majesty's Treasury (UK)
IDR	Indonesian Rupiah
IIMV	Ibero-American Securities Markets Institute
IMF	International Monetary Fund
IOSCO	International Organization of Securities Commissions
IT	Information Technology
JPY	Japanese Yen
MAS	Monetary Authority of Singapore
MoF	Ministry of Finance (Thailand)
MiCAR	Markets in Crypto-Assets Regulation (EU)
MiFID	Markets in Financial Instruments Directive (EU)
MoU	Memorandum of Understanding
MMoU	Multilateral MoU

MNB	Central Bank of Hungary
NCA	National competent authority (MiCAR)
NCUA	National Credit Union Administration (NCUA)
OCC	Office of the Comptroller of the Currency (US)
OJK	Indonesia Financial Services Agency (Otoritas Jasa Keuangan)
SCB	Securities Commission of The Bahamas
SCSI	Standing Committee on Standards Implementation (FSB)
SEC	Securities and Exchange Commission (Nigeria)
SEC	Securities and Exchange Commission (Philippines)
SEC	Securities and Exchange Commission (Thailand)
SFC	Securities and Futures Commission (Hong Kong)
SSB	Standard-setting body
SSF	Superintendencia de Servicios Financieros (Uruguay)
TRY	Turkish lira
UK	United Kingdom
US	United States
USD	US dollar
VASP	Virtual asset service provider (FATF)