International Association of Potential, New and Sitting Members
of the Board of Directors (IAMBD)
1200 G Street NW Suite 800, Washington DC, 20005-6705 USA
Tel: 202-449-9750 Web: www.iambd.org

News for the Board of Directors, January 2023

Dear members and friends,

The Securities and Exchange Commission proposed a rule to implement Section 27B of the Securities Act of 1933, a provision added by Section 621 of the Dodd-Frank Act.

The rule is intended to prevent the sale of asset-backed securities (ABS) that are tainted by material conflicts of interest.

Specifically, the rule would prohibit securitization participants from engaging in certain transactions that could incentivize a securitization participant to structure an ABS in a way that would put the securitization participant's interests ahead of those of ABS investors.

The Commission originally proposed a rule to implement Section 27B in September 2011.

"I am pleased to support this re-proposed rule as it fulfills Congress's mandate to address conflicts of interests in the securitization market, which contributed to the 2008 financial crisis," said SEC Chair Gary Gensler.

"This re-proposed rule is designed to help address conflicts of interest arising with market participants taking positions against investors' interests. Further, as required by Section 621 of the Dodd-Frank Act, the re-proposed rule provides exceptions for risk-mitigating hedging activities, bona fide market making, and certain liquidity commitments. These changes, taken together, would benefit investors and our markets."

If adopted, new Securities Act Rule 192 would prohibit an underwriter, placement agent, initial purchaser, or sponsor of an ABS, including affiliates or subsidiaries of those entities, from engaging, directly or indirectly, in any transaction that would involve or result in any material conflict of interest between the securitization participant and an investor in such ABS.

Under the proposed rule, such transactions would be "conflicted transactions." They include, for example, a short sale of the ABS or the purchase of a credit default swap or other credit derivative that entitles the securitization participant to receive payments upon the occurrence of specified credit events in respect of the ABS.

The prohibition on conflicted transactions would commence on the date on which a person has reached, or has taken substantial steps to reach, an agreement that such person will become a securitization participant with respect to an ABS, and it would end one year after the date of the first closing of the sale of the relevant ABS.

The proposed rule would provide certain exceptions for risk-mitigating hedging activities, bona fide market-making activities, and certain commitments by a securitization participant to provide liquidity for the relevant ABS.

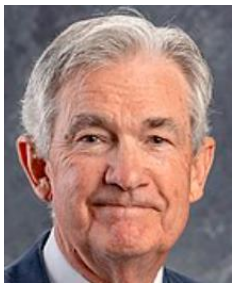
The proposed exceptions would focus on distinguishing the characteristics of such activities from speculative trading. The proposed exceptions would also seek to avoid disrupting current liquidity commitment, market-making, and balance sheet management activities.

The public comment period will remain open for 60 days following publication of the proposing release on the SEC's website or 30 days following publication of the proposing release in the Federal Register, whichever period is longer.

To read more: https://www.sec.gov/news/press-release/2023-17

Panel on "Central Bank Independence and the Mandate—Evolving Views"

Chair Jerome H. Powell, at the Symposium on Central Bank Independence, Sveriges Riksbank, Stockholm, Sweden



I will address three main points.

First, the Federal Reserve's monetary policy independence is an important and broadly supported institutional arrangement that has served the American public well.

Second, the Fed must continuously earn that independence by using our tools to achieve our assigned goals of maximum employment and price stability, and by providing transparency to facilitate understanding and effective oversight by the public and their elected representatives in Congress.

Third, we should "stick to our knitting" and not wander off to pursue perceived social benefits that are not tightly linked to our statutory goals and authorities.

Central bank independence and transparency

On the first point, the case for monetary policy independence lies in the benefits of insulating monetary policy decisions from short-term political considerations.

Price stability is the bedrock of a healthy economy and provides the public with immeasurable benefits over time. But restoring price stability when inflation is high can require measures that are not popular in the short term as we raise interest rates to slow the economy.

The absence of direct political control over our decisions allows us to take these necessary measures without considering short-term political factors. I believe that the benefits of independent monetary policy in the U.S. context are well understood and broadly accepted.

In a well-functioning democracy, important public policy decisions should be made, in almost all cases, by the elected branches of government.

Grants of independence to agencies should be exceedingly rare, explicit, tightly circumscribed, and limited to those issues that clearly warrant protection from short-term political considerations.

With independence comes the responsibility to provide the transparency that enables effective oversight by Congress, which, in turn, supports the Fed's democratic legitimacy.

At the Fed, we treat this as an active, not passive, responsibility, and over the past several decades we have steadily broadened our efforts to provide meaningful transparency about the basis for, and consequences of, the decisions we make in service to the American public.

We are tightly focused on achieving our statutory mandate and on providing useful and appropriate transparency.

Sticking to our mandate

It is essential that we stick to our statutory goals and authorities, and that we resist the temptation to broaden our scope to address other important social issues of the day. Taking on new goals, however worthy, without a clear statutory mandate would undermine the case for our independence.

In the area of bank regulation, too, the Fed has a degree of independence, as do the other federal bank regulators. Independence in this area helps ensure that the public can be confident that our supervisory decisions are not influenced by political considerations.

Today, some analysts ask whether incorporating into bank supervision the perceived risks associated with climate change is appropriate, wise, and consistent with our existing mandates.

Addressing climate change seems likely to require policies that would have significant distributional and other effects on companies, industries, regions, and nations. Decisions about policies to directly address climate change should be made by the elected branches of government and thus reflect the public's will as expressed through elections.

At the same time, in my view, the Fed does have narrow, but important, responsibilities regarding climate-related financial risks. These responsibilities are tightly linked to our responsibilities for bank supervision.

The public reasonably expects supervisors to require that banks understand, and appropriately manage, their material risks, including the financial risks of climate change.

But without explicit congressional legislation, it would be inappropriate for us to use our monetary policy or supervisory tools to promote a greener economy or to achieve other climate-based goals.7 We are not, and will not be, a "climate policymaker."

To read more:
https://www.federalreserve.gov/newsevents/speech/powell20230110a.htm

Agencies issue joint statement on crypto-asset risks to banking organizations

Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency

The Board of Governors of the Federal Reserve System (Federal Reserve), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) (collectively, the agencies) are issuing the following statement on crypto-asset1 risks to banking organizations.

The events of the past year have been marked by significant volatility and the exposure of vulnerabilities in the crypto-asset sector. These events highlight a number of key risks associated with crypto-assets and crypto-asset sector participants that banking organizations should be aware of, including:

- Risk of fraud and scams among crypto-asset sector participants.

- Legal uncertainties related to custody practices, redemptions, and ownership rights, some of which are currently the subject of legal processes and proceedings.

