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, February 2023

Dear members and friends,

We will start with the interesting Supervisory Convergence Plan for 2023, from EIOPA.

Convergence of supervisory practices should be built on a common interpretation of laws and regulations, and without prejudice to the application of supervisory judgment or of the proportionality principle.

Convergence of supervisory practices is not only achieved or assessed by outputs, i.e. by the number, quality and impact of supervisory tools published or assessments performed.

Convergence is also about working together as a supervisory community. The process of developing common benchmarks for supervisory practices, performing reviews, engaging in challenging interactions and providing training to NCAs in itself leads to supervisory convergence and EIOPA has observed an important development in these area.

Therefore, to achieve a high, effective and consistent level of supervision across Europe, EIOPA continues to confirm supervisory convergence as one of its main strategic goal for the years to come.

The Covid-19 pandemic, increasing losses arising from natural catastrophes and other more recent macro-economic trends (e.g. the invasion of Ukraine by Russian Forces, the energy and cost of living crisis) have demonstrated that ensuring supervisory convergence in extreme situations is even of greater relevance.

For 2023, EIOPA will continue its work on supervisory convergence as a collective effort by all NCAs and EIOPA staff.

1.1. COMMON SUPERVISORY CULTURE

As expected by any solid structure, the framework of supervisory convergence needs to be built upon clear, well-known and commonly understood foundations.

EIOPA's booklet, "A common supervisory culture — Key characteristics of high quality and effective supervision", was the first step in building such framework and continues to be a foundation for supervisors work.

The booklet defines the following five key characteristics of high-quality and effective supervision: risk-based and proportionate, forward-looking, preventive and proactive, challenging, sceptical and engaged, comprehensive and conclusive.

The work developed by EIOPA on supervisory convergence always have this characteristics into account.

A common supervisory culture cannot however be built overnight. It is a long journey where supervisors progressively work together, adopt a focused approach and challenge each other along the way.

In this way, supervisors build a strong and fair supervisory culture that promotes consumer protection and enhances the stability of the financial system for the benefit of Europe's business, economy and citizens.

As processes and procedures are easier to align than behaviours, convergence will occur at different paces but evolution should be visible.

The implementation of a common supervisory culture requires constant change and evolution.

This was recognised in the last amendments to the ESAs Regulations, in particular the amendments to article 29 of EIOPA Regulation, where tools such as establishing Union strategic supervisory priorities, establishing coordination groups to promote supervisory convergence and identify best practices or develop and maintain an up-to-date Union supervisory handbook have been identified.

It is of utmost importance that the supervisory community has, at all levels, easy access to EIOPA tools as well as the ability and willingness to use them. It is also important that whenever possible supervisory convergence tools are made public.

For this reason EIOPA promotes supervisory convergence through the release (after the public consultation) of public supervisory convergence tools, such as Opinions or Supervisory Statements when possible.

There are, however, certain contents that should be kept confidential among supervisors.

Although good use of the different tools was made, EIOPA has also considered that it is important to be more transparent on its Supervisory Handbook.

Following-up the publication of the Introduction and the table of contents of its Supervisory Handbook in October 2021, EIOPA is working on a strategy towards the public disclosure of some content of the handbook.

To read more:
https://www.eiopa.europa.eu/sites/default/files/publications/supervisory_convergence_plan_for_2023.pdf

EIOPA moves to close data gaps by revising reporting of occupational pensions

The European Insurance and Occupational Pensions Authority (EIOPA) has decided to revise the information it receives from national supervisors on occupational pensions, amending the system in place since 2018.

The new decision, which will be applicable as of 1 January 2025, closes important data gaps on emerging risks and fixes inconsistencies that have been reported to EIOPA over the past years.

The main changes compared to the previous regime concern better proportionality measures for small occupational pension funds and the inclusion of information on:

- high-level, look-through data on all investments in investment funds (including UCITs) as well as information on derivative positions – to fully understand the risk exposures of institutions for occupational retirement provision (IORPs) and the products they invest in,

- cross-border data – to accurately monitor cross-border relationships.

EIOPA has incorporated the feedback it received from stakeholders during the public consultation, in particular regarding proportionality.

The new decision eases reporting requirements for small occupational pension funds, exempting IORPs with less than EU 50 million in total assets from the full set of reporting as opposed to the previous threshold of EUR 25 million.

Moreover, new data requirements on the quarterly reporting of derivatives and cash flows will only be mandatory for IORPs with more than EUR 1 billion of assets under management.

The amendments make the reporting of occupational pensions information more proportionate and better fit-for-purpose.

It will allow EIOPA to better identify and assess the risks, resulting in the improved protection of pension scheme members and beneficiaries.
To read more: https://www.eiopa.europa.eu/document-library/decision/decision-of-board-of-supervisors-eiopas-regular-information-request_en

EIOPA aims to strengthen oversight of third country governance arrangements with supervisory statement

The European Insurance and Occupational Pensions Authority (EIOPA) has published a Supervisory Statement to strengthen the supervision and monitoring of insurance undertakings' and intermediaries' activities when using governance arrangements in third countries.

EIOPA-22/362
3 February 2023

Supervisory Statement on the use of governance arrangements in third countries to perform functions or activities

1. OBJECTIVE

1.1. The European Insurance and Occupational Pensions Authority (EIOPA) provides this Supervisory Statement on the basis of Article 29(2) of Regulation (EU) No 1094/2010[1]. This Article mandates EIOPA to play an active role in building a common Union supervisory culture and consistent supervisory practices, as well as in ensuring uniform procedures and consistent approaches throughout the Union.

