Solvency ii Association
1200 G Street NW Suite 800 Washington DC 20005-6705 USA
Tel: 202-449-9750 Web: www.solvency-ii-association.com

Solvency 2 News, October 2022

Dear members and friends,

The European Insurance and Occupational Pensions Authority (EIOPA) has set out its strategy for the period 2023 – 2026.

Current geopolitical tensions due to Russia's unprovoked invasion of Ukraine coupled with lingering effects of the pandemic, market volatility and inflation underline the need for effective supervision.

Building on a strong foundation, the strategy is designed to strengthen the resilience and sustainability of the insurance and pensions sectors, and to ensure the strong and consistent protection of consumer interests across the European Union.

Under the overall vision of building a safe and sustainable EU for citizens in times of transformation, EIOPA has identified strategic priorities on which to focus:

- Sustainable finance. Contribute to building up sustainable insurance and pensions, including by addressing protection gaps, for the benefit of citizens and businesses.

- Digital transformation. Support the supervisory community and industry to mitigate the risks and seize the opportunities of the digital transformation, including by further promoting a data-driven culture.

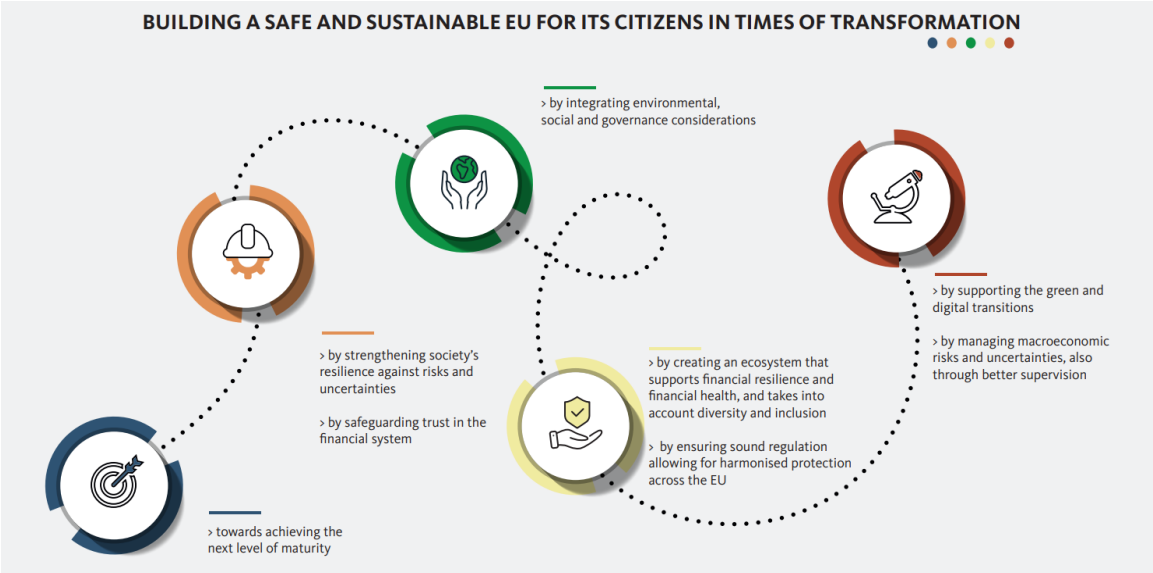
- Supervision. Promote sound, efficient and consistent prudential and conduct supervision throughout Europe, particularly in view of increased cross-border business.

- Policy. Deliver high-quality advice and other policy work taking into account changing and growing needs of society as well as the effects of new horizontal regulation.

- Financial stability. Further enhance financial stability, with particular focus on the analysis of financial sector risks, vulnerabilities, and emerging threats.

- Internal governance. Be a model EU Authority with high professional standards, cost-effective governance, and a positive reputation within the EU and globally.

To fulfil its objectives, EIOPA will continue to work in a collaborative and consultative way, valuing the guidance of its Board of Supervisors, and the input from a range of stakeholders.



The strategy:
https://www.eiopa.europa.eu/sites/default/files/publications/administrative/eiopa-strategy-2023-2026.pdf

Proposed Articles of the European Cyber Resilience Act

The proposal for a regulation on cybersecurity requirements for products with digital elements, known as the Cyber Resilience Act, bolsters cybersecurity rules to ensure more secure hardware and software products.

Hardware and software products are increasingly subject to successful cyberattacks, leading to an estimated global annual cost of cybercrime of €5.5 trillion by 2021.

Such products suffer from two major problems adding costs for users and the society:

- a low level of cybersecurity, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them, and

- an insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner.

While existing internal market legislation applies to certain products with digital elements, most of the hardware and software products are currently not covered by any EU legislation tackling their cybersecurity.

In particular, the current EU legal framework does not address the cybersecurity of non-embedded software, even if cybersecurity attacks increasingly target vulnerabilities in these products, causing significant societal and economic costs.

Two main objectives were identified aiming to ensure the proper functioning of the internal market:

- create conditions for the development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and ensure that manufacturers take security seriously throughout a product's life cycle; and

- create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements.

