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 2023

Dear members and friends,

The European Insurance and Occupational Pensions Authority (EIOPA) has outlined its strategic priorities for the period 2024 – 2026.

In a context of evolving challenges, risks and opportunities, EIOPA will focus on managing the uncertainty in times of transformation so that the insurance and pensions sectors can continue to deliver value to policyholders and beneficiaries, to business and the EU economy.

EIOPA has identified strategic priorities on which to focus:

1. Integrating sustainable finance considerations across all areas of work, including integrating ESG risks in the prudential frameworks on insurers and pension funds and addressing protection gaps.

2. Supporting the consumers, the market and the supervisory community through digital transformation, with a focus on defining the policy and implementing the Digital Operational Resilience

(DORA), the Artificial Intelligence Act and the European Single Access Point (ESAP).

3. Enhancing the quality and effectiveness of supervision, particularly in view of increased cross-border business, including the revision of the supervisory convergence materials considering the Solvency II review.

4. Ensuring technically sound prudential and conduct of business policy, including maintaining the integrity of the insurance regulatory framework as the review of Solvency II reaches its next stages.

5. Identifying, assessing, monitoring and reporting on risks to the financial stability and conduct of business and promoting preventative policies and mitigating actions, including the provision of timely and accurate financial stability analyses and risk assessments.

6. Providing effective recruitment, management and development of EIOPA's human capital to further enhance its position as an attractive employer.

More information on EIOPA's priorities can be found at:
https://www.eiopa.europa.eu/eiopa-sets-out-its-strategic-priorities-2024-2023-10-06_en

https://www.eiopa.europa.eu/system/files/2023-09/EIOPA%20Revised%20SPD%202024-2026.pdf

IAIS Newsletter September 2023

This month was marked by a series of productive committee, subcommittee, working group and task force meetings. Read the recaps to learn more about the current activities of the IAIS and what lies ahead.

Financial Stability Institute (FSI) Report

Financial Stability Institute | BIS

The Financial Stability Institute (FSI) was jointly created in 1998 by the Bank for International Settlements and the Basel Committee on Banking Supervision to assist supervisors around the world in improving and strengthening their financial systems.

New FSI Connect on operational resilience

Access to Insurance Initiative (A2ii) Report

access to insurance initiative

The Access to Insurance Initiative (A2ii) is a unique global partnership which inspires and supports insurance supervisors in promoting access to insurance for underserved and low-income populations. It is the IAIS implementation partner on financial inclusion.

To read more: https://www.iaisweb.org/uploads/2023/10/IAIS-Newsletter-Sept-2023.pdf

The EBA publishes 2023 list of third country groups and third country branches operating in the EU/EEA

The European Banking Authority (EBA) published the updated list of all third country groups (TCGs) with intermediate EU parent undertakings IPU(s), where applicable, and the list of all third country branches (TCBs) operating in the European Union and European Economic Area (EU/EEA).

This publication ensures that market participants have clarity on the direct ownership of the involved institutions.

BDT Capital Partners LLC	United States
Greenhill & Co. Inc.	United States
SKY Harbor Capital Management LLC	United States
Wellington Management Group LLP	United States
IBG LLC	United States
Brown Brothers Harriman & Co N.Y.	United States
Hamilton Lane Advisors L. L. C.	United States
DXC Technology Companyc	United States
Stifel Financial Corporation	United States
Northern Trust Corporation	United States
Jefferies Financial Group Inc.	United States
StoneX Group Inc.	United States
Citigroup Inc.	United States
The Goldman Sachs Group, Inc.	United States
Bank of America Corporation	United States
John Deere Capital Corporation	United States
Payden & Rygel	United States
Ford Motor Credit Company LLC	United States
International Business Machines Corp.	United States
The Bank of New York Mellon Corporation	United States
Warburg Pincus	United States
Morgan Stanley	United States
STATE STREET CORPORATION	United States
Wells Fargo & Company	United States
U.S. Bancorp	United States
Dell Inc	United States
Aon plc	United States
Cantor Fitzgerald LLP (US)	United States
Citadel Securities LP,	United States
Geneva Global Holdings, LLC	United States
Guggenheim Capital LLC	United States
Hudson River Trading LLC	United States
Berkshire Hathaway Inc	United States
Principal Financial Groupo Inc	United States
AllianceBernstein LP	United States
Virtu Financial, Inc.	United States
WisdomTree Investments Inc.	United States
Susquehanna International Holdings LLC	United States
KKR & Co. Inc.	United States

In the course of the 2023 exercise, 461 TCGs from 47 third countries have been identified as operational in the EU/EEA.

Out of them, 2 have an IPU in place. Moreover, 65 TCGs have branches in the EU/EEA with a total of 105 third country branches of credit institutions operating in the EU/EEA.

Legal basis and background

- According to Article 21b of Directive 2013/36/EU (Capital Requirements Directive - CRD), third country groups (TCGs) operating through more than one institution in the Union and with total assets of EUR 40 billion or more are required to have an intermediate EU parent undertaking (IPU).

- The EBA has a key role to play in facilitating cooperation between National Competent Authorities and in supporting their IPU decision-making process.

- In July 2021, the EBA Guidelines (EBA/GL/2021/08) provided a common methodology for the calculation of the total value of assets in order to achieve consistent application of Union law.

- In May 2022, the EBA published the decision (EBA/DC/441) on supervisory reporting for the threshold monitoring of the intermediate EU parent undertaking to ensure a timely application of the IPU requirement.

To read more: https://www.eba.europa.eu/eba-publishes-2023-list-third-country-groups-and-third-country-branches-operating-eueea

EIOPA consults on the supervision of captive (re)insurers with a focus on intra-group transactions, the prudent person principle and governance

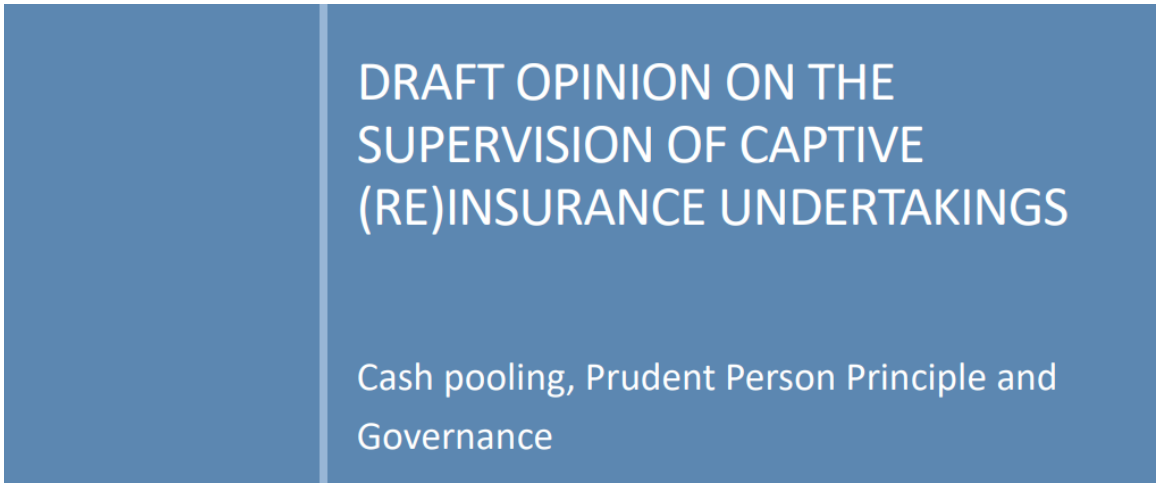
The European Insurance and Occupational Pensions Authority (EIOPA) launched a public consultation on its Opinion regarding the supervision of captive (re)insurance undertakings, with a particular view on intra-group transactions, the prudent person principle and governance.