EIOPA has previously emphasised that EU-based undertakings or intermediaries should not resemble empty-shell companies that do not have an appropriate level of corporate substance within the EU.

This can arise from situations where undertakings or intermediaries use third country branches to disproportionately perform essential functions or activities.

Given that such governance arrangements may lead to poor risk management, ineffective decision-making and pose operational, reputational, and financial risks – also to policyholders – EIOPA has decided to clarify its supervisory expectations.

To improve supervisory oversight and to ensure that similar risks are treated in a similar way regardless of the legal form of the governance arrangements, the supervisory expectations laid out in the statement follow the principle of substance over form.

In particular, EIOPA and National Competent Authorities expect that:

- undertakings and intermediaries using third country branches retain an appropriate level of corporate substance within the European Economic Area (EEA), proportionate to the nature, scale and complexity of their business in the bloc;

- third country branches serve primarily the markets in which they are established and that third country branches with the sole objective of supporting EU-based undertakings and intermediaries should be avoided; undertakings and intermediaries should not be disproportionately dependent on their third-country arrangements for activities in the EEA;

- undertakings appropriately oversee regulated functions and are in a position to take full responsibility for effective decision making and risk management;

- regulated functions and activities are not structured or conducted in a way that impairs the ability of supervisors to monitor compliance; and that

- undertakings and intermediaries considering or operating such third-country arrangements demonstrate to supervisors that the structuring of their activities can safeguard the ability of the supervisory authority to undertake proper supervision.

EIOPA and National Competent Authorities will closely monitor market developments regarding the use of third country governance arrangements following the publication of the Supervisory Statement.

Petra Hielkema, Chair of EIOPA said:

“For us supervisors, it is important that third country branches of EU insurers do what they are meant to do: primarily serve the people and businesses of the country in which they are established.

What we want to avoid is situations where overseas branches are more than outposts while the EU entities to which they are linked - together with their decision-making and risk management capacities - become empty shells."

To read more: https://www.eiopa.europa.eu/media/news/eiopa-aims-strengthen-oversight-of-third-country-governance-arrangements-supervisory

Governance arrangements that deserve particular attention with respect to the adequacy of the corporate structure

2.9 A particular governance arrangement where the required corporate substance may not be sufficiently present, and raises concerns, is where the undertakings or intermediaries use a branch in a third country to conduct regulated functions or activities (such as providing support with underwriting services). The branch performs that role for the undertaking or the intermediary, which ultimately serves policyholders in the EEA.

2.10 These governance arrangements may impair risk management and effective decision making, and have the potential to pose financial, operational and reputational risk and ultimately impair policyholder protection.

2.11 Furthermore, the use of these governance arrangements can affect materially the ability of the supervisory authorities to conduct proper supervision. Supervisory authorities may not have sufficient visibility of the functions performed in a third country if, for example, rights to carry out on-site inspections are impaired.

EIOPA issues its opinion on draft standards governing corporate sustainability disclosures

The European Insurance and Occupational Pensions Authority (EIOPA) has published its Opinion on the European Financial Reporting Advisory Group's technical advice concerning European Sustainability Reporting Standards (ESRS) following the request of the European Commission.

In this first Opinion, EIOPA assesses whether the draft ESRS promote the disclosure of high-quality material sustainability information, whether the standards facilitate interoperability with other EU legislation and global standards, and, finally, whether they are conducive to a consistent and proportionate application by undertakings.

Overall, EIOPA considers that the draft ESRS meet the above objectives even though some aspects can be enhanced upon.

In particular, EIOPA welcomes the general approach on the materiality assessment and the mandatory disclosure requirements that are crucial for financial market participants to calculate and report their principle adverse impact indicators under the Sustainable Finance Disclosure Regulation (SFDR).

Nonetheless, EIOPA is of the opinion that more clarity is needed on the boundaries of the value chain for insurers and pension funds so that relevant material sustainability impacts may be reported in a proportionate and risk-based manner.

Regarding consistency with EU sectoral standards, EIOPA notes that further guidance may be necessary to foster comparability with certain SFDR-related indicators and that a continued dialogue among all relevant stakeholders would be beneficial to ensure consistent and coherent implementation. It is also crucial that any upcoming amendments to the SFDR Delegated Regulation be reflected in ESRS.

Concerning international standards, EIOPA underlines the importance of avoiding the fragmentation of sustainability reporting requirements across jurisdictions.

To this end, compatibility between ESRS standards and IFRS standards should be ensured so that European companies reporting according to ESRS are automatically considered to be compliant with the IFRS sustainability reporting framework.

Whether the standards are interoperable with international standards

3.14. It is of importance that standards limit the risk of inconsistent reporting or administrative burden due to double reporting requirements for undertakings that operate globally. In the future, European undertakings listed in foreign jurisdictions may be subject to the reporting requirements set out by the International Sustainability Standards Board (ISSB), building on disclosure standards from the Task Force on Climate-Related Financial Disclosures (TFCD). In order to avoid the international fragmentation of sustainability reporting requirements across jurisdictions, EIOPA considers that ESRS standards should ensure that European companies that report under ESRS are automatically considered as complying with the IFRS sustainability reporting framework.