Four specific objectives were set out:
1. Ensure that manufacturers improve the security of products with digital elements since the design and development phase and throughout the whole life cycle;

2. Ensure a coherent cybersecurity framework, facilitating compliance for hardware and software producers;

3. Enhance the transparency of security properties of products with digital elements, and

4. Enable businesses and consumers to use products with digital elements securely.

For the purposes of this Regulation, the *following definitions* apply:

'Product with digital elements' means any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately;

'Remote data processing' means any data processing at a distance for which the software is designed and developed by the manufacturer or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions;

'Economic operator' means the manufacturer, the authorised representative, the importer, the distributor, or any other natural or legal person who is subject to obligations laid down by this Regulation;

'Manufacturer' means any natural or legal person who develops or manufactures products with digital elements or has products with digital elements designed, developed or manufactured, and markets them under his or her name or trademark, whether for payment or free of charge;

'Authorised representative' means any natural or legal person established within the Union who has received a written mandate from a manufacturer to act on his or her behalf in relation to specified tasks;

'Importer' means any natural or legal person established in the Union who places on the market a product with digital elements that bears the name or trademark of a natural or legal person established outside the Union;

'Distributor' means any natural or legal person in the supply chain, other than the manufacturer or the importer, that makes a product with digital elements available on the Union market without affecting its properties;

'Software' means the part of an electronic information system which consists of computer code;

'Hardware' means a physical electronic information system, or parts thereof capable of processing, storing or transmitting of digital data;

'Significant cybersecurity risk' means a cybersecurity risk which, based on its technical characteristics, can be assumed to have a high likelihood of an incident that could lead to a severe negative impact, including by causing considerable material or non-material loss or disruption;

Our strategic partner, Cyber Risk GmbH, is carefully monitoring the developments. You may visit: https://www.european-cyber-resilience-act.com

This is a difficult compliance challenge, as "the Regulation applies to products with digital elements, whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network."

Technical documentation of the methodology to derive EIOPA's risk-free interest rate term structures

Letter of the Executive Director

Solvency II aims at implementing an economic and risk-based supervisory framework in the field of insurance and reinsurance. The framework is built upon three pillars, all equally relevant, that provide for quantitative requirements (Pillar 1), qualitative requirements (Pillar 2) and enhanced transparency and disclosure (Pillar 3).

The starting point in Solvency II is the economic valuation of the whole balance sheet, where all assets and liabilities are valued according to market consistent principles.

The risk-free interest rate term structure (hereafter in this letter, risk-free interest rate) underpins the calculation of liabilities by insurance and reinsurance undertakings.

EIOPA is required to publish the risk-free interest rate. This technical document sets out the basis on which it will do so. It is the result of collaboration between EIOPA's members and its staff.

As a default approach, the risk-free interest rate is primarily derived from the rates at which two parties are prepared to swap fixed and floating interest rate obligations.

In the absence of financial swap markets, or where information of such transactions is not sufficiently reliable, the risk-free interest rate is based on the government bond rates of the country.

The risk-free interest rates are:

• Calculated for different time periods, reflecting that the liabilities of insurance and reinsurance undertakings stretch years and decades into the future.

• Calculated in respect of the most important currencies for the EU insurance market.

• Adjusted to reflect that a portion of the interest rate in a swap transaction (or a government bond) will reflect the risk of default of the counterparty

and hence without adjustment would not be risk-free.

• Based on data available from financial markets. For those periods in the more distant future for which data are not available, the rate is extrapolated from the point at which data are available to a macroeconomic long-term equilibrium rate.

An adjustment (the volatility adjustment) is made to the liquid part of the riskfree interest rate in order to reduce the impact of short-term market volatility on the balance sheet of undertakings.

EIOPA is required to provide, both on a currency and country basis, the size of this adjustment for volatility.

A different adjustment (the matching adjustment) is made in respect of predictable portfolios of liabilities.

An undertaking can assign to eligible portfolios assets with fixed cash flows that it intends to hold to maturity. EIOPA is required to provide an estimate of what portion of the spread of such assets above the riskfree interest rate reflects risks not faced by those who hold assets to maturity.

To read more:
https://www.eiopa.europa.eu/sites/default/files/risk_free_interest_rate/eiopa-bos-22-409-technical-documentation.pdf

EIOPA, Revised Single Programming Document 2023-2025

Including Annual Work Programme 2023

In a context characterised by evolving challenges, risks and opportunities EIOPA will focus on managing the uncertainty in times of transformation to ensure robust insurance and pensions sectors in Europe.

The Russian invasion has provoked a humanitarian crisis, a political crisis and an economic crisis. One that not only is urgent now, but that will also impact many economic and political decisions in the future.

In 2022, we have been observing an abrupt change in the economic and financial situation. Supply chain disruptions, spiking energy and commodity prices triggered by the prolonged pandemic crisis and the geopolitical tensions, are shifting the narrative from one dominated by protracted low yields and low inflation to an economic juncture driven by high inflation and uncertain economic growth.

At the same time, EIOPA will continue to contribute to the recovery of the EU economy following the pandemic, supporting Member States in building more resilient insurance and pensions sectors and further strengthening a common supervisory culture.

These times of transformation with uncertainties arising from an ever-changing macroeconomic environment, present potential increase in vulnerabilities of the insurance and pension sectors. Subsequently this calls for continued and forward-looking identification of risks in the context of a proactive and engaged supervisory community.

EIOPA will strive to provide supervisors with a reliable assessment of market vulnerabilities focusing on enhancing the methodological framework particularly for top-down and more streamlined vulnerability assessments while increasing capacity for emerging threats such as cyber and climate change.

Digitalisation, with its opportunities and risks, will require our attention to support the market and supervisory community through the digital transformation. As we see the digitalisation continue to accelerate, impacting business models, products and services as well as distribution channels, it is key to recognise threats and have measures in place that can keep the financial system safe and citizens included.

In addition to this, the digital transformation is also accelerating the interconnectedness of financial services, so that regulation is now becoming more horizontal.

EIOPA will strive to ensure that the insurance and pensions sectors are well represented in new cross-sectoral and horizontal regulation. Data is at the heart of the insurance and pension industry, and at the backbone of digital transformation and effective financial supervision.

To this end, EIOPA aims to enhance data availability and data standardisation, thus contributing to the development of a sound European Data Eco-System.

The insurance and pensions sectors have a unique opportunity and responsibility to address sustainabilityrelated challenges and thus facilitate the transition to a more sustainable and resilient economy, given their key role as society's risk managers and important long-term investors.