- Inaccurate or misleading representations and disclosures by crypto-asset companies, including misrepresentations regarding federal deposit insurance, and other practices that may be unfair, deceptive, or abusive, contributing to significant harm to retail and institutional investors, customers, and counterparties.

- Significant volatility in crypto-asset markets, the effects of which include potential impacts on deposit flows associated with crypto-asset companies.

- Susceptibility of stablecoins to run risk, creating potential deposit outflows for banking organizations that hold stablecoin reserves.

- Contagion risk within the crypto-asset sector resulting from interconnections among certain crypto-asset participants, including through opaque lending, investing, funding, service, and operational arrangements. These interconnections may also present concentration risks for banking organizations with exposures to the crypto-asset sector.

- Risk management and governance practices in the crypto-asset sector exhibiting a lack of maturity and robustness.

- Heightened risks associated with open, public, and/or decentralized networks, or similar systems, including, but not limited to, the lack of governance mechanisms establishing oversight of the system; the absence of contracts or standards to clearly establish roles, responsibilities, and liabilities; and vulnerabilities related to cyber-attacks, outages, lost or trapped assets, and illicit finance.

It is important that risks related to the crypto-asset sector that cannot be mitigated or controlled do not migrate to the banking system. The agencies are supervising banking organizations that may be exposed to risks stemming from the crypto-asset sector and carefully reviewing any proposals from banking organizations to engage in activities that involve crypto-assets.

Through the agencies' case-by-case approaches to date, the agencies continue to build knowledge, expertise, and understanding of the risks crypto-assets may pose to banking organizations, their customers, and the broader U.S. financial system.

Given the significant risks highlighted by recent failures of several large crypto-asset companies, the agencies continue to take a careful and cautious approach related to current or proposed crypto-asset-related activities and exposures at each banking organization.

To read more:
https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20230103a1.pdf

Addressing the risks in crypto: laying out the options

Matteo Aquilina, Jon Frost and Andreas Schrimpf

BIS

Key takeaways

• The recent high-profile failures of FTX and other crypto firms have re-ignited the debate on the appropriate policy response to address the risks in crypto, including through regulation.

• The "shadow financial" functions enabled by crypto markets share many of the vulnerabilities of traditional finance. These risks are exacerbated by specific features of crypto.

• Authorities may consider different – not mutually exclusive – lines of action to tackle the risks in crypto. These include containment or regulation of the crypto sector or an outright ban.

• Central banks and public authorities could also work to make TradFi more attractive. A key option is to encourage sound innovation with central bank digital currencies (CBDCs).

After the failure of several major crypto firms, addressing the risks from crypto markets has become a more pressing policy issue.

Cryptoasset markets have gone through booms and busts before, and so far, the busts have not led to wider contagion threatening financial stability. Yet the scale and prominence of recent failures heighten the urgency of addressing these risks before crypto markets become systemic.

The crypto ecosystem and the "shadow financial" functions it engages in, through centralised financial entities (CeFi) and decentralised finance (DeFi) protocols, share many of the vulnerabilities that are familiar from traditional finance (TradFi).

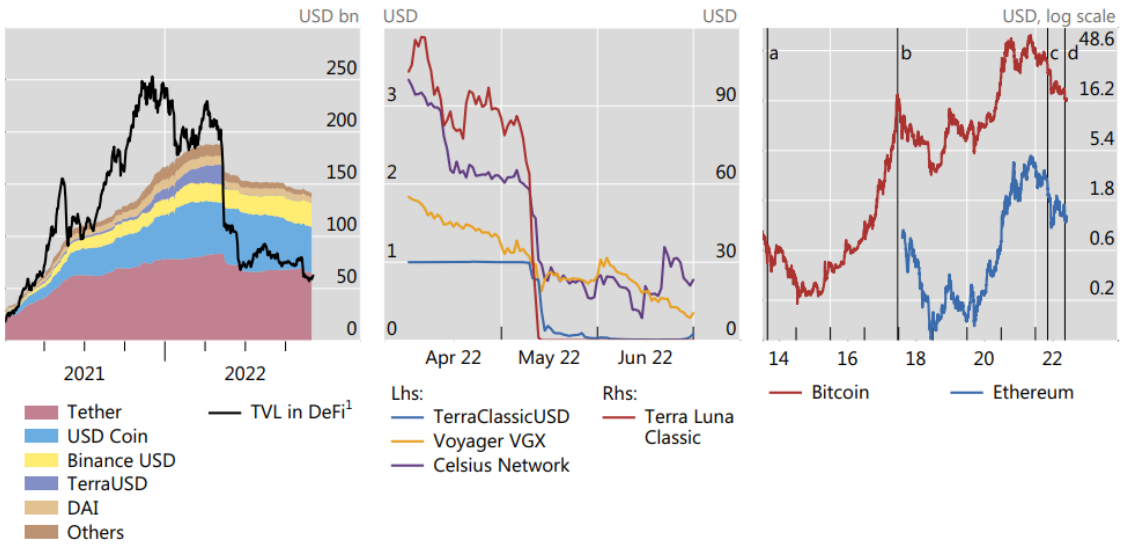
But several factors exacerbate the standard risks. These relate to high leverage, liquidity and maturity mismatches and substantial information asymmetries. Policy responses should consider how to address these sources of risk appropriately, given the borderless nature of crypto.

This bulletin briefly summarises the lessons of the 2022 turmoil. It then outlines three – non-mutually exclusive – lines of action to address the risks in crypto: a ban, containment and regulation, as well as their pros and cons. It also outlines complementary lines of policy action to address inefficiencies in TradFi and curb the demand for crypto.

One key option would be to encourage sound innovation with CBDCs. An online appendix gives a selective overview of ongoing initiatives in crypto regulation.

The recent crypto turmoil: features and lessons

Prices and market capitalisation of crypto assets and the 2022 turmoil — Graph 1



[a] Bankruptcy of Mt Gox on 28 February 2014. [b] Bursting of ICO bubble on 22 December 2017. [c] TerraUSD implosion on 9 May 2022. [d] Bankruptcy of FTX on 11 November 2022.

[1] TVL (total value locked) refers to the total dollar amount of assets that is staked across all DeFi protocols. It does not refer to transaction volumes or the market capitalisation of cryptocurrencies, but rather to the value of reserves that are "locked" into smart contracts. The TVL may vary depending upon the source and is subject to overestimation.

Sources: Bloomberg; CoinGecko; DefiLlama.

After peaking in late 2021, when cryptoasset prices, stablecoin volumes and DeFi activity reached all-time highs (Graph 1, left-hand panel), the crypto ecosystem faced turmoil in 2022.

The decline started early in the year, but problems became acute in May. It was then that a large stablecoin, TerraUSD (UST) – which relied on an algorithm to maintain its peg to the US dollar – collapsed, causing contagion in crypto markets (Graph 1, centre panel).