3.23. As referred to above, considering the potential broad implications of the implementation of the ESRS throughout the value chain of insurance companies and pension funds, a timely adoption of sector-specific European sustainability standards for the insurance industry should clarify the boundaries of the value chain and affected stakeholders for financial institutions. EIOPA is of the opinion that further clarity on the boundaries of the value chain is needed to enable financial market participants to report on relevant material sustainability impacts across the value chain in a proportionate and risk-based manner manner. Such guidance should ideally be available the latest as part of the second set of ESRS.

The CSRD requires all large companies and all companies with securities listed on EU regulated markets (except micro-companies), including insurers and pension funds, to regularly disclose information on societal, governance and environmental risks, opportunities and impacts.

This includes, for example, the disclosure of transition plans for climate change mitigation, policies on climate change mitigation and adaptation, or potential financial effects from material physical and transition risk.

Large companies are defined in the CSRD as EU companies exceeding at least two of the following three criteria: more than 250 employees on average during the financial year; a balance sheet total in excess of 20 million euros; a net turnover of more than 40 million euros.

Subject to the derogations for captive undertakings, it is expected that almost all insurance companies under Solvency II and an important number of pension funds will qualify for reporting, including pension funds with a limited number of employees.

The CSRD requires that the Commission takes into consideration technical advice from EFRAG when adopting delegated acts.

EFRAG issued exposure drafts of 13 standards for public consultation on 29 April 2022. EIOPA commented on exposure drafts ESRS 1 and ESRS 2.

In its comment letter to the exposure drafts, EIOPA encouraged EFRAG to seek a closer cooperation with the ISSB during the finalization of their standards, to review the rebuttable presumption accompanying the financial materiality definition, and review the definition of the value chain and use of approximations.

To read more: https://www.eiopa.europa.eu/document-library/opinion/eiopas-opinion-european-commission-efrags-technical-advice-esrs_en

Insurance Stress Test 2022 feedback

Bank of England

This letter contains the results of the PRA Insurance Stress Test 2022 (IST 2022) launched in May 2022. In total, 54 insurers took part (16 life insurers, 17 general insurers, and 21 Lloyd's syndicates).

Life insurers were asked to assess their solvency position following an adverse economic scenario and an increase in longevity; and general insurers and Lloyd's syndicates were asked to assess their solvency position against a set of insured natural catastrophe (NatCat) and cyber losses.

We would like to thank all participants for their cooperation in enabling us to meet the three objectives of this exercise; namely:

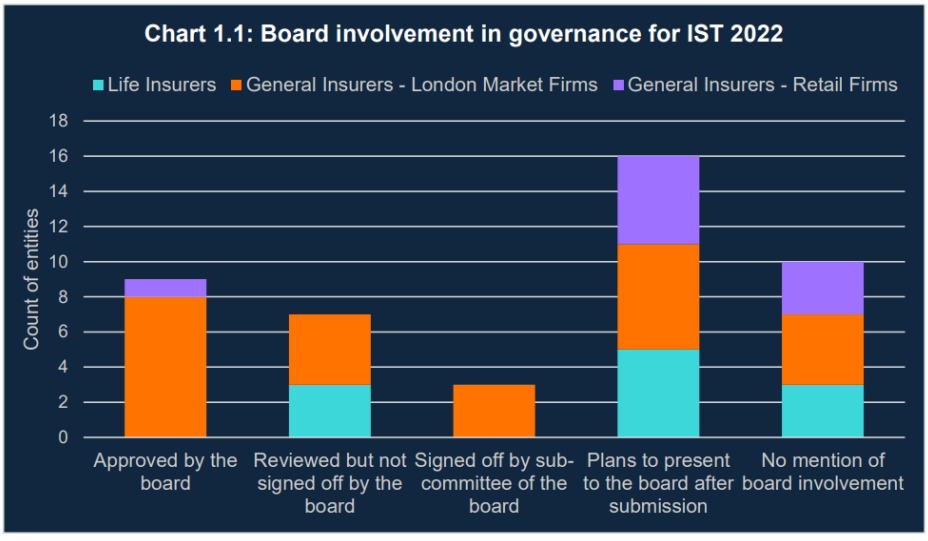
1) assessing sector resilience;

2) supporting capacity building in risk management; and

3) guiding supervisory activity.

This letter sets out our findings on sector resilience and provides thematic observations that support improvements in risk management.

PRA Supervision teams will use individual firm responses to inform their supervisory strategy, which may result in follow-up discussions and actions.



Sources: Firm submissions and PRA calculations. Results were aggregated across Group entities.

Please note: This letter has been prepared for the website. Square brackets show where this letter may differ slightly, along with formatting from those versions sent directly to firms.

Bank of England

Prudential Regulation Authority

Charlotte Gerken
Executive Director,
Insurance Supervision
Prudential Regulation Authority

23 January 2023

Dear [Chief Executive Officer]

Insurance Stress Test 2022 feedback

To read more: https://www.bankofengland.co.uk/prudential-regulation/letter/2023/ist-2022-report

Getting the full picture - the road ahead for climate stress testing

Dr Sabine Mauderer, Member of the Executive Board of the Deutsche Bundesbank, at the 2023 European Banking Authority workshop on climate risk stress testing.

1. Introduction

Ladies and gentlemen,

- How does climate change affect the economy?
- What impact does climate change have on growth and inflation?
- How does climate change affect the financial system?