Addressing protection gaps remains a priority among EIOPA's activities on sustainable finance. EIOPA will step up its work on identifying protection gaps with the aim to promote coverage of risks and increasing their insurability, also through possible shared resilience solutions.

EIOPA will strive to further increase consumer risk awareness and understanding of riskbased prevention measures to climate change as well as complement the insurance and pensions sectors efforts for climate

change mitigation and adaption by promoting open source data and modelling of climate change risks.

The transition to a more environmentally and socially sustainable economy will require assessing the possible impacts at macro-prudential level, as well as potential consumer detriment arising from greenwashing.

To achieve an even higher, more effective and further harmonised convergent level of supervision across the European Union, EIOPA will continue to strengthen supervisory convergence by ensuring consistent reviews and proportionate application of supervisory convergence tools, which shall remain fit-for-purpose.

At the same time, EIOPA will continue the monitoring of the implementation of supervisory convergence tools and follow-up measures at the national level.

The foundation for our supervision is good regulation. Solvency II, and particularly buffers, proved effective in protecting the insurance sector from market turmoil in the past economic crisis.

We need to make sure that Solvency II stays robust and fit for purpose taking into account that the European macroeconomic environment will remain challenging.

Additionally, EIOPA will step up its monitoring activities in order to ensure products are designed in the best interest of consumers, and can deliver value for money.

EIOPA aims to ensure that the products offered to policyholders offer value for money, that people's needs are put first before profit and that they are sold the products that are right for their individual situation.

Towards this end, EIOPA will strive to make sure that consumers have access to the right information and the right advice so they can make better informed decisions.

This includes efforts towards having disclosure documents that are truly consumer-focused and adapted for the digital age. In 2023 EIOPA will Chair the EU Agencies Network (EUAN) providing a forum for coordination, information exchange and agreement on common positions on issues of shared interest thus helping shape informed policies and laws at the EU and national level.

Furthermore, EIOPA will plan and manage resources in an agile manner that allows accelerated decision-making and allocation of resources towards key priorities.

Looking forward, EIOPA will continue to develop as a responsible and attractive organisation, promoting diversity and inclusion. Good governance, cost-effective processes and strong partnerships will make the Authority well equipped to contribute to a future in which the insurance and pension sectors fulfil an essential role in underpinning a strong and sustainable recovery in Europe, for the benefit of citizens, business, and the economy.

To read more:
https://www.eiopa.europa.eu/sites/default/files/publications/administrative/eiopa-revised-spd-2023-2025.pdf

EIOPA publishes supervisory statements on exclusions related to systemic events and the management of non-affirmative cyber exposures

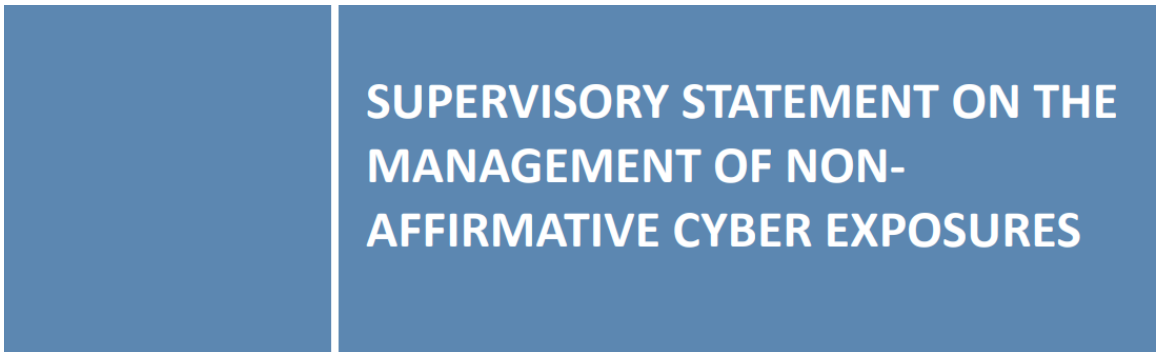
The European Insurance and Occupational Pensions Authority (EIOPA) published two Supervisory Statements on:

- exclusions related to systemic events such as pandemic, natural catastrophes or large cyber-attacks, and on

- the management of non-affirmative cyber exposures.

You may visit: https://www.eiopa.europa.eu/document-library/supervisory-statement/supervisory-statement-exclusions-insurance-products-related_en

https://www.eiopa.europa.eu/document-library/supervisory-statement/supervisory-statement-management-of-non-affirmative-cyber_en



Supervisory statement on exclusions in insurance products in relation to risks arising from systemic events

As the frequency of systemic events increases, there is a risk that insurance products covering them become unaffordable or unavailable.

At the same time, products covering such events or products silent about the coverage may explicitly exclude them in the future.

These developments have the potential to further widen existing protection gaps, which can have a detrimental effect on consumers and make our economies and societies less resilient.

EIOPA's supervisory statement aims to promote supervisory convergence in how national competent authorities assess the treatment of exclusions as part of the product design and terms and conditions drafting process.

The statement seeks to ensure that the interests of existing and prospective policyholders are duly taken into account when products are developed or revised or when events casting doubt on the scope of the coverage materialise.

Beyond general contract clarity and language simplicity requirements, EIOPA recommends that national competent authorities monitor whether insurance manufacturers appropriately assess the terms and conditions and the scope of coverage whenever the risk arising from a systemic event becomes uninsurable or there is lack of clarity as to whether the risk is covered or not.

More broadly, beyond general product oversight and governance requirements, when new products are developed, EIOPA recommends assessing the target market's needs, objectives and characteristics with respect to the exclusion of risks arising from systemic events – including when determining whether risks stemming from systemic events are covered or not.