A period of relative calm followed, but crypto markets again saw serious stress in November 2022, when the FTX crypto trading platform declared bankruptcy. In the past, despite repeated turmoil, the crypto ecosystem has survived and prices have often recovered (Graph 1, right-hand panel).

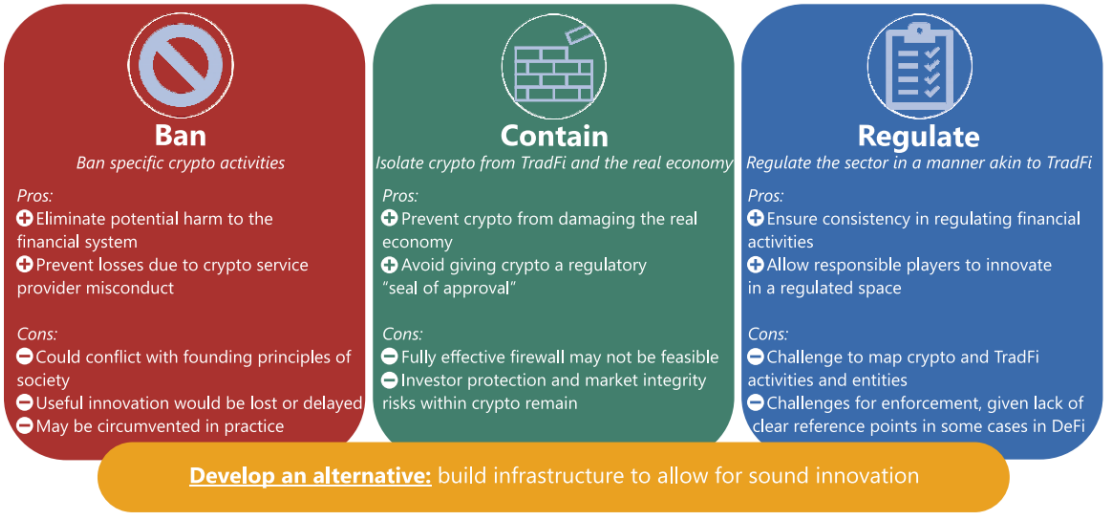
There are thus reasons to doubt that crypto will fade away on its own. In particular, a substantial part of the crypto community firmly believes in the ideological pursuit of a decentralised system as an alternative to TradFi.

And in response to recent events, many proponents of crypto claim that decentralisation and the underlying crypto technology are the solution rather than the problem.

They argue that while CeFi entities like FTX were at the epicentre of the stress, DeFi protocols and underlying blockchains continued to function, concluding that only "true" DeFi can be resilient.1

To read more: https://www.bis.org/publ/bisbull66.pdf

Options for addressing the risks in crypto: pros and cons Graph 2



Public responses to consultation on achieving greater convergence in cyber incident reporting

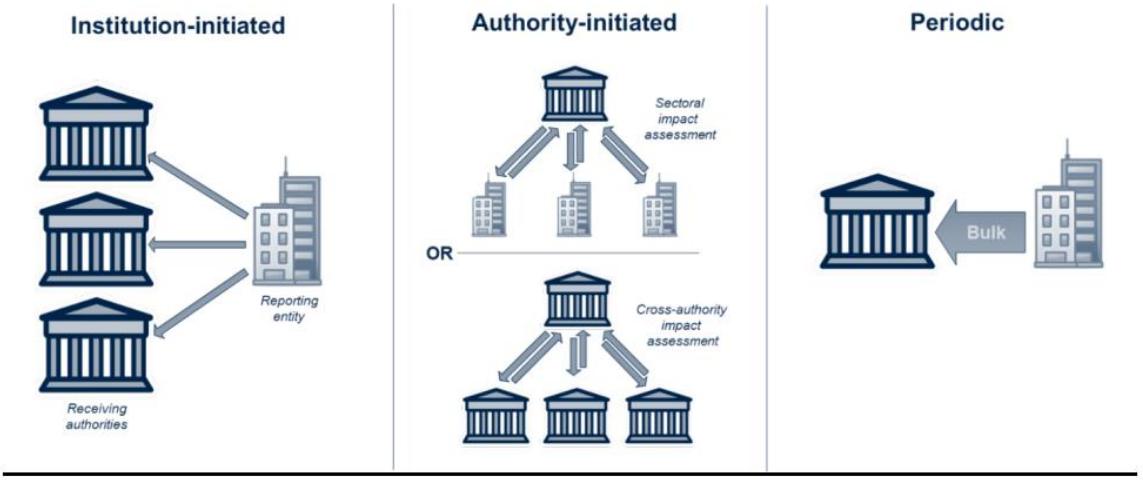
On 17 October 2022, the FSB published Achieving Greater Convergence in Cyber Incident Reporting – Consultative document. You may visit: https://www.fsb.org/2022/10/achieving-greater-convergence-in-cyber-incident-reporting-consultative-document/

FSB FINANCIAL STABILITY BOARD

Achieving Greater Convergence in Cyber Incident Reporting

Consultative Document

Illustration of reporting types Figure 6

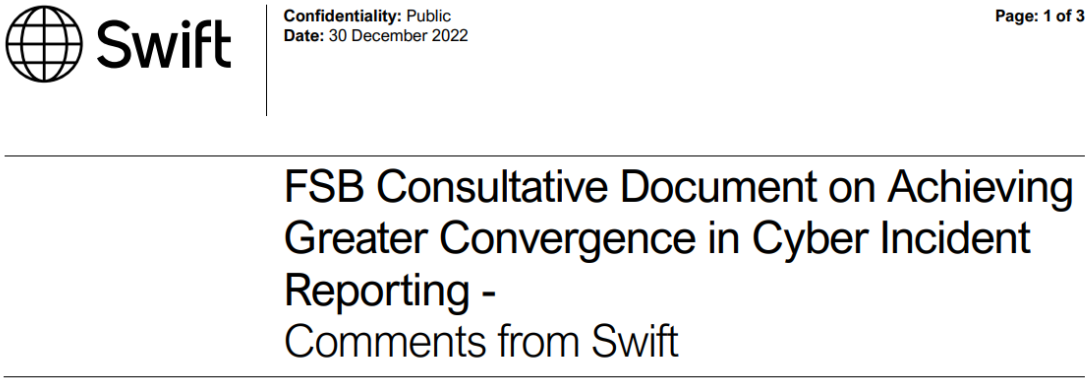


Interested parties were invited to provide written comments by 31 December 2022. The public comments received are available below.

The FSB thanks those who took the time and effort to express their views. The FSB expects to publish the final report in April 2023.