Policymakers need answers to these questions.

Understanding climate-related risks and their transmission channels is essential for designing targeted policies. Central banks and supervisors have outstanding analytical capabilities.

Dealing with financial risks is our bread and butter business. This ample expertise can help to strengthen the understanding of climate-related financial risks. These risks are not a new risk category per se. Climate risk drivers can exacerbate "traditional" financial risks and existing vulnerabilities, such as credit risks and market risks.

Stress tests have been an integral part of the toolbox of central banks and supervisors for a long time. Stress tests provide valuable insights into the risk exposure and resilience of individual banks and the financial system. Climate stress tests can complement common stress tests to give a fuller picture.

2. Climate scenarios – A glimpse of possible futures

Stress tests are forward-looking analytical exercises that build on baseline and adverse scenarios.

The same goes for climate stress tests. This is where climate scenarios come into play. Climate scenarios give us a glimpse of different possible future outcomes. They can help us to understand how climate-related risks could evolve and what the implications might be for the economy and the financial system.

The Network for Greening the Financial System (NGFS) has developed and repeatedly refined a set of six climate scenarios. The scenarios fall into three categories and explore the impact of climate change (physical risk) and climate policy (transition risk). In the orderly scenarios, the early and gradual introduction of climate policies leads to subdued physical and transition risks.

The disorderly scenarios assume that climate policies are delayed or divergent across countries and sectors. These scenarios are associated with higher transition risk as, for instance, carbon prices might need to rise sharply and abruptly.

In the hot house world scenarios, global warming cannot be limited due to insufficient global efforts. As a result, extreme weather events become more severe and more frequent. Physical risks increase drastically.

All these NGFS scenarios help quantify the economic impacts of different emission and policy pathways. They show that both climate change and policies to contain it come at a price. But taking ambitious climate action too late or failing to act altogether would be much more costly in the end.

For instance, what happens if we keep delaying action today but still want to reach net zero by mid-century? This scenario shows that a delayed transition would lead to a drastic surge in carbon prices from 2030 onwards.

By 2050, carbon prices would have to rise to nearly 400 dollars per ton in this scenario. The scenarios already put a price tag on policy action – or lack thereof. In order to further improve the usability of the scenarios, the NGFS is continuously bringing them up to date.

In September 2022, the NGFS published the Phase III update, which introduced several enhancements. For instance, the modelling of physical risks was improved.

This iteration considered, for the first time, the impacts of acute physical risks under different scenarios. In addition, the granularity in the transport and industry sectors was improved, giving a clearer picture of transition risks.

The NGFS scenarios help central banks and supervisors to beef up macro models and climate stress tests.
For example, ECB Banking Supervision used macro-financial scenarios that are based on the NGFS scenarios for its 2022 climate stress test. The Bundesbank is working on a top-down climate stress test that will also build on the NGFS scenarios.

In its 2021 Financial Stability Review, the Bundesbank explored the impact of transition risks on the German financial system. This assessment was also based on the NGFS scenarios.

3. Challenges & way forward

These examples all show that climate scenarios are a useful tool for assessing climate-related risks. Having said that, some obstacles and challenges remain.

Allow me to touch upon three of them.

The first challenge concerns time horizons. Standard stress tests usually look at time horizons of one to three years.

By contrast, climate scenarios have considered much longer time horizons of 10-30 years, as it may take longer for climate-related risks to materialise and for climate policies to have an effect. These long time horizons carry the risk of climate scenarios underestimating the near-term impact of climate-related risk. A number of factors compound the problem.

Which brings me to the second challenge. The non-linearity of climate change means that various tipping points may cause rapid shifts with far-reaching consequences. As a result, climate-related risks are surrounded by deep uncertainty and tail risks cannot be ruled out. For these reasons, the NGFS has described the first climate scenario analyses as learning opportunities that need further fine-tuning.

The NGFS is exploring additional scenarios and looking at options for introducing short-term scenarios. Moreover, the NGFS aims to further expand and improve the sectoral granularity and the geographic coverage as well.

Other factors to consider going forward are geopolitical shifts and changes in global energy markets. Russia's invasion of Ukraine has upended energy markets, with likely long-term impacts for energy prices and energy security.

These developments also carry implications for the transition to net zero and the associated risks. On the one hand, high and volatile prices reinforce incentives to speed up the energy transition and boost renewable energy. On the other hand, as governments are moving to secure energy supplies and keep energy prices in check, there is a non-negligible risk of carbon lock-in.

For instance, according to the International Energy Agency (IEA), global coal consumption hit an all-time high in 2022.

Likewise, new, longer-term contracts for liquefied natural gas deliveries may complicate the transition away from fossil fuels. In this environment, the NGFS sees a higher risk of a delayed or disorderly transition.

The network is working on including these developments in the upcoming iteration of the climate scenarios. These planned updates will further enhance the usability of the NGFS scenarios.

Last but not least, the issue of data availability and data quality has been a longstanding problem. We all know that the lack of consistent and granular data continues to be an obstacle that complicates the adequate calibration of shocks in stress testing models. Central banks and supervisors can play a part in overcoming this obstacle.

Last summer, the NGFS launched a directory for climate data with over 700 links to relevant data sources. The directory supports financial sector stakeholders in finding relevant climate-related data sources and facilitates access to these data.