This draft Opinion is addressed to competent authorities and outlines the supervisory expectations while taking into account the specificities of a captive (re)insurer's business model.

The Opinion aims at facilitating a risk-based and proportionate supervision of captive (re)insurance undertakings and further support the convergence of supervisory expectations in the context of creating a level playing field within the EU.

The Opinion sets out supervisory expectations in several areas, including intra-group transactions (especially cash pooling), the consistent application of the prudent person principle as well as governance-related aspects in connection with key functions and outsourcing requirements.

The Opinion seeks to ensure a high-quality and convergent supervision of captive (re)insurance undertakings and is part of EIOPA's priorities as defined in the 2022 and 2023 Supervisory Convergence Plans.



The Solvency II Directive takes account of the specific nature of captive insurance and captive reinsurance undertakings.

As those undertakings only cover risks associated with the industrial or commercial group to which they belong, appropriate approaches should be provided in line with the principle of proportionality to reflect the nature, scale and complexity of their business.

Captives (re)insurance undertakings are defined in Article 13(2) and 13(5) of the Solvency II Directive.

Supervision of the groups to which they belong is governed by Article 213(2)(d) in conjunction with Article 265 , according to which only intra-group transactions in the meaning of Article 13(19) are to be supervised.

The specific business model of captive (re)insurance undertakings aims to provide the industrial or commercial group to which they belong a cost-efficient risk financing program, namely to efficiently obtain coverage for their risks and be protected in case an event happens on a pooled basis, i.e. together with all companies and individuals of this group that might be impacted by such an event, or jointly take these risks or parts of these risks.

The peculiar aspects related to the business model of captive (re)insurance undertakings itself lead to specific supervisory expectations and the need to apply regulation proportionally.

This might raise concerns regarding the level playing field. The reliance on specific approaches and the potential for regulatory and supervisory arbitrage led EIOPA to issue this Opinion.

This Opinion aims at facilitating a risk-based and proportionate supervision of captive (re)insurance undertakings and further harmonise, in the context of creating a level playing field within the EU, supervisory expectations in the topics touched upon.

While further convergence of supervisory practices is needed, National Competent Authorities (NCAs) may take into account national specificities of the captive (re)insurance sector when implementing the principles included in this Opinion.

The Solvency II framework is principle based and takes particular account of the principle of proportionality. It has already led to some simplifications, for example for the calculation of the Solvency Capital Requirement of captive (re)insurance undertakings.
Additional proportionality measures are being discussed under the review of Solvency II.

This Opinion aims at supporting the implementation of the regulatory framework with a focus on intragroup transactions (especially cash

pooling), on the consistent application of the Prudent Person Principle and on governance-related aspects in connection with key functions and outsourcing requirements, taking into account the proportionality principle.

To read more: https://www.eiopa.europa.eu/eiopa-consults-supervision-captive-reinsurers-focus-intra-group-transactions-prudent-person-2023-10-06_en

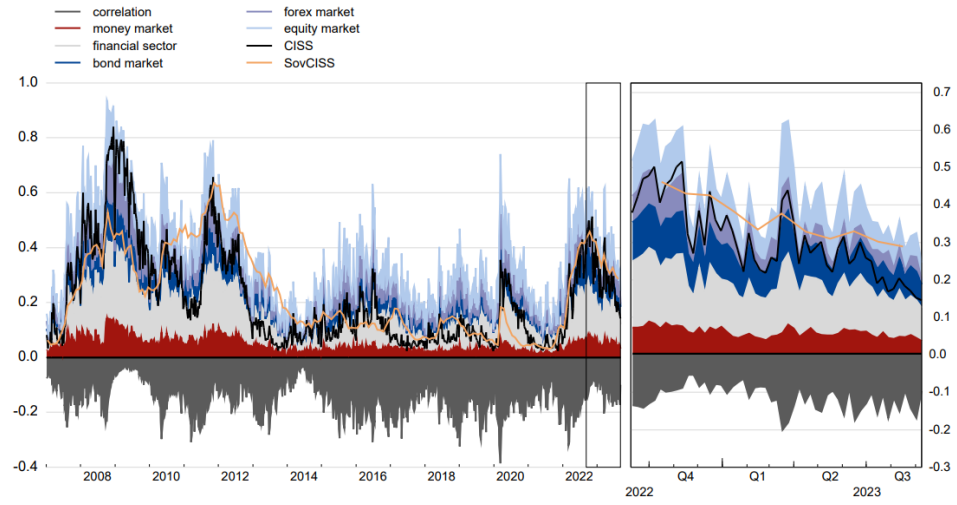
Risk Dashboard

ESRB
European Systemic Risk Board
European System of Financial Supervision

The ESRB risk dashboard is a set of quantitative and qualitative indicators of systemic risk in the EU financial system. It is published quarterly, one week after its adoption by the General Board, and is accompanied by two annexes that explain the methodology and describe the indicators.

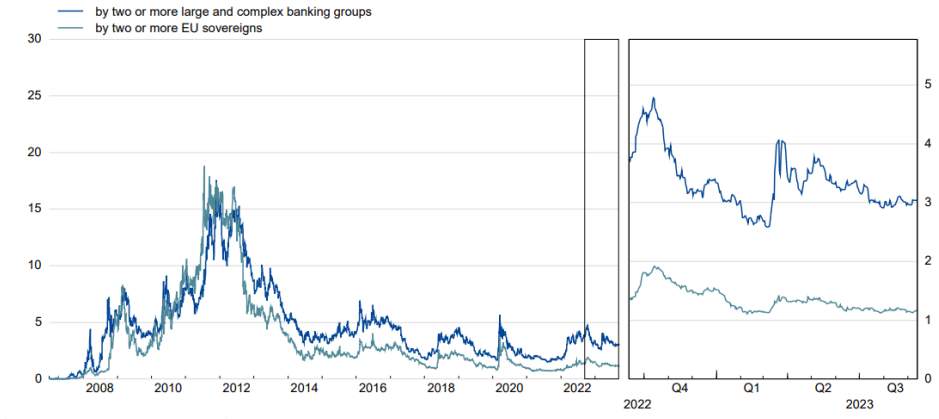
The risk dashboard should not be considered to be a policy statement on systemic risks. Additional indicators that support systemic risk assessment in the EU financial system are available in the Macro-prudential database maintained by the ECB.