We have very interesting responses from:

- Banking Association of South Africa
- EBA Clearing
- European Banking Federation
- Financial Services Sector Coordinating Council
- German Banking Industry Committee
- Global Financial Markets Association
- Global Legal Entity Identifier Foundation
- Google Cloud
- Institute of International Finance
- Insurance Europe
- Intesa Sanpaolo
- NASDAQ
- SWIFT
- Swiss Insurance Association
- UK Finance
- Unipol
- World Council
- World Federation of Exchanges


Swift

Confidentiality: Public
Date: 30 December 2022

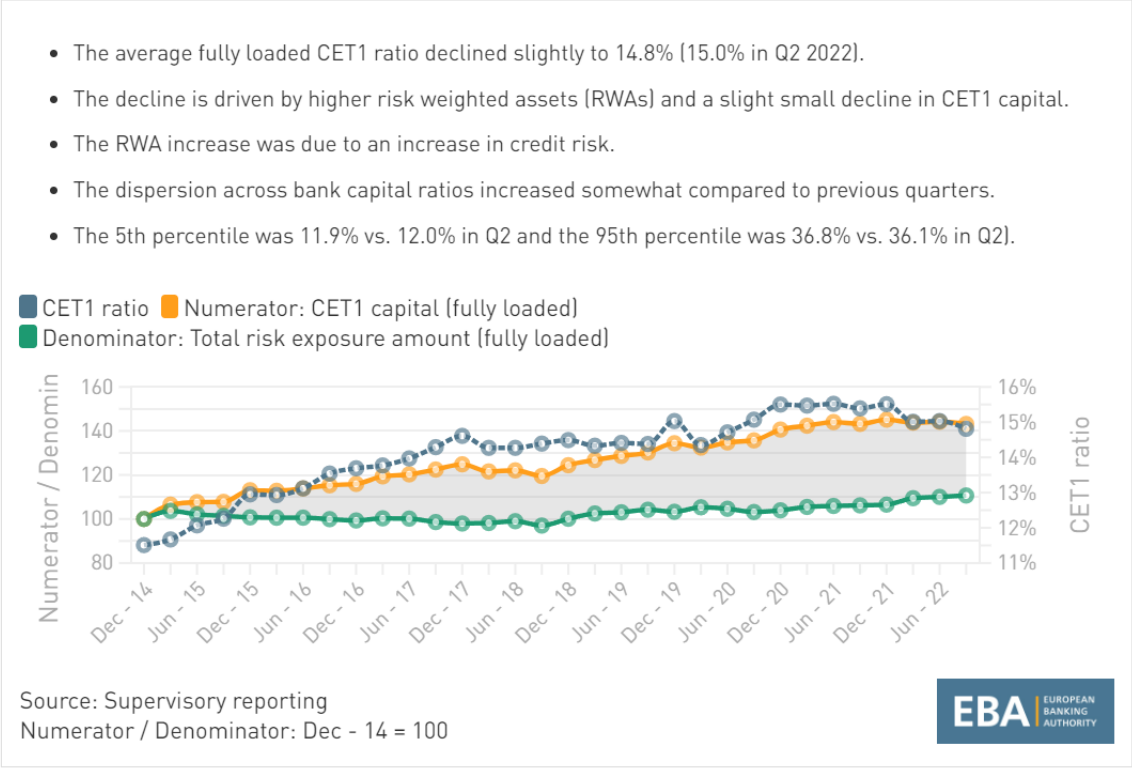
Page: 1 of 3

FSB Consultative Document on Achieving Greater Convergence in Cyber Incident Reporting -
Comments from Swift

To read more: https://www.fsb.org/2023/01/public-responses-to-consultation-on-achieving-greater-convergence-in-cyber-incident-reporting/

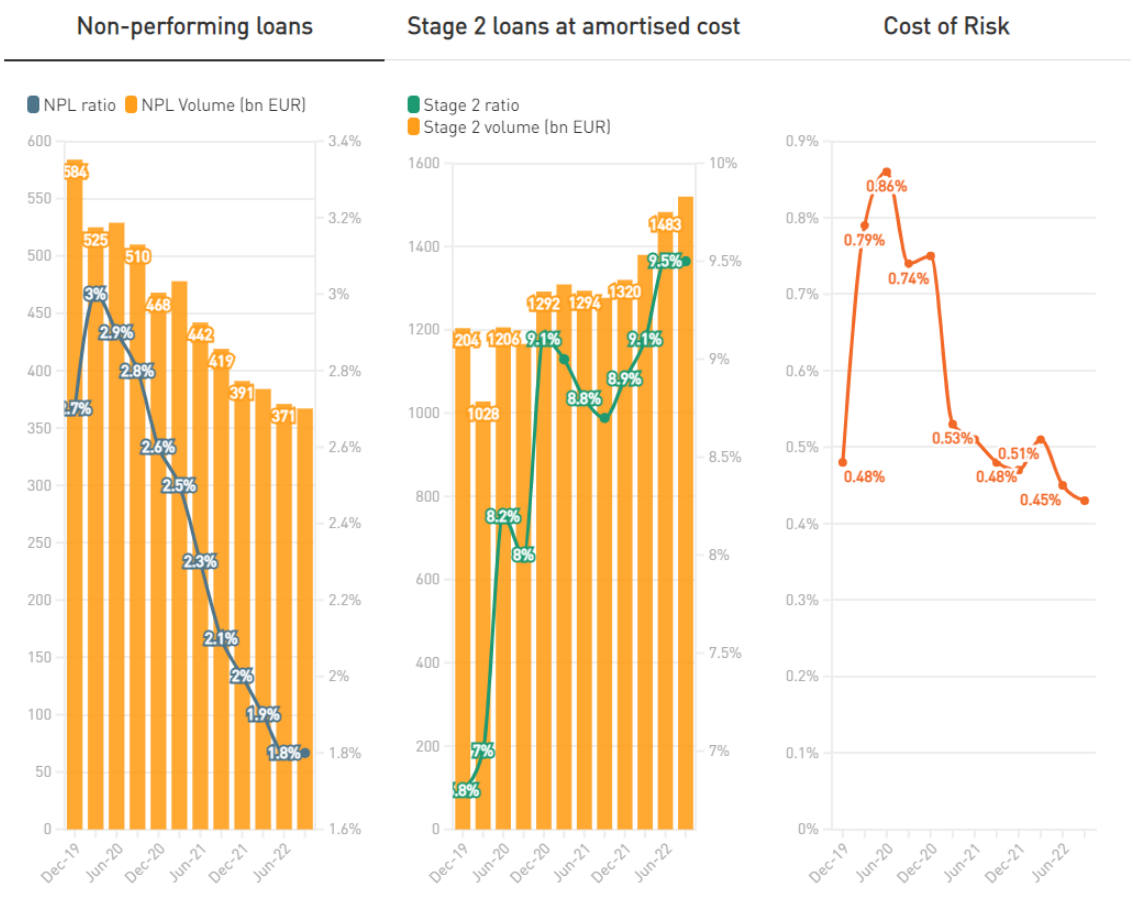
EBA Risk Dashboard shows that capital and liquidity ratios remain robust

The European Banking Authority (EBA) published its quarterly Risk Dashboard together with the results of the autumn edition of the Risk Assessment Questionnaire (RAQ).