In addition, in December 2021, the NGFS published a guide on climate-related disclosures for central banks. The Eurosystem took up this "invitation". Starting in March 2023, it will publish climate-related information on its corporate bond holdings and its non-monetary policy portfolios on a yearly basis.

The Bundesbank already took a first step in July 2022. We published our first climate report and disclosed the climate impact of our non-monetary policy portfolio.

In this way, central banks and supervisors can help to improve the data situation.

Brussels is also taking action to tackle this issue. The EU's Corporate Sustainability Reporting Directive (CSRD) will gradually come into effect from 2024 onwards. The CSRD will require around 50,000 companies to disclose detailed information on sustainability matters.

The initiative will address data gaps, which will also help to increase the reliability of climate stress tests. At the same time, the absence of granular data is no excuse for inaction.

4. Conclusion

Let me conclude.

Climate scenarios and climate stress tests are not perfect yet and the results they provide have to be taken with a grain of salt. Nonetheless, they are already viable instruments for shedding light on the exposure and resilience of banks to climate-related risks.

Central banks and supervisors have to continue along this path and further refine climate scenarios and climate stress tests. This includes striking a balance between short-term and long-term scenarios as well as bridging data gaps.

As the work continues, climate scenarios will become more usable and climate stress tests will paint a clearer picture. In order to facilitate progress with climate scenarios and climate stress tests, international coordination and exchange is vital. This workshop is an excellent opportunity to find common ground on the challenges that lie ahead.

To read more: https://www.bundesbank.de/en/press/speeches/getting-the-full-picture-the-road-ahead-for-climate-stress-testing-738186

Big techs in finance: forging a new regulatory path

Agustín Carstens, General Manager, Bank for International Settlements, at the BIS conference "Big techs in finance – implications for public policy", Basel, Switzerland.

It is my great privilege to welcome you today to the BIS conference on big techs in finance – implications for public policy.

This high-level conference brings together prominent officials from international bodies, central banks and supervisory authorities, as well as renowned academics and private sector representatives.

It will provide a unique forum to exchange views on the most pressing policy challenges associated with big techs' involvement in the financial sector.

Current circumstances have allowed us to invite you to join us in person here in Basel, and it gives me great pleasure to see many of you could accept our invitation. Of course, let me also welcome those of you who are joining us remotely today.

Big techs and data

We at the BIS have been closely following large technology firms (big techs) and their advances into finance. Big techs' reach extends across a wide range of industries, with existing core businesses grounded in e-commerce and social media, among others. From this base, they have expanded into finance.

To understand how big techs can easily make forays into finance, one must grasp the key role of data. Indeed, big techs have fully embraced the centrality of data in the digital economy. This is what distinguishes them from other firms. It also shapes their unique characteristics. Let me mention those that are particularly relevant for policymakers.

First, big techs can overcome limits to scale in financial services provision by using user data from their existing businesses. Their business model revolves around users' direct interactions and the data generated as a by-product of these interactions. They use that data to offer a range of

services that exploit the inherent network effects in digital services, a phenomenon where more users attract ever more users.

In this way, big techs can establish a substantial presence in financial services very quickly through what we call the "data-network-activities" (DNA) loop.

Second, big techs collect different types of data from the various business lines they straddle. They are uniquely positioned to combine that data to uncover patterns and insights that can help them improve their services or offer new ones.

This combination of different types of data across sectors carries efficiency gains and is key to big techs' provision of digital services.

Third, big techs are unrivalled experts in data management and analysis. They devote significant resources to developing or acquiring state-of-the-art technologies. After all, access to large troves of data generates value only if you also have the technological capabilities to analyse it and monetise it.

Big techs have been pioneers in leveraging artificial intelligence techniques for this purpose.

To be sure, these capabilities have high fixed costs, but once that is overcome the marginal cost of handling more data is negligible. Therefore, big techs benefit from significant economies of scale in their use of data.

For other firms, reaping the benefits of such economies of scale is a tall order. Data management is thus at the core of big tech activities, and the financial sector is all about managing information. Coupled with big techs' relentless drive to expand, their growing and already substantial footprint in financial services should come as no surprise.

Moreover, the trend towards greater digitalisation, which the Covid-19 pandemic has accelerated, has allowed big techs to fortify their market positions even further.

Public policy challenges

Given their size and customer reach, big techs' entry into finance could trigger rapid change in the industry, generating both opportunities and challenges.
The potential benefits of big techs' entry into finance include improved customer outcomes, increased financial market efficiency and enhanced financial inclusion.

For example, BIS research has shown that access to innovative (QR code-based) payment methods provided by big techs helps micro firms build up credit history, and the use of big tech credit can ease access to bank credit. And there are many more examples.