1.1 Composite indicator of systemic stress
(Last observation: 8 Sep. 2023)

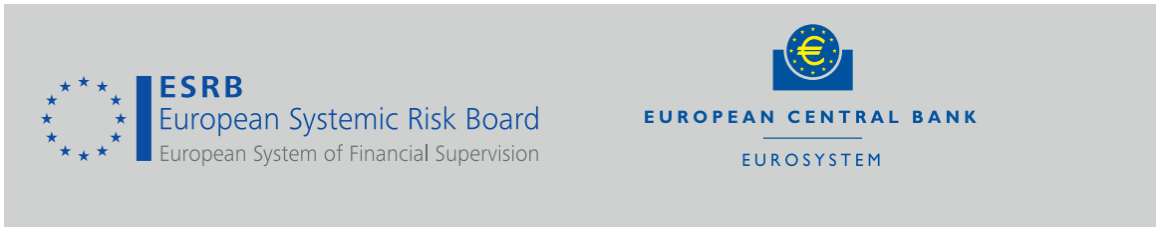


Sources: Thomson Reuters, ECB and ECB calculations.
Notes: The CISS is unit-free and constrained to lie within the interval (0, 1). See Hollo, D., Kremer, M. and Lo Duca, M., "CISS - a composite indicator of systemic stress in the financial system", Working Paper Series, No 1426, ECB, March 2012. The Sovereign CISS applies the same methodological concept of the CISS. On aggregation of different measures of stress in different euro area sovereign bond markets see Garcia-de-Andoain, C. and Kremer, M., "Beyond spreads: measuring sovereign market stress in the euro area", Economics Letters, Vol. 159, 2017, pp. 153-156.

1.2 Probability of a simultaneous default
(Percentages; last observation: 12 Sep. 2023)



Sources: Bloomberg, Thomson Reuters and ECB calculations.
Note: See Box 8, Financial Stability Review, ECB, June 2012.



ESRB risk dashboard

To read more: https://www.esrb.europa.eu/pub/rd/html/index.en.html

Risk classification for the insurance industry: more clarity

German Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht).

BaFin Federal Financial Supervisory Authority

BaFin is becoming more transparent in its supervisory practice: in future, it will inform insurance companies, pension funds and insurance groups of their individual risk scores. To date, it only reports the results for the entire sector.

BaFin uses an internal classification procedure to assess the risks that insurance companies, pension funds and insurance groups currently face or might face in future. The procedure enables BaFin to manage its supervision, facilitating decisions such as how frequently, extensively and intensively companies are to be analysed or inspected on site.

To date, BaFin has only published aggregated results of its risk classification in its annual reports. In future, it will communicate and explain the individual risk scores to the supervised entities and groups in bilateral discussions. This will provide the supervised entities with even more clarity about where BaFin sees their main weaknesses and strengths.

The additional information will make supervisory action more transparent and more understandable for the companies and groups. It will also stimulate the dialogue between supervisors and companies. Companies will be given the opportunity to respond more quickly to BaFin's assessments of company-specific developments. Importantly, however, supervised entities are not allowed to publish the risk classification results or to use them for advertising purposes.

How risk classification works

The risk classification procedure is based on the guidelines of the European Insurance and Occupational Pensions Authority (EIOPA) on the supervisory review process. It takes into account the nature, scale and complexity of the business activities conducted by the companies and groups, as well as the risks associated with such business activities. BaFin bases the score on two factors: market impact and quality.

EIOPA-BoS-14/179 EN

Guidelines on supervisory review process

To analyse market impact, BaFin applies a four-tier scale to assess the effects that the problems of a company or group could have on the stability of the financial system.

The impact for tier 1 is low; for tier 2, medium; for tier 3, high; for tier 4, very high. BaFin generally uses thresholds for this assessment.

Depending on the segment, this may be the total of all investments or of the gross premium income written, for example.

BaFin classifies the quality of the companies and groups on a scale from A to D, with A being of high quality and D of low quality. The supervisors determine the overall score on the basis of the following categories: “net assets and financial position”, “results of operations”, “system of governance”, “future viability” and “holders of significant holdings”. For insurance groups, instead of using the category “holders of significant holdings”, BaFin uses the category “group-specific factors”.

BaFin determines the scores for the first two categories using insurance-specific indicators. The two categories “system of governance” and “holders of significant holdings” are assessed with the help of qualitative criteria, such as shortcomings in the risk management system.

The “future viability” category comprises quantitative or qualitative criteria for specific classes of insurance that are suitable for assessing the

company's/the group's prospective development. In addition, for "group-specific factors", BaFin assesses all group-specific aspects going above and beyond the first four categories.

IT-based assessment system

For a consistent approach, BaFin uses an IT-based assessment system. The system is calibrated using long-term industry values and proposes scores based on the key indicators. In addition to these indicators, supervisors take into account various additional indicators and information for the overall score. Should supervisors consider individual aspects to be of particular importance, they may give greater weight to those aspects.

In order to understand the risk classification, it is important to consider that the scores only reflect the status as at the most recent regular assessment. In most cases, this is 30 September.

If BaFin subsequently receives new information about a supervised entity or a group that significantly changes its assessment, it can carry out an ad hoc risk classification. This may also give rise to a change in the risk classification score between two reference dates.

Essential information may include the approval or discontinuance of a business line, changes in ownership structure, portfolio transfers as well as significant new findings regarding the financial situation or the system of governance in place at an entity or group.

When does BaFin inform companies of their scores?

BaFin decides when it will inform the companies and groups of their risk classification results. However, BaFin is careful to ensure that the scores are as up-to-date as possible. In the case of insurance groups, BaFin aims to report the results of the group and those of the group's individual entities at the same time.

BaFin's explanations of the score may be more or less comprehensive, depending on the risk situation of the company or group. At a minimum, BaFin explains the overall score and its main reasons for the result. As to the level of detail used to explain the scores for individual categories, this is left to the discretion of the competent supervisor. The focus will be on the weaknesses, i.e. the categories with a score of C or D, as well as decisive and/or particularly poor indicators with a score of C or D.

In the event that scores are good (A or B), BaFin will probably only briefly mention the key indicators. BaFin will not publicly disclose details of the

calculation and weighting of the indicators or the weightings of the individual categories.

To read more:
https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2023/fa_bj_2309_Risikoklassifizierung_Assekuranz_en.html

Crypto-assets regulation: from patchwork to framework

DeNederlandscheBank
EUROSYSTEEM

Hello everyone – offline, and also, hello everyone online.

It is a pleasure to be back in London. Back at the Bank of England. Back at the 'Old Lady of Threadneedle Street'. The Old Lady that battles inflation, safeguards financial stability and firmly protects… the gold in her vaults. Gold that lies right here, under our feet. 400 000 bars of gold, to be precise.

Now, I am not here to take a peek at that small fraction of gold that is ours. No, today, I was invited to talk about a new type of gold – or, at least, to some it is. I am referring to crypto-assets. Something the Financial Stability Board has consistently been monitoring since 2018.

For a long time, crypto-assets were an experiment on the fringes of the financial system. No shop owner would accept bits and bytes instead of cash or card.

But soon, certain illicit online marketplaces got wind of this new digital asset: selling illegal services or products online had never been this easy. So, regulators and law enforcement agencies sprang into action and took coordinated action to combat money laundering.

Nonetheless, in those early days, chances were very slim that someone had heard of bitcoin or ether, let alone owned them.

And then suddenly – seemingly overnight – crypto-assets became the talk of the town, and everybody seemed to wonder: is this the new gold?

As a result, the total market capitalization of crypto-assets exploded. At the same time, ties with traditional financial parties grew. As did the interest in the underlying technologies.