- Overall, banks maintain robust capital and liquidity ratios.
- The average Common Equity Tier 1 (CET1) ratio declined slightly to 14.8% from 15% in the previous quarter on a fully loaded basis.
- The average Liquidity Coverage Ratio (LCR) reached 162.5% (164.9% in Q2 2022) while the average Net Stable Funding Ratio (NSFR) remained at 126.9%.
- The non-performing loan (NPL) ratio declined slightly to just below 1.8%. However, banks' asset quality expectations have further deteriorated, notably for SME and consumer finance.
- Average return on equity (RoE) remains stable supported by increases in net interest income
- Banks and analysts remain optimistic about profitability prospects.

- EU Taxonomy used by banks engaged in green lending



To read more: https://www.eba.europa.eu/eba-risk-dashboard-shows-capital-and-liquidity-ratios-remain-robust

Wi-Fi Could Help Identify When You're Struggling to Breathe

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Wi-Fi routers continuously broadcast radio frequencies that your phones, tablets and computers pick up and use to get you online. As the invisible frequencies travel, they bounce off or pass through everything around them — the walls, the furniture and even you.

Your movements, even breathing, slightly alter the signal's path from the router to your device.

Those interactions don't interrupt your internet connection, but they could signal when someone is in trouble. NIST has developed a deep learning algorithm, called BreatheSmart, that can analyze those minuscule changes to help determine whether someone in the room is struggling to breathe. And it can do so with already available Wi-Fi routers and devices. This work was recently published in IEEE Access.

In 2020 NIST scientists wanted to help doctors fight the COVID-19 pandemic.

Patients were isolated; ventilators were scarce. Previous research had explored using Wi-Fi signals to sense people or movement, but these setups often required custom sensing devices, and data from these studies were very limited.

"As everybody's world was turned upside down, several of us at NIST were thinking about what we could do to help out," says Jason Coder, who leads NIST's research in shared spectrum metrology. "We didn't have time to develop a new device, so how can we use what we already have?"

Working with colleagues at the Office of Science and Engineering Labs (OSEL) in the FDA's Center for Devices and Radiological Health, Coder and research associate Susanna Mosleh advanced a new way to use existing Wi-Fi routers to measure the breathing rate of a person in the room.

In Wi-Fi, the "channel state information," or CSI, is a set of signals sent from the client (such as a cellphone or laptop) to the access point (such as the router).

The CSI signal sent by the client device is always the same, and the access point receiving the CSI signals knows what it should look like. But as the CSI signals travel through the environment, they get distorted as they bounce off things or lose strength. The access point analyzes the amount of distortion to adjust and optimize the link.

These CSI streams are small, less than a kilobyte, so it doesn't interfere with the flow of data over the channel. The team modified the firmware on the router to ask for these CSI streams more frequently, up to 10 times per second, to get a detailed picture of how the signal was changing.

They set up a manikin used to train medical professionals in an anechoic chamber with a commercial off-the-shelf Wi-Fi router and receiver.

This manikin is designed to replicate several breathing conditions, from normal respiration to abnormally slow breathing (called bradypnea), abnormally rapid breathing (tachypnea), asthma, pneumonia and chronic obstructive pulmonary diseases, or COPD.

What alters the Wi-Fi signal is the way the body moves as we breathe. Think of how your chest moves differently when you are wheezing or coughing, compared with breathing normally.

As the manikin "breathed," the movement of its chest altered the path traveled by the Wi-Fi signal. The team members recorded the data provided by the CSI streams.

Although they collected a wealth of data, they still needed help to make sense of what they had gathered.

"This is where we can leverage deep learning," Coder said.

Deep learning is a subset of artificial intelligence, a type of machine learning that mimics humans' ability to learn from their past actions and improves the machine's ability to recognize patterns and analyze new data.

Mosleh worked on a deep learning algorithm to comb through the CSI data, understand it, and recognize patterns that indicated different breathing problems.

The algorithm, which they named BreatheSmart, successfully classified a variety of respiratory patterns simulated with the manikin 99.54% of the time.

"Most of the work that's been done before was working with very limited data," Mosleh says. "We were able to collect data with a lot of simulated respiratory scenarios, which contributes to the diversity of the training set that was available to the algorithm."

There has been a lot of interest in using Wi-Fi signals for sensing applications, Coder says. He and Mosleh hope that app and software developers can use the process presented in the work as a framework to create programs to remotely monitor breathing.

"All the ways we're gathering the data is done on software on the access point (in this case, the router), which could be done by an app on a phone," Coder says. "This work tries to lay out how somebody can develop and test their own algorithm. This is a framework to help them get relevant information."

To read more: https://www.nist.gov/news-events/news/2022/12/wi-fi-could-help-identify-when-youre-struggling-breathe

The EU Digital Operational Resilience Act (DORA)

EUR-Lex
Access to European Union law

Article 1, Subject matter

1. In order to achieve a high common level of digital operational resilience, this Regulation lays down uniform requirements concerning the security of network and information systems supporting the business processes of financial entities as follows:

(a) requirements applicable to financial entities in relation to:

(i) information and communication technology (ICT) risk management;

(ii) reporting of major ICT-related incidents and notifying, on a voluntary basis, significant cyber threats to the competent authorities;

(iii) reporting of major operational or security payment-related incidents to the competent authorities by financial entities referred to in Article 2(1), points (a) to (d);

(iv) digital operational resilience testing;

(v) information and intelligence sharing in relation to cyber threats and vulnerabilities;

(vi) measures for the sound management of ICT third-party risk;

(b) requirements in relation to the contractual arrangements concluded between ICT third-party service providers and financial entities;

(c) rules for the establishment and conduct of the Oversight Framework for critical ICT third-party service providers when providing services to financial entities;

(d) rules on cooperation among competent authorities, and rules on supervision and enforcement by competent authorities in relation to all matters covered by this Regulation.

2. In relation to financial entities identified as essential or important entities pursuant to national rules transposing Article 3 of Directive (EU) 2022/2555, this Regulation shall be considered a sector-specific Union legal act for the purposes of Article 4 of that Directive.

3. This Regulation is without prejudice to the responsibility of Member States' regarding essential State functions concerning public security, defence and national security in accordance with Union law.