While there may be a limit to insurability, EIOPA is of the view that consumers and small businesses can assess the risks involved better – including those stemming from systemic events – when coverage is clear and aligned to the target market's needs.

The supervisory statement therefore advocates greater clarity and specific tailoring to the target market.

3. SUPERVISORY EXPECTATIONS

1.14 Given the context outlined, EIOPA recommends NCAs to dedicate higher attention to the supervision of cyber underwriting risk, in particular to (re)insurance undertakings that have potentially significant exposure to non-affirmative cyber insurance risk and to those who have not yet developed a plan to identify and manage non-affirmative cyber underwriting risk, including tailored considerations regarding the specificities of the multiple Lines of Business and products impacted.

1.15 In particular, considering also challenges to draw a straight line between affirmative and non-affirmative risk, EIOPA recommends to engage in a supervisory dialogue with the undertakings and follow a more holistic and risk based approach in the supervision of at least the following aspects:

a) top-down strategy and appetite for (re)insurance undertakings to underwrite cyber risk;

b) identification and measurement of risks exposure with the purpose of implementing sound cyber underwriting practices, with particular regard to the non-affirmative cyber risk;

c) cyber underwriting risk management and risk mitigation, including the reinsurance strategy.

To read more: https://www.eiopa.europa.eu/media/news/eiopa-publishes-supervisory-statements-exclusions-related-systemic-events-and-management_en

ESAs warn of rising risks amid a deteriorating economic outlook

The three European Supervisory Authorities (EBA, EIOPA and ESMA - ESAs) issued today their Autumn 2022 joint risk report.


JOINT COMMITTEE REPORT ON
RISKS AND VULNERABILITIES IN THE EU FINANCIAL SYSTEM
SEPTEMBER 2022

The report highlights that the deteriorating economic outlook, high inflation and rising energy prices have increased vulnerabilities across the financial sectors.

The ESAs advise national supervisors, financial institutions and market participants to prepare for challenges ahead.

The post-pandemic economic recovery in Europe has dwindled as a result of the Russian invasion of Ukraine.

Russia's war on Ukraine and the disruptions in trade caused a rapid deterioration of the economic outlook.

It adds to pre-existing inflationary pressures by strongly raising energy- and commodity prices, exacerbates imbalances in supply and demand, and weakens the purchasing power of households.

The risk of persistent inflation and stagflation has risen.

These factors, coupled with the deteriorated economic outlook, have significantly impacted the risk environment of the financial sector. Financial market volatility has increased across the board given high uncertainties.

After a long period of low interest rates, central banks are tightening monetary policy.

The combination of higher financing costs and lower economic output may put pressure on government, corporate and household debt refinancing while also negatively impacting the credit quality of financial institutions' loan portfolios.

The reduction of real returns through higher inflation could lead investors to higher risk-taking at a time when rate rises are setting in motion a far-reaching rebalancing of portfolios.

Financial institutions also face increased operational challenges associated with heightened cyber risks and the implementation of sanctions against Russia.

The financial system has to date been resilient despite the increasing political and economic uncertainty.

In light of the above risks and vulnerabilities, the Joint Committee of the ESAs advises national competent authorities, financial institutions and market participants to take the following policy actions:

Financial institutions and supervisors should continue to be prepared for a deterioration in asset quality in the financial sector and monitor developments including in assets that benefitted from temporary measures related to the pandemic and those that are particularly vulnerable to a deteriorating economic environment, to inflation as well as to high energy and commodity prices.

The impact of further increases in policy rates and of potential sudden increases in risk premia on financial institutions and market participants at large should be closely monitored.

Financial institutions and supervisors should closely monitor the impact of inflation risks.

Supervisors should continue to monitor risks to retail investors, in particular with regard to products where consumers may not fully realise the extent of the risks involved, such as crypto-assets.

Financial institutions and supervisors should continue to carefully manage environmental risks and cyber risks to address threats to information security and business continuity.

The report: https://www.eiopa.europa.eu/document-library/report/joint-committee-report-risks-and-vulnerabilities-eu-financial-system-1_en

BIS Working Paper No 1039

Cyber risk in central banking

by Sebastian Doerr, Leonardo Gambacorta, Thomas Leach, Bertrand Legros and David Whyte - Monetary and Economic Department

The rising number of cyber attacks in the financial sector poses a threat to financial stability and makes cyber risk a key concern for policy makers.

This paper presents the results of a survey among members of the Global Cyber Resilience Group on cyber risk and its challenges for central banks.

The survey reveals that central banks have notably increased their cyber security-related investments since 2020, giving technical security control and resiliency priority.

Central banks see phishing and social engineering as the most common methods of attack, and the potential losses from a systemically relevant cyber attack are deemed to be large, especially if the target is a big tech providing critical cloud infrastructures.

Generally, respondents judge the preparedness of the financial sector for cyber attacks to be inadequate. While central banks in most emerging market economies provide a framework for the collection of information on cyber attacks on financial institutions, less than half of those in advanced economies do.

Cooperation among public authorities, especially in the international context, could improve central banks' ability to respond to cyber attacks.

The survey reveals four main insights.

First, central banks from AEs and EMEs differ in their assessment of the frequency and cost of different cyber attacks. All central banks deem phishing and other forms of social engineering as the most likely type of attack vectors. AE central banks are significantly more worried about supply chain attacks than their EME counterparts.

When it comes to the costs resulting from an attack, advanced persistent malware and ransomware attacks rank highest. Turning to the who of these attacks, AE central banks deem organised crime and state-sponsored entities to be the main perpetrators. Among EME central banks, it is organised crime and individuals or activists.

Second, central banks actively discuss and develop policy responses to cyber attacks and have increased their cyber security-related investments notably since 2020.

Technical security control and resiliency feature high on the priority list in terms of areas for investment in cyber security.