When the 'crypto winter' hit us last year, it became crystal clear however, that not all that glitters is gold. A sudden change in investor sentiment caused a sharp decrease in crypto-asset prices. That, in turn, led to the spectacular failure of several crypto-intermediaries. Total crypto-asset market capitalization was never really able to recover after that.
But even as crypto-asset prices are in a rut presently, crypto-asset market structures continue to develop at a rapid pace. And at the same time, we

see a growing involvement of traditional finance with the crypto-ecosystem – which means that the financial interlinkages between these two worlds are growing as well.

So we cannot exclude that, sooner rather than later, vulnerabilities in crypto-asset markets become big enough to form an actual, transmissible risk to global financial stability. And this risk looms larger if we don't implement comprehensive regulation.

All over the world, national regulators have not been waiting on me to say this. A lot of decisive action has been taken already.

The FSB welcomes these initiatives because they show much-needed willingness to act.

But at the same time, we see a challenge due to crypto's inherent global reach. And that is: how do we ensure consistency between all these regulations?

And how do we deal with crypto parties that choose to operate exactly from those jurisdictions that don't really prioritise the effective regulation and supervision of crypto-asset activities?

To overcome these challenges, the FSB developed a Global Regulatory Framework. This framework, published last July, aims to promote the consistency of regulatory and supervisory practices to address the financial stability risks of crypto-asset activities.

Developing this framework on the basis of consensus among the FSB member authorities has required a careful threading of the needle. And so, I think it is fitting that we find ourselves on Threadneedle Street, today. The perfect place to discuss the FSB's finalized policy work on broader crypto-asset markets and global stablecoin arrangements.

The latter is a specific type of crypto-asset – one that aims to maintain a stable value relative to a pool of assets, usually fiat money. One that carries heightened risks to global financial stability because of its potential systemic relevance in multiple jurisdictions. And so, one that requires special attention.

Because the FSB recommendations are high-level, national authorities can apply these recommendations flexibly, whilst also ensuring a baseline – a baseline that provides for a consistent application of comprehensive regulation across the globe. A baseline that embraces both already existing rules in some countries, and to be drafted regulations in others. A baseline

with a clear thread of gold – and that is the principle of "same activity, same risk, same regulation".

Many crypto-asset activities perform functions and, hence, carry risks, that strongly resemble those of traditional financial activities. Think, for example, of the similarities between staking and deposit-taking, or between crypto-lending and securities financing transactions. And so, we believe they should be regulated as such.

A number of our recommendations have to do with the vulnerabilities of centralized crypto-asset intermediaries. And I stress 'centralized' because, however 'de-centralized' the crypto-asset ecosystem claims to be, economic reality tells a different story. In fact, some of these intermediaries already seem to play a systemic role within the crypto-ecosystem.

That is why we recommend that authorities require a number of things from these entities. For instance to have in place robust governance frameworks and to set up risk management practices.

Of course, I know that implementation takes time. But I also know it's high time – as I have often heard my British colleagues say – to 'crack on'. So, let's prioritise the full and consistent implementation of our high-level recommendations.

Because in the meantime, people investing in crypto-assets continue to run serious risks. In the meantime, linkages between the crypto-ecosystem and traditional finance may very well continue to grow. So, in the meantime, risks to financial stability can still escalate.

There are several ways through which we can prevent crypto-asset volatility from spilling over to the traditional financial system. One important way to do this, is with the full and consistent implementation of the BCBS prudential framework for the treatment of banks' crypto-asset exposures.

Putting this global framework into practice limits the chance that crypto-volatility reaches banks and hence becomes a threat to financial stability.

To keep a close eye on the progress made, the FSB will start monitoring implementation. Our first review should be finalized by the end of 2025.

And the FSB will not only monitor progress. If we are serious about regulating what is essentially a cross-border phenomenon, we also need to be serious about cross-border cooperation. About information sharing. About working together.

This also means that we need to venture outside of the FSB jurisdictions. Because several jurisdictions with material crypto-asset activities are not members of the FSB.

Nevertheless, global financial stability ties all of us together. And to safeguard that stability, the FSB members need to engage with these jurisdictions. We need to ensure the needle of their regulatory compass points in the same direction as ours.

To do so, we want to start with positive incentives like outreach, technical workshops, and capacity building to get them prepared. We'll work closely with the IMF, the World Bank and other international organizations on this.

However, chances are we may still see regulatory competition. And so, we cannot exclude that a toughening of regulation in one part of the world pushes crypto-asset parties to relocate to other parts of the world. Parts of the world with weaker regulatory standards.

What we can do, though, is require that traditional financial institutions take additional measures to manage the risks of interacting with crypto intermediaries operating in such jurisdictions. Measures necessary to protect global financial stability. We are not there yet, but if you ask me, we should be heading in that direction.

Just like crypto-asset threats don't stop at national borders, the thread of crypto-asset risks doesn't only weave through financial stability. There are also macroeconomic risks. Specifically for emerging markets and developing countries.

In EMDEs, crypto-assets are relatively popular. The more popular they are, the more they could erode the effectiveness of domestic monetary policy. Because people may start preferring crypto-assets or stablecoins over domestic currencies.

This risk of currency substitution, or so-called 'crypto-ization', means EMDE's might face even greater risks from crypto-assets than advanced economies. A potentially dangerous cocktail of financial stability and macroeconomic risks.

For this reason, the Indian G20 Presidency asked the FSB and the IMF to combine their work on this subject in a synthesis paper. This was published in September. A key conclusion is that crypto-assets do indeed have implications for macroeconomic and financial stability, but even more, that these implications are mutually interactive and reinforcing.

In our view, this underlines, once more, the need for a global regulatory and supervisory baseline to oversee crypto-asset activities.

A baseline that addresses both financial stability and macroeconomic risks. A baseline that all national regulators can adhere to, but at the same time allows them to take targeted and time-bound measures to address jurisdiction-specific circumstances.

To help EMDEs address these serious risks to financial stability, the FSB will investigate how cross-border cooperation between advanced and developing economies can practically be enhanced.

Dear colleagues, today, I've talked about crypto-assets – a concept that is not even 20 years old. The Bank of England's nickname, the 'Old Lady of Threadneedle Street', dates back more than two hundred years. To 1797.

When crypto-assets were still the distant future. Banknotes could still be converted to gold. And France declared war on Britain, and landed on its shores.

Within hours, people rushed to the Bank of England. Asking for gold. The very gold that lies under our feet. And the famous vaults were rapidly emptying out.

Then-prime minister, William Pitt the Younger, tried to put a halt to that. Not because he wanted to preserve gold for financial stability reasons, but to use it to defend Britain. In a famous cartoon, probably familiar to many of you, you can see William Pitt the Younger trying to 'woo' an old lady (more information(Refers to an external site)).

But in fact, all he wants, is the gold in her pockets and in the chest she sits on. Of course, she is not inclined to give in. Ever since, the Bank of England has been known as the 'Old Lady of Threadneedle Street'.

Today, the 'Old Ladies' many of us work for, will no longer exchange banknotes for gold. But still people look for stable assets – assets that maintain their value over time and allow them to transact with people from around the globe.

Today, these 'Old Ladies', can still not easily be 'woo-ed'. And remain firmly seated on their chests of gold – or, rather, vaults. And today, once more, these 'Old Ladies' are willing to defend what knits us all together and helps to bring global prosperity – and that's financial stability. Thank you.