Article 2, Scope

1. Without prejudice to paragraphs 3 and 4, this Regulation applies to the following entities:

(a) credit institutions;

(b) payment institutions, including payment institutions exempted pursuant to Directive (EU) 2015/2366;

(c) account information service providers;

(d) electronic money institutions, including electronic money institutions exempted pursuant to Directive 2009/110/EC;

(e) investment firms;

(f) crypto-asset service providers as authorised under a Regulation of the European Parliament and of the Council on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 ('the Regulation on markets in crypto-assets') and issuers of asset-referenced tokens;

(g) central securities depositories;

(h) central counterparties;

(i) trading venues;

(j) trade repositories;

(k) managers of alternative investment funds;

(l) management companies;

(m) data reporting service providers;

(n) insurance and reinsurance undertakings;

(o) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries;

(p) institutions for occupational retirement provision;

(q) credit rating agencies;

(r) administrators of critical benchmarks;

(s) crowdfunding service providers;

(t) securitisation repositories;

(u) ICT third-party service providers.

2. For the purposes of this Regulation, entities referred to in paragraph 1, points (a) to (t), shall collectively be referred to as 'financial entities'.

3. This Regulation does not apply to:

(a) managers of alternative investment funds as referred to in Article 3(2) of Directive 2011/61/EU;

(b) insurance and reinsurance undertakings as referred to in Article 4 of Directive 2009/138/EC;

(c) institutions for occupational retirement provision which operate pension schemes which together do not have more than 15 members in total;

(d) natural or legal persons exempted pursuant to Articles 2 and 3 of Directive 2014/65/EU;

(e) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries which are microenterprises or small or medium-sized enterprises;

(f) post office giro institutions as referred to in Article 2(5), point (3), of Directive 2013/36/EU.

4. Member States may exclude from the scope of this Regulation entities referred to in Article 2(5), points (4) to (23), of Directive 2013/36/EU that are located within their respective territories. Where a Member State makes use of such option, it shall inform the Commission thereof as well as of any subsequent changes thereto. The Commission shall make that information publicly available on its website or other easily accessible means.

To read more: https://eur-lex.europa.eu/eli/reg/2022/2554/oj

Preparing the economy and financial system for hybrid war - Finland's experience

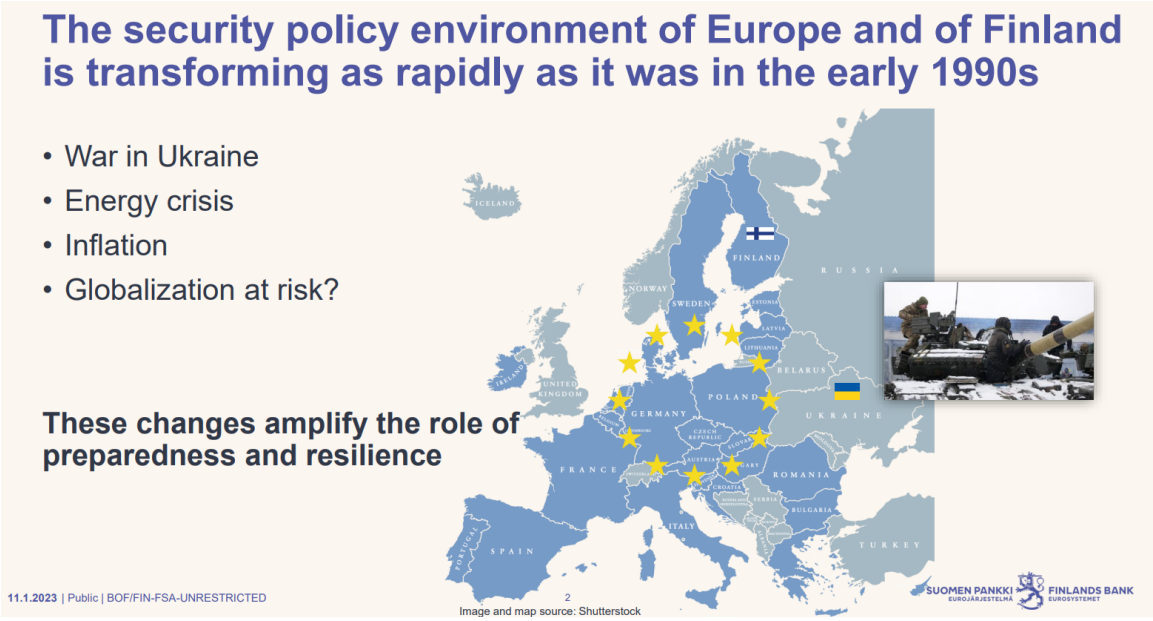
Olli Rehn, Governor of the Bank of Finland, at the Peterson Institute for International Economics (PIIE) Financial Statements web event series

Ladies and Gentlemen,

Greetings from a snowy Helsinki – and thank you very much for this opportunity to exchange views with you at this event today. The topic of my talk is Finland's experience in building up resilience and preparing the economy and financial system to cope with hybrid warfare.

Around a year ago, a rapid recovery from the COVID-19 pandemic was well under way in Europe. Those positive prospects were crushed last February by Russia's illegal and brutal attack against Ukraine.

The horrific bombardment of critical Ukrainian infrastructure has left millions of Ukrainians at the mercy of winter conditions, and no end to the war is in sight.



We need to be prepared for a long confrontation between Putin's Russia and the liberal West, or more broadly between authoritarian governments and liberal democracies.

Russia's war has been a litmus test of European unity. Supporting Ukraine in its fight for freedom remains a policy priority. For Finns, this is really close to our hearts, also by our own experience.

After all, we ourselves were attacked by the Soviet Union in the Second World War, and we still have Europe's longest border with Russia: 832 miles, or 1340 kilometres.

To read more: https://www.suomenpankki.fi/en/media-and-publications/speeches-and-interviews/2023/governor-olli-rehn-preparing-the-economy-and-financial-system-for-hybrid-war-finlands-experience/

SUOMEN PANKKI EUROJÄRJESTELMÄ FINLANDS BANK EUROSYSTEMET

Pilot Climate Scenario Analysis Exercise

Participant Instructions, January 2023

Executive Summary

The Board is conducting a pilot CSA exercise to learn about large banking organizations' climate risk-management practices and challenges and to enhance the ability of both large banking organizations and supervisors to identify, measure, monitor, and manage climate-related financial risks.

To accomplish these objectives, the Board designed the pilot CSA exercise to gather qualitative and quantitative information about the climate risk-management practices of large banking organizations.

Over the course of the exercise, the Board will engage with participants to understand their approaches and challenges with respect to the financial risks of climate change.