Training existing staff on cyber security or hiring new staff with the relevant skills are also considered important, especially among EME central banks. Beyond investments, central banks focus on developing concrete policy responses.

All central banks put a high focus on developing an incident response plan in case their own institution is attacked, and several central banks are also developing a formal strategy for responding to an attack on the financial system at large.

All central banks run internal exercises to simulate cyber attacks, and the most frequently modelled scenarios are an attack on the system of the central bank itself, as well as an outage of the payments system or other critical FMI.

While supervisory authorities in most EMEs provide a framework for the collection of information on cyber attacks on financial institutions, less than half of those in AEs do.

Similarly, while supervised firms are mandated to report losses related to cyber attacks to the central bank in almost all EMEs, only two-thirds of AE respondents report that such disclosure is required.

No jurisdiction requires firms to disclose such losses publicly, however.

Third, central banks deem the potential losses from a systemically relevant cyber attack to be large, and think that losses from cyber attacks in the financial sector have increased over the past year.

Only a few central banks fully agree that the financial sector is adequately prepared for cyber attacks, and over half of the respondents think that investment in cyber security has been inadequate over the past year.

Beyond traditional financial institutions, respondents reported that they see fintechs to be more at risk from a cyber attack than big techs, even though most respondents agree that a successful attack on a big tech would lead to materially higher aggregate costs than an attack on a fintech.

And **fourth,** central banks in AEs and EMEs already cooperate widely on a range of topics. Bilateral cooperation among central banks, as well as cooperation in bodies at the regional and global levels, is the norm.

When it comes to specific topics related to cooperation, information sharing, simulations and policy formulations to improve cyber resilience stand out in AEs. Among EMEs, central banks frequently cooperate in the realms of information sharing and policy formations.

In addition, over two-thirds of respondents develop common standards and protocols for the financial sector.

The BIS supports central banks' cyber security work, as well as global cooperation in this domain, in several ways – for example, through its Cyber Resilience Coordination Centre or projects of the BIS Innovation Hub.

To read more: https://www.bis.org/publ/work1039.pdf

Federal Reserve Board invites comment on updates to operational risk-management requirements for certain systemically important financial market utilities (FMUs) supervised by the Board

The Federal Reserve Board has invited comment on updates to operational risk-management requirements for certain systemically important financial market utilities (FMUs) supervised by the Board.

FMUs provide essential infrastructure to clear and settle payments and other financial transactions upon which the financial markets and the broader economy rely to function effectively.

The proposed updates generally provide more specificity to the existing requirements.

The broad operational risk, technology, and regulatory landscape in which FMUs operate has evolved significantly since the Board last updated its risk management requirements for FMUs in 2014.

New challenges have emerged, such as the global pandemic and cyber events, while new technological advancements may improve resilience. The proposed changes would promote effective risk management in this rapidly evolving risk environment.

"In light of the rapidly evolving risk landscape, the proposed changes will help ensure that key financial market utilities operate with a high level of resilience and remain a source of strength for the financial system," said Vice Chair Lael Brainard.

The proposal addresses four key areas: incident management and notification; business continuity management and planning; third-party risk management; and review and testing of operational risk management measures.

For example, the proposal would explicitly require FMUs to establish an incident management framework and would emphasize the need for FMUs to continue to advance their cyber resilience capabilities. The proposed updates are largely consistent with existing measures that FMUs take to comply with the current requirements.

Comments on the proposed changes must be submitted within 60 days from the date of publication in the Federal Register.

For media inquiries, email media@frb.gov or call (202) 452-2955.

To read more:
https://www.federalreserve.gov/newsevents/pressreleases/bcreg20220923a.htm

Banks' exposures to cryptoassets – a novel datase

BIS

Since 2018, the Basel Committee has been pursuing a multi-pronged set of analytical, supervisory and policy initiatives related to cryptoassets.

As part of this work, a new cryptoasset data collection template was introduced starting with the current Basel III monitoring exercise based on end-2021 data.

The template was specifically designed to support the Committee's two consultative documents on the prudential treatment of banks' cryptoasset exposures, which were published on 10 June 2021 and 30 June 2022.

It collects granular information on banks' holdings of cryptoassets, including information at the level of individual cryptoassets. This special feature provides some analysis on banks' exposures to cryptoassets based on the data collected.

Overall, 19 banks submitted cryptoasset data – 10 from the Americas, seven from Europe and two from the rest of the world (Graph , left panel).

All reporting banks are Group 1 banks, except for three Group 2 banks (of these, two Group 2 banks do not participate in the wider Basel III monitoring exercise and appear to specialise in cryptoassets).

These banks make up a relatively small part of the wider sample of 182 banks considered in the Basel III monitoring exercise – 2.4% of total RWA, and 7.2% of overall leverage ratio exposure measure (LREM) (Graph 1, right panel), with banks from the Americas contributing to approximately three quarters of these amounts.

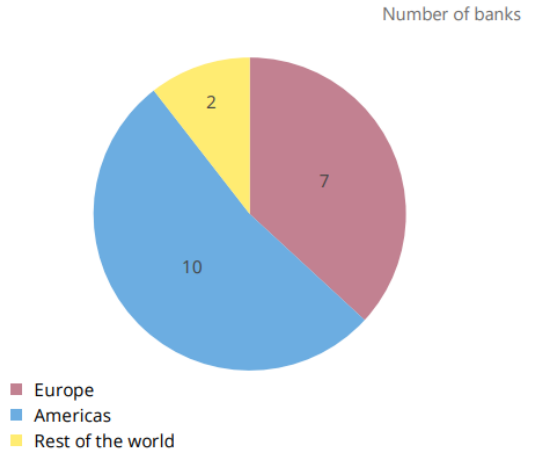
As this is the first data collection using the new template, the results in this special feature are subject to a number of data quality caveats and potential biases.