To read more: https://www.dnb.nl/en/general-news/speech-2023/crypto-assets-regulation-from-patchwork-to-framework/

EIOPA launches survey on access to cyber insurance by SMEs

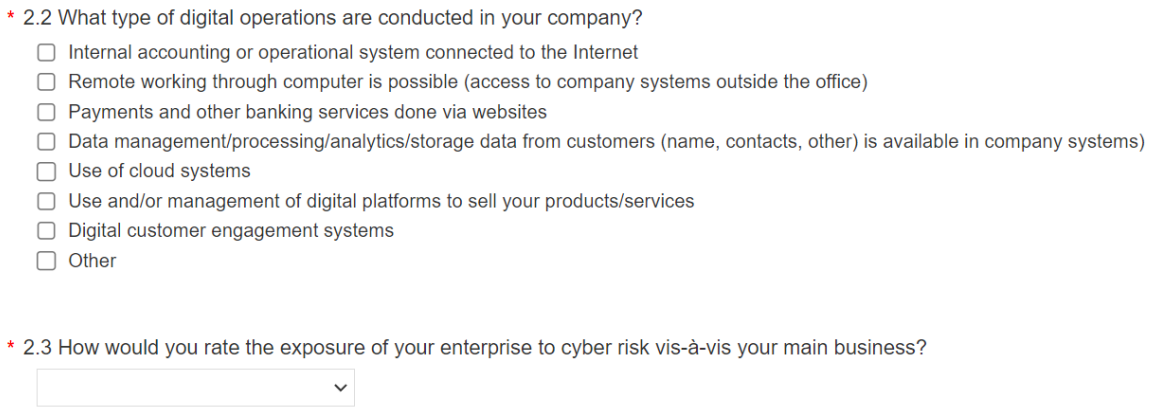
The European Insurance and Occupational Pensions Authority (EIOPA) launched a survey on access to cyber insurance by Small and Medium Enterprises (SMEs) to gain deeper insights into the challenges small businesses face in protecting themselves from cyber risks and to evaluate the level of access to cyber insurance.

Access to (cyber) insurance coverage plays a significant role in mitigating risks stemming from digitalisation by absorbing shocks and managing risks associated with irregular and unpredictable income. Insurance can make SMEs resilient to shocks, also making them more financially sound.

The survey will gather information on the size and type of business of the surveyed enterprises, the level of cyber risk awareness vis-à-vis their business, the availability, affordability, and understanding of cyber insurance products.

It will also shed light on the experience and perceptions of SMEs regarding cyber insurance, including whether they have considered purchasing a policy, the factors that influenced their decision (not) to purchase coverage, and the potential barriers to access.

The survey is available in all 24 official EU languages, and SMEs are invited to take part until 20 March 2024.



The survey:
https://ec.europa.eu/eusurvey/runner/SMESurveyCyberInsurance2023

* 2.4 What are the main cyber risks that your company might face, considering the digital operations (as identified above) it performs?

- ☐ Phishing attempts (Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually performed through email to steal sensitive data or to install malware on the victim's machine)
- ☐ Malware attacks (Malware attacks are any type of malicious software designed to cause harm or damage to a computer, server, client or computer network and/or infrastructure without end-user knowledge It is most frequently used to steal personal, financial or business information)
- ☐ Network security breaches (A network security breach is any unauthorized access to a device, network, program, or data. Security breaches happen when network or device security protocols are penetrated or otherwise circumvented)
- ☐ Data breaches (A data breach is a security incident in which malicious insiders or external attackers gain unauthorized access to confidential data or sensitive information such as medical records, financial information or personally identifiable information)
- ☐ Insider data theft, including the leak of clients' personal information (Insider data theft may be due to a malicious employee taking or selling your corporate data or simply making an unintentional mistake)
- ☐ Ransomware (Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files until a ransom is paid)
- ☐ Attacks through third-party provider (A third-party provider attack is a form of a cyberattack that originates through third party vendors)
- ☐ Denial of Service attacks (A Denial-of-Service attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users)
- ☐ Other

To read more: https://www.eiopa.europa.eu/eiopa-launches-survey-access-cyber-insurance-smes-2023-09-20_en

CFPB Issues Guidance on Credit Denials by Lenders Using Artificial Intelligence

Consumers must receive accurate and specific reasons for credit denials

The Consumer Financial Protection Bureau (CFPB) issued guidance about certain legal requirements that lenders must adhere to when using artificial intelligence and other complex models.

The guidance describes how lenders must use specific and accurate reasons when taking adverse actions against consumers.

This means that creditors cannot simply use CFPB sample adverse action forms and checklists if they do not reflect the actual reason for the denial of credit or a change of credit conditions.

This requirement is especially important with the growth of advanced algorithms and personal consumer data in credit underwriting.

Explaining the reasons for adverse actions help improve consumers' chances for future credit, and protect consumers from illegal discrimination.

"Technology marketed as artificial intelligence is expanding the data used for lending decisions, and also growing the list of potential reasons for why credit is denied," said CFPB Director Rohit Chopra. "Creditors must be able to specifically explain their reasons for denial. There is no special exemption for artificial intelligence."

In today's marketplace, creditors are increasingly using complex algorithms, marketed as artificial intelligence, and other predictive decision-making technologies in their underwriting models.

Creditors often feed these complex algorithms with large datasets, sometimes including data that may be harvested from consumer surveillance.

As a result, a consumer may be denied credit for reasons they may not consider particularly relevant to their finances.

Despite the potentially expansive list of reasons for adverse credit actions, some creditors may inappropriately rely on a checklist of reasons provided in CFPB sample forms. However, the Equal Credit Opportunity Act does not allow creditors to simply conduct check-the-box exercises when

delivering notices of adverse action if doing so fails to accurately inform consumers why adverse actions were taken.

In fact, the CFPB has confirmed in a circular from last year, that the Equal Credit Opportunity Act requires creditors to explain the specific reasons for taking adverse actions.

CFPB Acts to Protect the Public from Black-Box Credit Models Using Complex Algorithms

Companies relying on complex algorithms must provide specific and accurate explanations for denying applications

MAY 26, 2022

You may visit: https://www.consumerfinance.gov/about-us/newsroom/cfpb-acts-to-protect-the-public-from-black-box-credit-models-using-complex-algorithms/

This requirement remains even if those companies use complex algorithms and black-box credit models that make it difficult to identify those reasons. Today's guidance expands on last year's circular by explaining that sample adverse action checklists should not be considered exhaustive, nor do they automatically cover a creditor's legal requirements.

Specifically, today's guidance explains that even for adverse decisions made by complex algorithms, creditors must provide accurate and specific reasons. Generally, creditors cannot state the reasons for adverse actions by pointing to a broad bucket.

For instance, if a creditor decides to lower the limit on a consumer's credit line based on behavioral spending data, the explanation would likely need to provide more details about the specific negative behaviors that led to the reduction beyond a general reason like "purchasing history."

Creditors that simply select the closest factors from the checklist of sample reasons are not in compliance with the law if those reasons do not sufficiently reflect the actual reason for the action taken.

Creditors must disclose the specific reasons, even if consumers may be surprised, upset, or angered to learn their credit applications were being graded on data that may not intuitively relate to their finances.