Information collected and discussed with participants will include detailed documentation of governance and risk-management practices, measurement methodologies, data challenges and limitations, estimates of the potential impact on specific portfolios, and lessons learned from this exercise that could inform any future CSA exercises.

The pilot CSA exercise comprises two separate and independent modules: a physical risk module and a transition risk module.

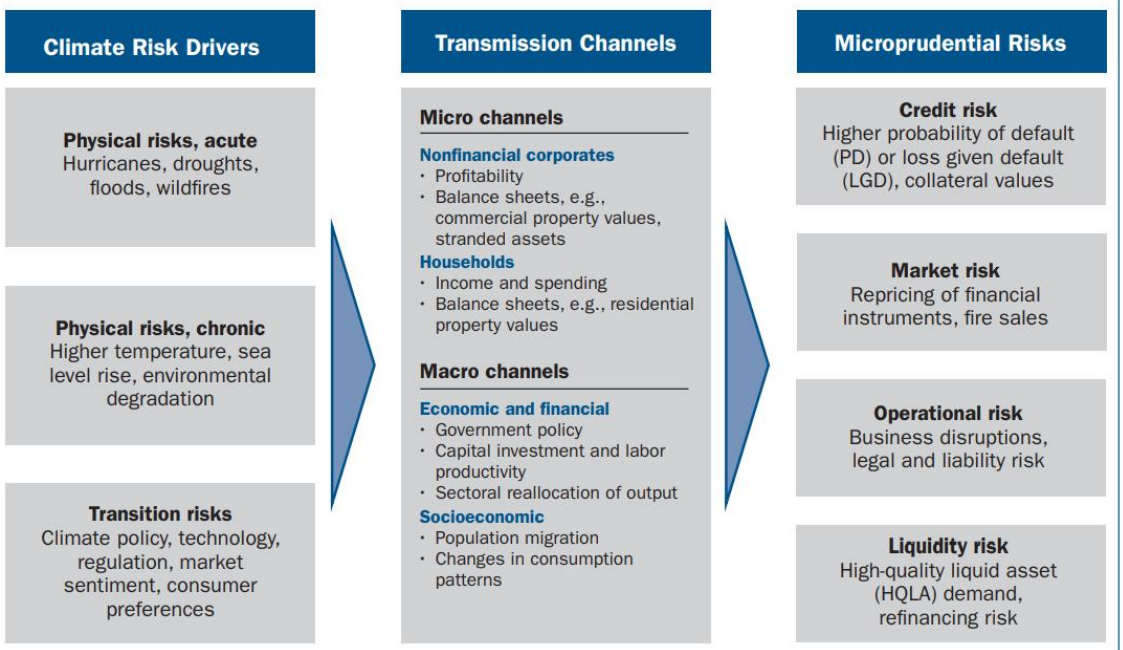
Physical risks represent the harm to people and property that may result from climate-related events, while transition risks represent stresses that may result from the transition to a lower carbon economy.

Both can manifest as traditional prudential risks for large banking organizations.

For both the physical and transition risk modules, the Board will describe forward-looking scenarios to participating large banking organizations, including core climate, economic, and financial variables, where appropriate.

Figure 1. Climate risk drivers manifest as prudential risks

Climate risk drivers could bring about microprudential risks to supervised financial institutions. These risks may manifest through a variety of transmission channels.



Note: Examples are indicative and not exhaustive.

In selecting scenarios for this exercise, the Board leveraged existing work conducted by the Intergovernmental Panel on Climate Change (IPCC) and the Network of Central Banks and Supervisors for Greening the Financial System (NGFS).

The climate scenarios used in the CSA exercise are neither forecasts nor policy prescriptions. They do not necessarily represent the most likely future outcomes or a comprehensive set of possible outcomes.

Rather, the pilot CSA exercise includes a range of plausible future outcomes that can help build understanding of how certain climate-related financial risks could manifest for large banking organizations and how these risks may differ from the past.

Participants will estimate the effect of these scenarios on a relevant subset of their loan portfolios over a future time horizon.

For each loan, participants will calculate and report to the Board credit risk parameters, such as probability of default (PD), internal risk rating grade (RRG), and loss given default (LGD), as appropriate.

Participants will respond to qualitative questions describing their governance, risk-management practices, measurement methodologies, results for specific portfolios, and lessons learned.

Focusing on changes to risk metrics like PD, RRG, and LGD, rather than on estimates of losses, will provide information about how the relative riskiness of exposures within participants' credit portfolios may evolve over time in response to different climate scenarios.

Loss estimates would involve additional assumptions around the evolution of participants' balance sheets and business models and would be incomplete given the partial nature of the exercise, which focuses on specific regions and certain portfolios for six participants.

Six U.S. bank holding companies (BHCs) will participate in this pilot exercise: Bank of America Corporation; Citigroup Inc.; The Goldman Sachs Group, Inc.; JPMorgan Chase & Co.; Morgan Stanley; and Wells Fargo & Company.

These six banking organizations will submit completed data templates, supporting documentation, and responses to qualitative questions to the Federal Reserve Board by July 31, 2023. The Board anticipates publishing insights gained from this pilot exercise around the end of 2023.

The Board expects to disclose aggregated information about how large banking organizations are incorporating climate-related financial risks into their existing risk-management frameworks.

Consistent with the objectives and design of the pilot exercise, the Board does not plan to disclose quantitative estimates of potential losses resulting from the scenarios included in the pilot exercise. No firm-specific information will be released.

This pilot CSA exercise will support the Board's responsibilities to ensure that supervised institutions are appropriately managing all material risks, including financial risks related to climate change.

To read more: https://www.federalreserve.gov/publications/files/csa-instructions-20230117.pdf

Exploring multilateral platforms for cross-border payments

This report provides an assessment of whether and how multilateral platforms could bring meaningful improvements to the cross-border payments ecosystem.

It was written by the Bank for International Settlements' Committee on Payments and Market Infrastructures (CPMI) in collaboration with the BIS Innovation Hub, the International Monetary Fund (IMF) and the World Bank.

The report analyses the potential costs and benefits of these platforms and how they might alleviate some of the cross-border payment frictions. It also evaluates the risks, barriers and challenges to establishing multilateral platforms and explores two paths for their evolution.

The analysis is based on a stocktake, conducted by the CPMI, of existing and potential multilateral platforms as well as bilateral discussions with existing platform operators.

A multilateral platform is a payment system for cross-border payments that is multi-jurisdictional by design. It can substitute for or operate alongside traditional correspondent banking relationships or bilateral interlinking of domestic payment infrastructures.

A multilateral platform can potentially shorten transaction chains by allowing participants in different jurisdictions to send or receive payments directly instead of via multiple intermediaries.

Depending on its design, a platform can offer extended operating hours to meet the requirements of participants in different time zones and ease compliance checks related to anti-money laundering and combating the financing of terrorism (AML/CFT).