As the cryptoasset market is fast evolving, it is difficult to ascertain whether some banks have under- or over-reported their exposures to cryptoassets, and the extent to which they have consistently applied the same approach to classifying any exposures.

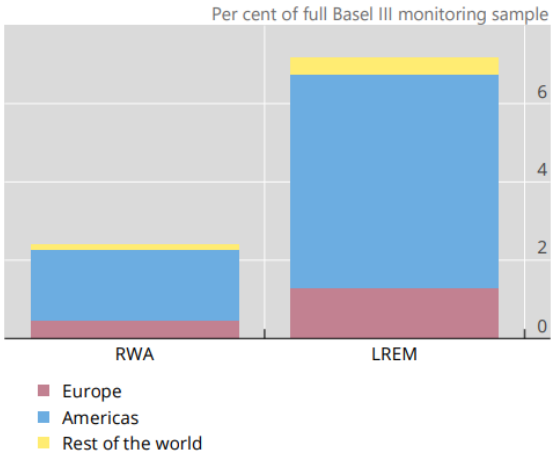
As such, while they are helpful in providing a broad indication of banks' cryptoasset activity, they should interpreted with a degree of caution.

A small proportion of banks reported crypto exposures at end-2021 Graph 1

Number of banks reporting cryptoasset exposures[1]



Proportion of banks reporting crypto exposures[2]

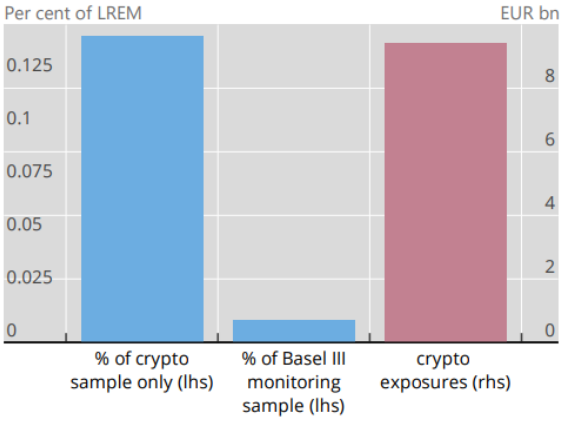


[1] All reporting banks are Group 1 banks, except for three Group 2 banks. Two Group 2 banks participated only in the crypto exercise and did not participate in the wider Basel III monitoring exercise. [2] The denominators used also account for the amounts of the two Group 2 banks which only participate in the crypto exercise and are not included in the general analysis of the Basel III monitoring exercise.

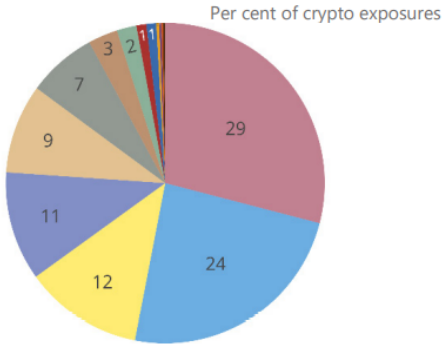
Source: BCBS end-2021 data collection and Secretariat calculations.

Crypto exposures are relatively small and unevenly distributed across banks Graph 2

Reported crypto exposures



Distribution of total crypto exposures across banks[1]



[1] Each slice represents one of the banks which reported crypto exposures.

Source: BCBS end-2021 data collection and Secretariat calculations.

Overall amounts

Total cryptoasset exposures reported by banks amount to approximately €9.4 billion. In relative terms, these exposures make up only 0.14% of total exposures on a weighted average basis across the sample of banks reporting cryptoasset exposures.

When considering the whole sample of banks included in the Basel III monitoring exercise (ie also those that do not report cryptoasset

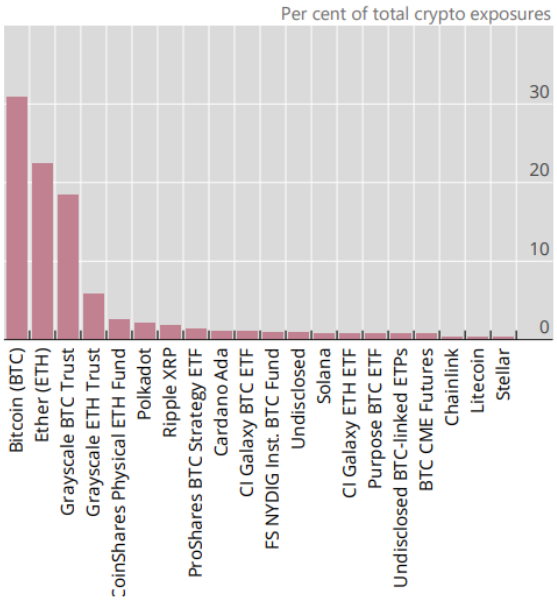
exposures), the amount shrinks to 0.01% of total exposures (Graph 2, left panel).

Cryptoasset exposures are distributed unevenly across reporting banks, with two banks making up more than half of overall cryptoasset exposures, and four more banks making up just below 40% of the remaining exposures (Graph 2, right panel).

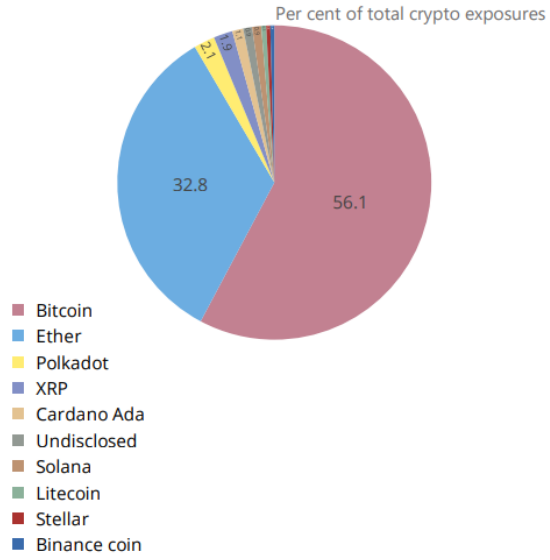
Bitcoin, Ether and related cryptoassets make up the vast majority of crypto exposures

Graph 3

Top 20 reported cryptoassets by exposure amount



Top 10 reported cryptoassets grouped by underlying asset



Source: BCBS end-2021 data collection and Secretariat calculations.