In addition to today's and last year's circulars, the CFPB has issued an advisory opinion that consumer financial protection law requires lenders to provide adverse action notices to borrowers when changes are made to their existing credit.

CFPB Issues Advisory Opinion on Coverage of Fair Lending Laws

Equal Credit Opportunity Act continues to protect borrowers after they have applied for and received credit

MAY 09, 2022

You may visit: https://www.consumerfinance.gov/about-us/newsroom/cfpb-issues-advisory-opinion-on-coverage-of-fair-lending-laws/

The CFPB has made the intersection of fair lending and technology a priority.

For instance, as the demand for digital, algorithmic scoring of prospective tenants has increased among corporate landlords, the CFPB reminded landlords that prospective tenants must receive adverse action notices when denied housing.

The CFPB also has joined with other federal agencies to issue a proposed rule on automated valuation models, and is actively working to ensure that black-box models do not lead to acts of digital redlining in the mortgage market.

To read more: https://www.consumerfinance.gov/about-us/newsroom/cfpb-issues-guidance-on-credit-denials-by-lenders-using-artificial-intelligence/

FDIC Launches Public Campaign to Raise Awareness About Deposit Insurance

Federal Deposit Insurance Corporation (FDIC)

To increase the public's awareness of deposit insurance and how it can protect people's money in the event of a bank's failure, the Federal Deposit Insurance Corporation (FDIC) launched a national campaign, "Know Your Risk. Protect Your Money."

What Does Deposit Insurance Cover?

FDIC deposit insurance protects money you hold at an FDIC-insured bank in traditional deposit accounts like:

- Checking accounts,
- Savings accounts,
- Money market deposit accounts (MMDAs), and
- Certificates of deposit (CDs).

Coverage is automatic when you open one of these types of accounts at an FDIC-insured bank. Learn more about what's covered:

Are My Accounts Covered? >
Is My Bank Insured? >
How Much of My Money is Insured? >

What Financial Products are Not Covered?

The FDIC only insures your money if it is in a deposit account at an FDIC-insured bank. Banks offer some financial products and services that are not deposits, and the FDIC does not insure them. These include:

- Mutual funds
- Annuities
- Life insurance policies
- Stocks and bonds
- Crypto assets
- Municipal securities
- Safe deposit contents

What FDIC Insurance Doesn't Cover >

The consumer-focused campaign aims to reach those who may have lower confidence in the U.S. banking system or who are unbanked, as well as those who use mobile payment systems, alternative banking services and financial products that may appear to be FDIC-insured but are not.

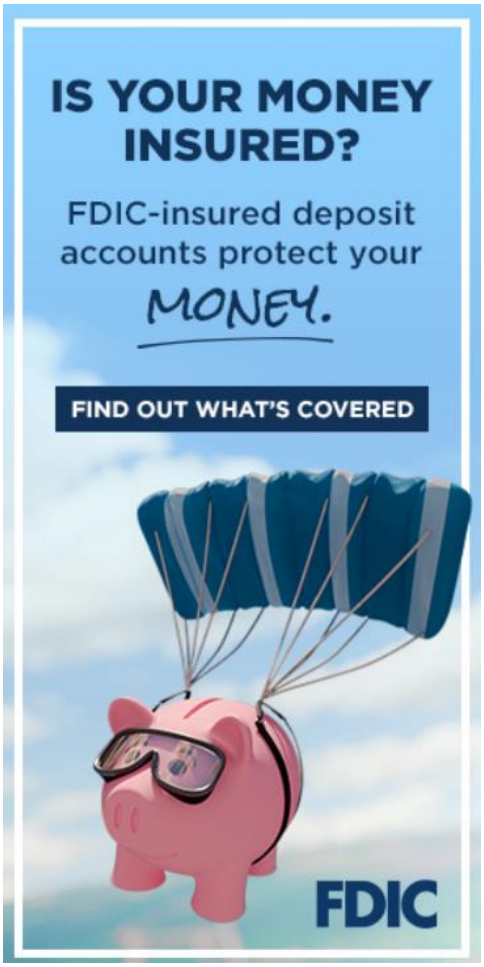
"Consumers today have a variety of options for where they can put their money. Evidence suggests many people may be confused whether their funds are protected by deposit insurance," said FDIC Chairman Martin J. Gruenberg. "In light of concerns raised by the bank failures earlier this year, this is an important moment for the FDIC to reach out to the public and ensure that more consumers understand deposit insurance and how it protects their money."

Following three regional bank failures earlier this year, a Gallup poll found nearly half of Americans surveyed are worried about the safety of their money deposited into banks and other financial institutions.

This uncertainty also suggests a significant percentage of those surveyed are unaware money deposited into an FDIC-insured bank is protected up to at least $250,000. More than 99 percent of deposit accounts in the U.S. today are under this deposit insurance coverage limit and are fully

protected by the FDIC. Since the FDIC's creation 90 years ago, no depositor has lost a penny of their insured deposits.

The FDIC has also observed an increasing number of instances online where firms or individuals have misused the FDIC's name or logo, or have made false or misleading representations about deposit insurance, raising confusion among consumers about the insurability of nonbanks and crypto-assets.



To determine if an institution is FDIC-insured, you can ask a representative of the institution, look for the FDIC sign at the institution, or use the FDIC's BankFind tool. Learn more about FDIC deposit insurance and which financial products are covered.

The FDIC's public awareness campaign features a piggy bank, which is commonly associated with money and personal savings, placed in potentially risky situations. Recognizing that many Americans may be putting their money at risk, the advertisements emphasize, "Know Your Risk. Protect Your Money."

The campaign consists of digital display ads, including web banners, as well as search engine marketing and sponsored social media that connect consumers to deposit insurance information and resources on the FDIC's website in English and Spanish. The digital campaign will run through November and will resume in January 2024 with the start of traditional tax filing season and when many consumers receive refund payments.

For more information or to access campaign resources and toolkits, please visit FDIC.gov/news/campaigns/know-your-risk and follow on social media at #IsYourMoneyInsured

About the FDIC:

The Federal Deposit Insurance Corporation (FDIC) is an independent agency created by the Congress to maintain stability and public confidence in the nation's financial system. The FDIC insures deposits; examines and supervises financial institutions for safety, soundness, and consumer

protection; makes large and complex financial institutions resolvable; and manages receiverships.

To read more: https://www.fdic.gov/news/press-releases/2023/pr23083.html

BIS Quarterly Review, September 2023
International banking and financial market developments

BIS

Resilient risk-taking in financial markets

With the end of the hiking phase in sight, investors focused on macroeconomic developments during the review period, while staying attuned to their policy implications.

Government bond yields rose in advanced economies (AEs), with term structures reflecting increasingly diverse economic outlooks.

Despite a spell of derisking in August, risk-taking was generally resilient, including in emerging market economies (EMEs).

Notable differences marked the evolution of government bond yields in China, the euro area and the United States.

While US long-term yields reached highs not seen since before the Great Financial Crisis, such yields barely rose in the euro area.

These dissimilar paths were driven by inflation-adjusted, ie real, yields consistent with a stronger economic outlook in the US than in the euro area.

As short-term rates rose in the euro area on the back of stubborn inflation, the term structure there inverted further.

Bond yields largely declined in China, amid a faltering recovery from Covid restrictions and monetary policy easing.