To read more: https://www.bis.org/speeches/sp230208.pdf

Countercyclical capital buffer

ESRB
European Systemic Risk Board
European System of Financial Supervision

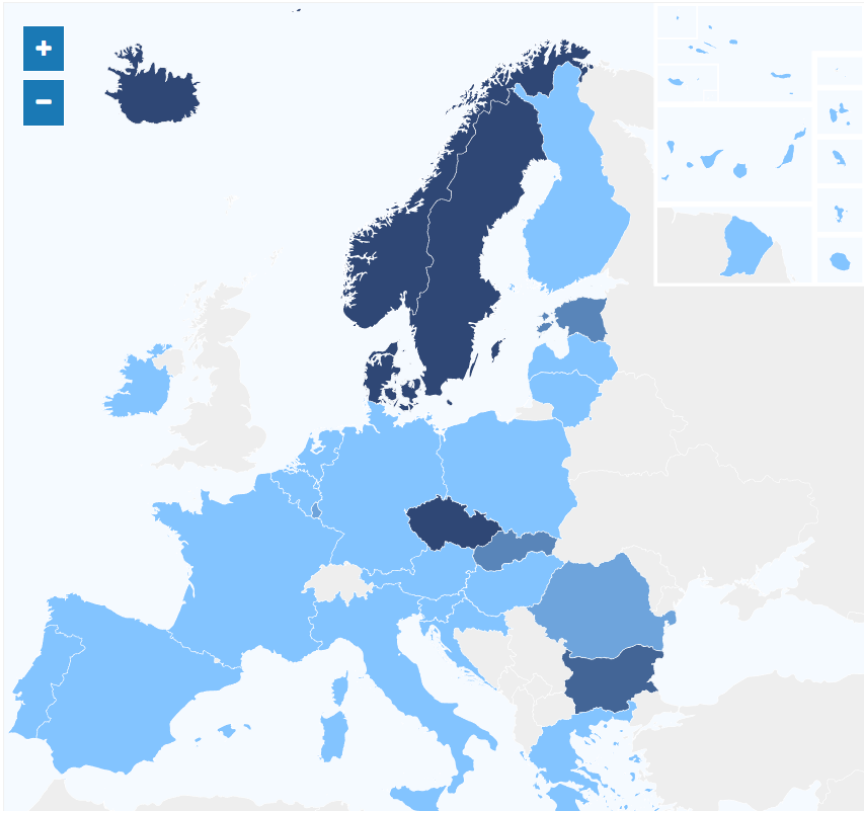
The countercyclical capital buffer (CCyB) is designed to counter procyclicality in the financial system.

When cyclical systemic risk is judged to be increasing, institutions should accumulate capital to create buffers that strengthen the resilience of the banking sector during periods of stress when losses materialise.

This will help maintain the supply of credit to the economy and dampen the downswing of the financial cycle. The CCyB can also help dampen excessive credit growth during the upswing of the financial cycle.

Please consult the respective national authorities' websites for the most up-to-date information. The tables below will be updated after the ESRB has received official notifications of the measures (last updated: 10 January 2023).

The following map shows current CCyB rates set (i.e. after the 12-month phase-in period) in Europe:



Country	Implementation date	Current CCyB
Austria	1 Jan 2016	0%
Belgium	1 Apr 2020	0%
Bulgaria	1 Jan 2023	1.5%
	1 Oct 2023	2%
Croatia	1 Jan 2016	0%
	31 Mar 2023	0.5%
	31 Dec 2023	1%
Cyprus	1 Jan 2016	0%
	30 Nov 2023	0.5%
Czech Republic	1 Jan 2023	2%
	1 Apr 2023	2.5%
Denmark	31 Dec 2022	2%
	31 Mar 2023	2.5%
Estonia	7 Dec 2022	1%
	1 Dec 2023	1.5%
Finland	16 Mar 2015	0%
France	1 Apr 2020	0%
	7 Apr 2023	0.5%
	2 Jan 2024	1%
Germany	1 Apr 2020	0%
	1 Feb 2023	0.75%
Greece	1 Jan 2016	0%
Hungary	1 Jan 2016	0%
	1 Jul 2023	0.5%
Iceland	29 Sep 2022	2%
Ireland	1 Apr 2020	0%
	15 Jun 2023	0.5%
Italy	1 Jan 2016	0%
Latvia	1 Feb 2016	0%
Liechtenstein	1 Jul 2019	0%
Lithuania	1 Apr 2020	0%
	1 Oct 2023	1%
Luxembourg	1 Jan 2021	0.5%
Malta	1 Jan 2016	0%
Netherlands	1 Jan 2016	0%
	25 May 2023	1%
Norway	31 Dec 2022	2%
	31 Mar 2023	2.5%
Poland	1 Jan 2016	0%
Portugal	1 Jan 2016	0%
Romania	17 Oct 2022	0.5%

To read more:
https://www.esrb.europa.eu/national_policy/ccb/html/index.en.html

Statement by National Security Advisor Jake Sullivan on the New U.S.-EU Artificial Intelligence Collaboration

THE WHITE HOUSE

The United States and the European Union signed an administrative arrangement to bring together experts from across the U.S. and Europe to further research on artificial intelligence (AI), computing, and related privacy protecting technologies, as underscored in the U.S.-EU Trade and Technology Council (TTC) commitment.

This collaborative effort will drive responsible advancements in AI to address major global challenges with a joint development model and integrated research to deliver benefits to our societies through five key areas of focus: Extreme Weather and Climate Forecasting, Emergency Response Management, Health and Medicine Improvements, Electric Grid Optimization, and Agriculture Optimization.

Together, we are confident the results of our research will extend beyond our partnership to benefit additional international partners and the global science community.

Today's announcement also builds on the vision set forth in the Declaration for the Future of the Internet (DFI) for an open, free, reliable, and secure Internet and digital technologies around the world.

THE WHITE HOUSE

FACT SHEET: United States and 60 Global Partners Launch Declaration for the Future of the Internet

We look forward to deepening our cooperation with the EU through this initiative.