Composition across cryptoassets

Reported cryptoasset exposures are primarily composed of Bitcoin (31%), Ether (22%) and a multitude of instruments with either Bitcoin or Ether as the underlying cryptoassets (25% and 10% respectively).

Together, these make up almost 90% of reported exposures (Graph 3).

Focusing on the top 20 reported cryptoassets by exposure amount, other relatively significant reported cryptoassets include Polkadot (2% of reported exposures), Ripple XRP (2%), Cardano Ada (1%), Solana (1%), Litecoin (0.4%) and Stellar (0.4%).

These exposures would likely be classified as Group 2 cryptoassets under the current consultative proposal of the Basel Committee.

Banks also reported, in smaller amounts, a stablecoin (USD coin) and tokenised assets (not shown).

To read more: https://www.bis.org/bcbs/publ/d541_crypto.pdf

The Financial Stability Oversight Council Releases Report on Digital Asset Financial Stability Risks and Regulation

FSOC

Note: The Financial Stability Oversight Council (FSOC or Council) was established by the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act). The purposes of the Council under the Dodd-Frank Act are:

(1) to identify risks to the financial stability of the United States that could arise from the material financial distress or failure, or ongoing activities, of large, interconnected bank holding companies or nonbank financial companies, or that could arise outside the financial services marketplace;

(2) to promote market discipline by eliminating expectations on the part of shareholders, creditors, and counterparties of such companies, that the Government will shield them from losses in the event of failure; and

(3) to respond to emerging threats to the stability of the United States (U.S.) financial system.

Executive Summary

Crypto-asset activities could pose risks to the stability of the U.S. financial system if their interconnections with the traditional financial system or their overall scale were to grow without adherence to or being paired with appropriate regulation, including enforcement of the existing regulatory structure.

The scale of crypto-asset activities has increased significantly in recent years. Although interconnections with the traditional financial system are currently relatively limited, they could potentially increase rapidly.

Participants in the cryptoasset ecosystem and the traditional financial system have explored or created a variety of interconnections. Notable sources of potential interconnections include traditional assets held as part of stablecoin activities.

Crypto-asset trading platforms may also have the potential for greater interconnections by providing a wide variety of services, including leveraged trading and asset custody, to a range of retail investors and traditional financial institutions. Consumers can also increasingly access crypto-asset activities, including through certain traditional money services

businesses. Some characteristics of crypto-asset activities have acutely amplified instability within the crypto-asset ecosystem.

Many crypto-asset activities lack basic risk controls to protect against run risk or to help ensure that leverage is not excessive.

Crypto-asset prices appear to be primarily driven by speculation rather than grounded in current fundamental economic use cases, and prices have repeatedly recorded significant and broad declines.

Many crypto-asset firms or activities have sizable interconnections with crypto-asset entities that have risky business profiles and opaque capital and liquidity positions.

In addition, despite the distributed nature of crypto-asset systems, operational risks may arise from the concentration of key services or from vulnerabilities related to distributed ledger technology.

These vulnerabilities are partly attributable to the choices made by market participants, including crypto-asset issuers and platforms, to not implement or refuse to implement appropriate risk controls, arrange for effective governance, or take other available steps that would address the financial stability risks of their activities.

Many nonbank firms in the crypto-asset ecosystem have advertised themselves as regulated.

Firms often emphasize money services business regulation, though such regulation is largely focused on anti-money laundering controls or consumer protection requirements and does not provide a comprehensive framework for mitigating financial stability vulnerabilities arising from other activities that may be undertaken, for example, by a trading platform or stablecoin issuer.

While some firms in the crypto-asset ecosystem have attempted to avoid the existing regulatory system, other firms have engaged with the existing regulatory system by obtaining trust charters or special state-level crypto-asset-specific charters or licenses.

Compliance with and enforcement of the existing regulatory structure is a key step in addressing financial stability risks. For example, certain crypto-asset platforms may be listing securities but are not in compliance with exchange or broker-dealer registration requirements.
In addition, certain crypto-asset issuers have offered and sold crypto-assets in violation of federal and state securities laws, because the offering and sale were not registered or conducted pursuant to an available exemption.

Regulators have taken enforcement actions over the past several years to address many additional instances of non-compliance with existing rules and regulations, including illegally offered crypto-asset derivatives products, false statements about stablecoin assets, and many episodes of fraud and market manipulation.

In addition, false and misleading statements, made directly or by implication, concerning availability of federal deposit insurance for a given product, are violations of the law, and have given customers the impression that they are protected by the government safety net when they are not.

Further, misrepresentations by crypto-asset firms about how they are regulated have also confused consumers and investors regarding whether a given crypto-asset product is regulated to the same extent as other financial products.

Though the existing regulatory system covers large parts of the crypto-asset ecosystem, this report identifies three gaps in the regulation of crypto-asset activities in the United States.

First, the spot markets for crypto-assets that are not securities are subject to limited direct federal regulation. As a result, those markets may not feature robust rules and regulations designed to ensure orderly and transparent trading, prevent conflicts of interest and market manipulation, and protect investors and the economy more broadly.