US Treasuries were at the centre of heightened market volatility in early August. Yield rises accelerated as investors became more convinced that higher rates were here to stay following better than expected US growth numbers.

In addition, several, almost concurrent announcements fueled investor unease and led to a sell-off: an unexpected increase in the issuance of long-dated bonds by the US government; the greater flexibility in the Bank of Japan's yield curve control policy; and a downgrade of the US sovereign credit rating.

The upward pressure on US yields spilled over to other AE government bond markets. Risky assets held up firmly, but also exhibited some divergence across major economies due to the differing outlooks.

Consistent with developments in core bond markets, stock returns were higher in the US than in the euro area and China.

Likewise, sentiment in corporate credit markets seemed to improve in the US but remained relatively subdued in the euro area. US credit spreads narrowed below historical landmarks and issuance gained some traction.

In contrast, bank lending to firms was still sluggish across jurisdictions. Financial market developments in EMEs reflected a new phase of monetary policy across most jurisdictions as well as external factors.

Short yields fell as the monetary policy stance began to turn, with most central banks pausing rate hikes or implementing cuts.

Risk-taking continued, with higher-yielding currencies attracting capital inflows.

In August, EME spreads and exchange rates also appeared sensitive to the temporary bout of de-risking in AE financial markets: the appreciation of Latin American currencies came to a halt, speculative positions in currency futures declined, and the rise of long-term yields accelerated.

In addition, headwinds seemed to emerge from China's slowdown.

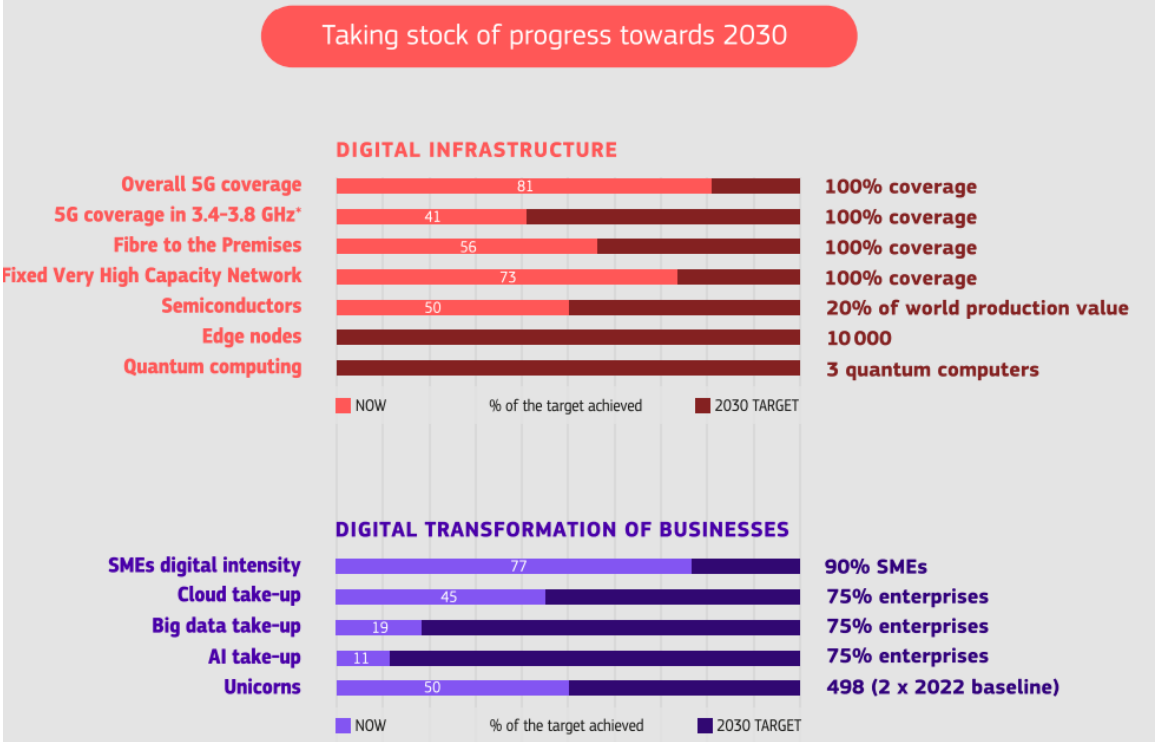
International banking and financial market developments

Special features

To read more: https://www.bis.org/publ/qtrpdf/r_qt2309.pdf

27 September 2023 - The first State of the Digital Decade report

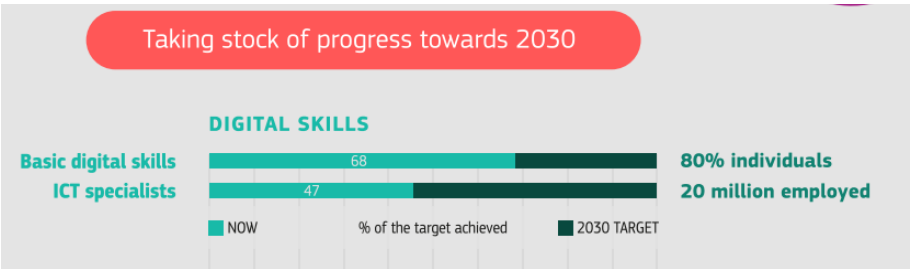
1. Introduction: Delivering the Digital Decade



The first State of the Digital Decade report takes stock of the EU's progress towards a successful digital transformation for people, businesses, and the environment as set out in the Decision establishing the Digital Decade Policy Programme 2030 ("the Digital Decade Decision").

It reviews digital policy developments and describes how the EU is advancing towards the agreed targets and objectives, thus outlining where the EU stands at the outset of the implementation of the Digital Decade Policy Programme.

The overall analysis of the EU's progress against the Digital Decade objectives and targets is shown in Figure 1 and the country reports presented in an annex to this report provide a more detailed picture.



3.3 DIGITAL DECADE OBJECTIVE: CYBERSECURITY

The global cyber threat landscape continues to be volatile, with a rise in cyberthreats of 150% in a year [69], in particular distributed denial of service (DDoS) attacks and an estimated 280 ransomware incidents attacks per month [70]. During 2021, 22.2% of EU enterprises experienced an ICT security-related incident leading to unavailability, destruction or corruption of data, or the disclosure of confidential data [71]. Increased dependencies and the development of new technologies, such as quantum computing and AI, add complexity to the threat landscape and introduce new risks for which further preparedness is needed.

While cybersecurity is not included as a target for 2030, improving resilience to cyberattacks, contributing to increasing risk-awareness and the knowledge of cybersecurity processes, and increasing the efforts of public and private organisations to achieve at least basic levels of cybersecurity is one of the general objectives set out in the Digital Decade Decision [72]. Moreover, the Digital Decade Decision points to the development of a possible specific target as part of its review planned in 2026 [73].

To read more: https://digital-strategy.ec.europa.eu/en/library/2023-report-state-digital-decade

Project Mariana: BIS and central banks of France, Singapore and Switzerland successfully test cross-border wholesale CBDCs

Foreign exchange (FX) is the largest financial market in the world, trading about $7.5 trillion a day (BIS (2022b)).

It operates 24 hours a day, five and a half days a week.