To read more:
https://www.whitehouse.gov/briefing-room/statements-releases/2022/12/05/u-s-eu-joint-statement-of-the-trade-and-technology-council/

https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet_Launch-Event-Signing-Version_FINAL.pdf

https://www.whitehouse.gov/briefing-room/statements-releases/2023/01/27/statement-by-national-security-advisor-jake-sullivan-on-the-new-u-s-eu-artificial-intelligence-

collaboration/#:~:text=Today%2C%20the%20United%20States%20and,Trade%20and%20Technology%20Council%20(TTC)

A DECLARATION *for the* FUTURE *of the* INTERNET

We are united by a belief in the potential of digital technologies to promote connectivity, democracy, peace, the rule of law, sustainable development, and the enjoyment of human rights and fundamental freedoms. As we increasingly work, communicate, connect, engage, learn, and enjoy leisure time using digital technologies, our reliance on an open, free, global, interoperable, reliable, and secure Internet will continue to grow. Yet we are also aware of the risks inherent in that reliance and the challenges we face.

We call for a new Declaration for the Future of the Internet that includes all partners who actively support a future for the Internet that is an open, free, global, interoperable, reliable, and secure. We further affirm our commitment to protecting and respecting human rights online and across the digital ecosystem. Partners in this Declaration intend to work toward an environment that reinforces our democratic systems and promotes active participation of every citizen in democratic processes, secures and protects individuals' privacy, maintains secure and reliable connectivity, resists efforts to splinter the global Internet, and promotes a free and competitive global economy. Partners in this Declaration invite other partners who share this vision to join us in working together, with civil society and other stakeholders, to affirm guiding principles for our role in the future of the global Internet.

Federal Reserve Board announces denial of application by Custodia Bank, Inc. to become a member of the Federal Reserve System

The Federal Reserve Board announced its denial of the application by Custodia Bank, Inc., Cheyenne, Wyoming, to become a member of the Federal Reserve System.

The Board has concluded that the firm's application as submitted is inconsistent with the required factors under the law.

Custodia is a special purpose depository institution, chartered by the state of Wyoming, which does not have federal deposit insurance.

The firm proposed to engage in novel and untested crypto activities that include issuing a crypto asset on open, public and/or decentralized networks.

The firm's novel business model and proposed focus on crypto-assets presented significant safety and soundness risks.

The Board has previously made clear that such crypto activities are highly likely to be inconsistent with safe and sound banking practices.

The Board also found that Custodia's risk management framework was insufficient to address concerns regarding the heightened risks associated with its proposed crypto activities, including its ability to mitigate money laundering and terrorism financing risks.

In light of these and other concerns, the firm's application as submitted was inconsistent with the factors the Board is required to evaluate by law.

The Board's order will be released following a review for confidential information.

To read more:
https://www.federalreserve.gov/newsevents/pressreleases/orders20230127a.htm

Engineering Personal Data Sharing

This report attempts to look closer at specific use cases relating to personal data sharing, primarily in the health sector, and discusses how specific technologies and considerations of implementation can support the meeting of specific data protection.

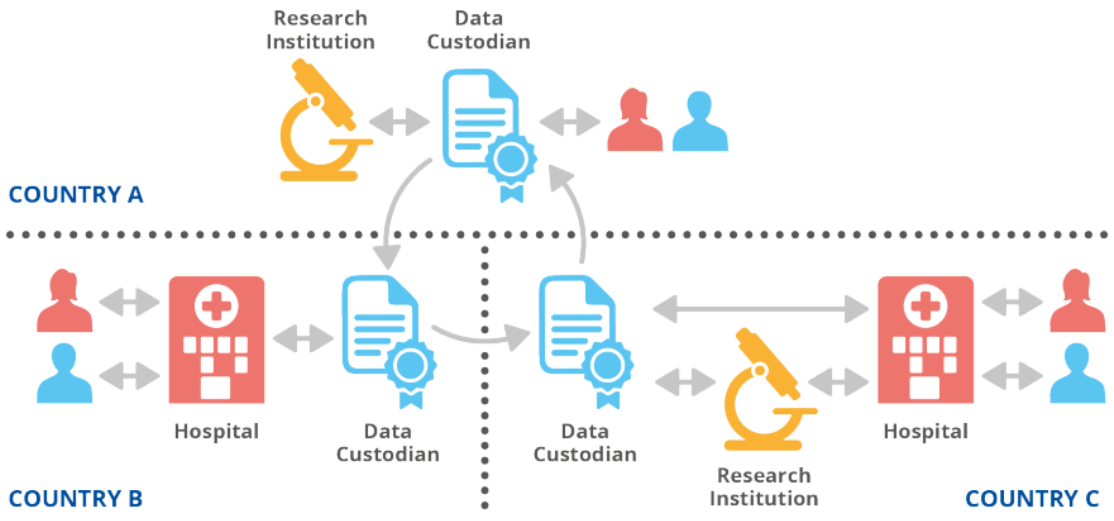
After discussing some challenges in (personal) data sharing, this report demonstrates how to engineer specific technologies and techniques in order to enable privacy preserving data sharing.

More specifically it discusses specific use cases for sharing data in the health sector, with the aim of demonstrating how data protection principles can be met through the proper use of technological solutions relying on advanced cryptographic techniques.

Next it discusses data sharing that takes place as part of another process or service, where the data is processed through some secondary channel or entity before reaching its primary recipient.