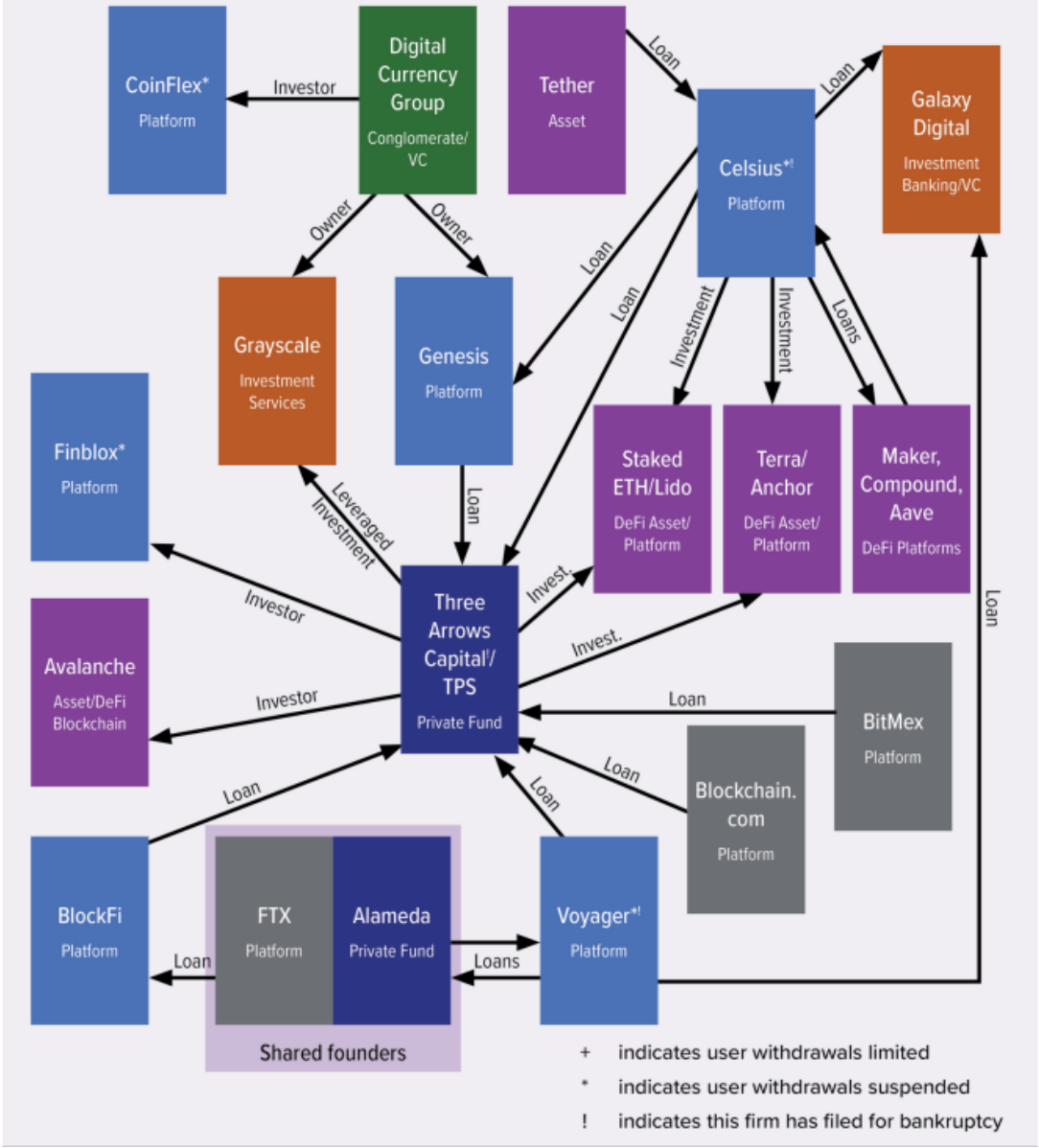
Second, crypto-asset businesses do not have a consistent or comprehensive regulatory framework and can engage in regulatory arbitrage. Some crypto-asset businesses may have affiliates or subsidiaries operating under different regulatory frameworks, and no single regulator may have visibility into the risks across the entire business.

Third, a number of crypto-asset trading platforms have proposed offering retail customers direct access to markets by vertically integrating the services provided by intermediaries such as broker-dealers or futures commission merchants. Financial stability and investor protection implications may arise from retail investors' exposure to certain practices commonly proposed by vertically integrated trading platforms, such as automated liquidation.

To ensure appropriate regulation of crypto-asset activities, the Council is making several recommendations in part 5 of this report, including the consideration of regulatory principles, continued enforcement of the existing regulatory structure, steps to address each regulatory gap, and bolstering member agencies' capacities related to crypto-asset data and expertise.

FSOC Report on Digital Asset Financial Stability Risks and Regulation

Figure B-1: Reported Interconnections of Three Arrows Capital



FSOC

FINANCIAL STABILITY OVERSIGHT COUNCIL

Report on Digital Asset Financial Stability Risks and Regulation 2022

The report: https://home.treasury.gov/system/files/261/FSOC-Digital-Assets-Report-2022.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.

Solvency II Association

At every stage of your career, our association provides networking, training, certification, information, updates, alerts, and services you can use. Join us. Stay current. Take advantage of the new opportunities. Read our monthly newsletter. Get certified.

You can explore what we offer to our members:

1. Membership – Become a standard, premium or lifetime member. You may visit: https://www.solvency-ii-association.com/How_to_become_member.htm

2. Monthly Updates – Visit the Reading Room of the association at: https://www.solvency-ii-association.com/Reading_Room.htm

3. Training and Certification – You may visit: https://www.solvency-ii-association.com/CSiiP_Distance_Learning_Online_Certification_Program.htm

For instructor-led training, you may contact us. We tailor Solvency II presentations, awareness and training programs for supervisors, boards of directors, employees, service providers and consultants.