Project Mariana looks to the future and envisions a world in which central banks have issued central bank digital currencies (CBDCs) and explores how foreign exchange (FX) trading and settlement might look.

Mariana borrows ideas and concepts from decentralised finance (DeFi) and studies whether so-called automated market-makers (AMMs) can simplify FX trading and settlement with a view to enhancing market efficiency and reducing settlement risk.

Project Mariana is a proof of concept (PoC) for a global interbank market for spot FX featuring both an AMM and wholesale CBDCs (wCBDCs).

In the PoC, wCBDCs circulate on domestic platforms and so-called bridges allow them to be moved on to a transnational network that hosts the AMM.

Project Mariana extends previous experimentation on cross-border settlement using wCBDC arrangements and distributed ledger technology.

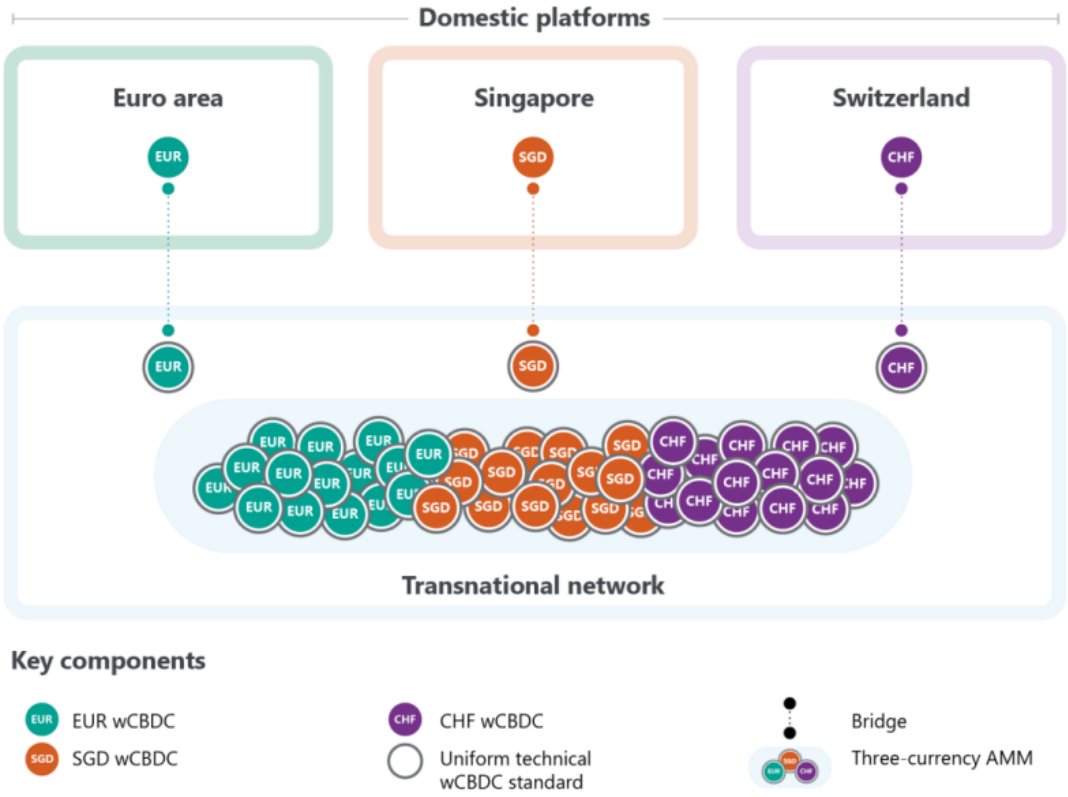
It successfully demonstrates the technical feasibility of the proposed architecture and adds novel insights on the potential of tokenisation in three dimensions.

First, wCBDCs are implemented as smart contracts, enabling central banks to manage their wCBDC without the need to directly operate or control the underlying platform.

Their design followed best practices from the public blockchain space, building on a widely used standard (ie ERC-20), as well as enabling upgradeability.

Second, bridges may serve as a mechanism to enable broader interoperability in an emerging tokenised ecosystem.

Mariana high-level architecture Graph 1



As implemented in the PoC, they may enable the seamless and safe transfer of wCBDC between domestic platforms and the transnational network without manual intervention.

The bridge design features controls and safeguards and ensures resilience through on-chain (ie bridge smart contracts) and off-chain (ie communication between bridge smart contracts) infrastructure managed by central banks.

Third, the AMM, as tested and calibrated in Mariana, fulfilled requirements based on selected FX Global Code (FXGC) principles. It delivers the contours of a possible future tokenised FX market that has a number of potential benefits.

These include supporting simple and automated execution of FX transactions, providing options to broaden the range of currencies, eliminating settlement risk and enabling transparency.

However, the use of AMMs requires the pre-funding of liquidity and their adoption would therefore entail a significant departure from the ex post funding (deferred net settlement) in use in today's FX markets.

To learn more: https://www.bis.org/publ/othp75.pdf

ESAs specify criticality criteria and oversight fees for critical ICT third-party providers under DORA in response to the European Commission's call for advice

The European Supervisory Authorities (EBA, EIOPA and ESMA – the ESAs) published their joint response to the European Commission's Call for Advice on two EC delegated acts under the Digital Operational Resilience Act (DORA) specifying further criteria for critical ICT third-party service providers (CTPPs) and determining oversight fees levied on such providers.

In relation to the criticality criteria, the ESAs propose 11 quantitative and qualitative indicators along with the necessary information to build up and interpret such indicators following a two-step approach.

The ESAs also put forward minimum relevance thresholds for quantitative indicators, where possible and applicable, to be used as starting points in the assessment process to designate critical third-party providers.

This joint response does not include any details of the designation procedure nor of the related methodology as these are out of the scope of this Call for Advice.

However, the ESAs plan to define these details no later than six months after the adoption of the delegated act by the Commission.

Regarding the oversight fees, the ESAs make proposals for determining the amount of the fees to be levied on CTPPs and the way in which they are to be paid.

The ESAs' proposals cover the types of estimated expenditures (for both the ESAs and the competent authorities) that shall be covered by oversight fees as well as the basis for the expenditures' calculation and the available information for determining the applicable turnover of the CTPPs (the basis of fee calculation) and the method of fee calculation together with other practical issues regarding the collection of fees.

In addition, the advice proposes a financial contribution for voluntary opt-in requests.

The ESAs will specify other practical aspects on the estimation of oversight expenditures and operational aspects in the context of the implementation of the oversight framework.

Background

In December 2022, the Commission issued to the ESAs a Call for Advice (CfA) in relation to two delegated acts under DORA to:

1) specify further criteria for critical ICT third-party service providers, and

2) determine the fees levied on such providers.

To inform the responses, the ESAs held a public consultation (May-June 2023). In light of the 41 responses received from various stakeholders, the ESAs have amended the draft advice on the criticality criteria to increase the role of critical or important functions in the assessment and further streamlined the proposed set of indicators.

Regarding the oversight fees, the ESAs have, among others, adapted their advice by proposing to define the scope of the applicable turnover on a narrower basis.

Overall, market participants expressed support to the proposals related to the other aspects of the advice, while requesting clarifications on some other points.

To read more: https://www.eiopa.europa.eu/esas-specify-criticality-criteria-and-oversight-fees-critical-ict-third-party-providers-under-dora-2023-09-29_en

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.