Built as new, it can also reduce dependencies on legacy systems by implementing the latest technology and payment message standards.

To the extent a multilateral platform is able to mitigate these underlying frictions, it could reduce the costs and increase the safety, speed and transparency of cross-border payments.

Multilateral platforms could enhance cross-border payments but often involve more complicated legal and operational issues relative to domestic payment systems.

Any decision to increase the role of multilateral platforms should weigh all relevant trade-offs, risks and benefits relative to other cross-border arrangements such as correspondent banking, not merely the added risks relative to domestic systems.

These considerations vary depending on the current state of cross-border payment arrangements in a specific geographical region or for a specific payment system function, as well as on the purpose and chosen approach for increasing the role of multilateral platforms.

The actual improvements that a potential platform can bring to the cross-border payments ecosystem will, of course, depend on its concrete design. Hence, this report can only offer some high-level considerations, without pre-empting potential future considerations on individual business cases.

This report explores two conceptual implementation approaches: the growth approach and the greenfield approach.

The growth approach involves expanding existing multilateral platforms to additional jurisdictions, currencies and participants (including by extending access to foreign participants and interlinking with domestic systems and other platforms).

This option could be based on existing institutional arrangements but may nevertheless require additional public-private sector involvement and coordination.

The greenfield approach involves building a new, potentially global infrastructure for crossborder payments.

This option could foster greater alignment of certain aspects of cross-border payments but may entail complex governance discussions and cooperative oversight arrangements as well as careful balancing of the roles of public and private sector stakeholders.

Policymakers have different options to consider as they analyse the potential development and implementation of multilateral platforms.

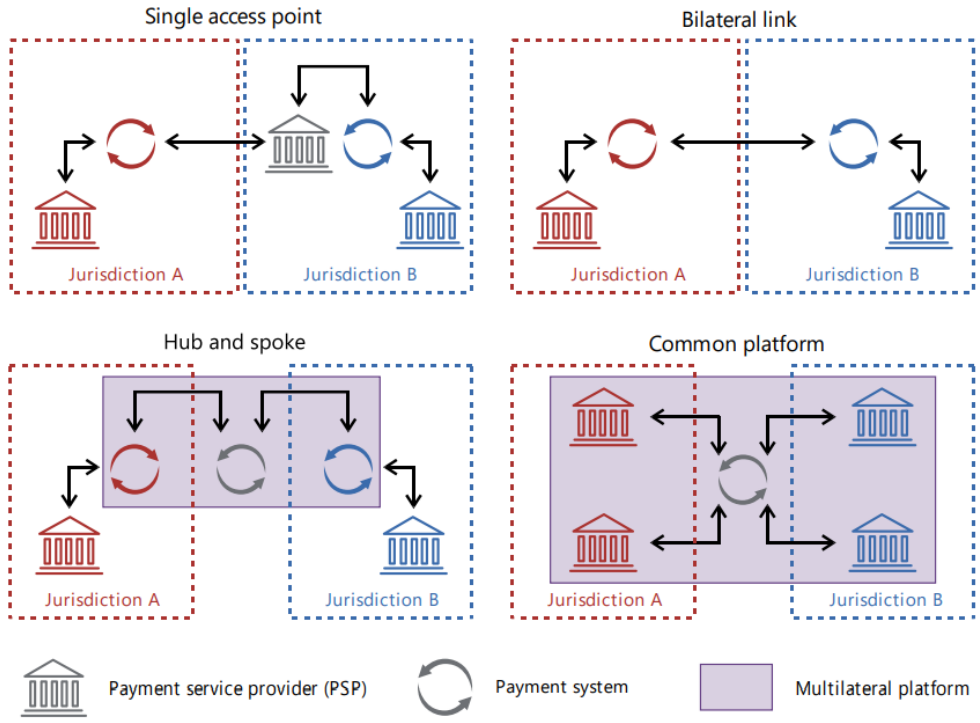
Any evaluation should carefully consider the trade-offs of multilateral platforms and account for the evolving nature of the cross-border payments market. To this end, possible further measures could entail efforts by regional bodies, operators and/or international organisations to realise the potential of multilateral platforms.

Taking advantage of the momentum generated by the G20 cross-border payments programme, payment system operators and authorities contemplating the expansion or establishment of multilateral platforms

can use this analysis as a basis for evaluating the best approach for their specific circumstances. Such preparatory steps could allow relevant stakeholders to gain a sound basis from which to plan and assess future actions.

Contents

Stylised models for interlinking cross-border payment systems[1, 2] Graph 1



[1] Examples include euroSIC (single access point), Directo a México (bilateral link), the Regional Payment and Settlement System (REPSS) of the Common Market for Eastern and Southern Africa (hub and spoke) and Southern African Development Community (SADC)-RTGS (common platform). [2] The multilateral platform includes the participants and the entity operating the arrangement. In the hub and spoke model, the participants are payment systems. In the common platform model, the participants are PSPs.

Source: Adapted from CPMI (2022d).

To read more: https://www.bis.org/cpmi/publ/d213.pdf

Disclaimer

The Association tries to enhance public access to information about risk and compliance management.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any particular individual or entity;

- should not be relied on in the particular context of enforcement or similar regulatory action;

- is not necessarily comprehensive, complete, or up to date;

- is sometimes linked to external sites over which the Association has no control and for which the Association assumes no responsibility;

- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);

- is in no way constitutive of an interpretative document;

- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;

- does not prejudge the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts.

It is our goal to minimize disruption caused by technical errors. However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

The Association accepts no responsibility with regard to such problems incurred as a result of using this site or any linked external sites.

International Association of Potential, New and Sitting Members of the Board of Directors (IAMBD)

The IAMBD offers standard, premium and lifetime membership, networking, training, certification programs, a monthly newsletter with alerts and updates, and services we can use.

The association develops and maintains three certification programs and many specialized tailor-made training programs for directors.

Join us. Read our monthly newsletter with news, alerts, challenges and opportunities. Get certified. Provide independent evidence that you are an expert.

You can explore what we offer to our members:

1. Membership - Become a premium or lifetime member.
You may visit:
https://www.iambd.org/HowToBecomeMember.html

2. Monthly Updates – Visit the Reading Room of the association at:
https://www.iambd.org/Reading_Room.htm

3. Training and Certification - Become a Certified Member of the Board of Directors (CMBD), Certified Member of the Risk Committee of the Board of Directors (CMRBD) or Certified Member of the Corporate Sustainability Committee of the Board of Directors (CMCSCBD).

You may visit:
https://www.iambd.org/Distance_Learning_and_Certification.htm

For instructor-led training, you may contact us. We can tailor all programs to meet specific requirements.