Lastly, it identifies challenges, considerations and possible architectural solutions on intervenability aspects (such as the right to erasure and the right to rectification when sharing data).

Figure 17: Cross border data exchange with data custodians



When two or more parties decide to share their data, they become part of a larger data ecosystem where they can take advantage of the combined data set that enables the discovery, by way of computation, of new information

or trends relating to individuals, groups of individuals, or to society as a whole.

The easiest and most straightforward way to achieve this goal would be to exchange the raw data that each actor holds across technical interfaces putting them on a common table (i.e. a single database) but this hypothetical option is not really feasible.

In reality we are pursuing trusted sharing environments that will make full use of the potential offered by a safe and secure exchange and use of personal data while respecting data protection principles.

This report attempted to look closer at specific use cases relating to personal data sharing, primarily in the health sector, and to discuss how specific technologies and considerations of implementation can support the engineering of personal data sharing in practice.

The analysis ranged from user-controlled data sharing to large scale personal data gathering and data sharing using third party service.

Despite the potential of the data sharing concept and the relevant Union policy and law in the area, there are still considerations on which are the appropriate technical and organizational measures and how to engineer them into practice.

The European legislative initiatives on data sharing described in Section 1.1 entail the processing of large quantities of data which will also include personal data.

Therefore, in addition to the consistency of their provisions with the GDPR, it is important to remove any legal uncertainty on the roles and obligations, not only for individuals as highlighted by the EDPB and the EDPS but also for the entities involved in the data sharing.

In order to leverage the potential of data sharing across the EU, practitioners could be provided with directions on which technologies and techniques can be considered, under which circumstances and which data protection principles can be met.

There are several commonly used (cryptographic) techniques (i.e. asymmetric encryption, pseudonyms, access control etc) that are already acknowledged as able to alleviate data protection risks.

Some of them were discussed in Section 2, Section 3 and Section 4. In emerging concepts such as data spaces and data intermediaries, however,

the risks introduced cannot always be adequately addressed only by such techniques.

This is due to the fact that data subjects want to preserve confidentiality of the data they are sharing, they might not know beforehand with whom they might be sharing data with or might want to share accumulated datasets.

Although there are advanced techniques that are still evolving, they should not be considered as of purely academic interest since there exist practical implementations in real use case scenarios.

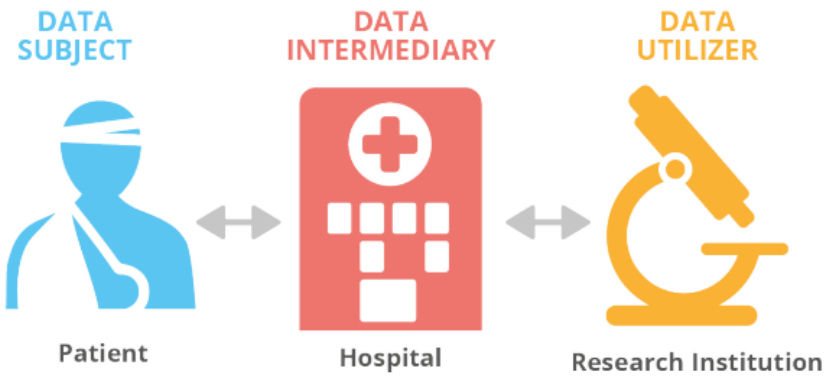
Lastly, since the majority of the technologies described earlier and in previous ENISA reports rely on asymmetric cryptography, the advent of quantum computing and the impact on the security of currently used asymmetric ciphers should be anticipated.

Following the deployment of data sharing infrastructures and services, we cannot expect that they will cease to operate due to possible inadequacy of the asymmetric ciphers.

This is where crypto agility becomes relevant as it allows for a switch between algorithms, cryptographic primitives, and other encryption mechanisms without significant changes in the overall IT system or process.

To read more: https://www.enisa.europa.eu/publications/engineering-personal-data-sharing

Figure 14: Data sharing scenario with data intermediaries



SEC Publishes Annual Staff Report on Nationally Recognized Statistical Rating Organizations

The Securities and Exchange Commission published a staff report that provides a summary of the staff's examinations of nationally recognized statistical rating organizations (NRSROs) and discusses the state of competition, transparency, and conflicts of interest among NRSROs.

"The Office of Credit Ratings is critical to the Commission's work to protect investors and ensure the integrity of the rating process, including through the office's oversight of Nationally Recognized Statistical Rating Organizations," said SEC Chair Gary Gensler.

"Through the 2022 staff report, the OCR continues its work to ensure credit ratings are accurate, reliable, and fair."

"Our risk-based approach to NRSRO examinations protects investors by focusing on specific NRSRO activities and assessing compliance with applicable laws and rules," said Lori Price, Director of the Office of Credit Ratings. "The comprehensive staff report summarizes the findings from our annual examinations and also provides information about NRSROs, their credit ratings businesses, and the industry more broadly."

As described in the report, the staff's NRSRO examinations during 2022 considered a number of factors, including:

- Rating surveillance practices;

- The impact of COVID-19 on commercial real estate credit ratings;

- Whether business communications are conducted through unauthorized means;

- Securities ownership by NRSRO employees;

- The effect on credit ratings from the marketing and development of stand-alone ESG products; and

- Ratings of firms based in China.
- Prior years' reports from the Office of Credit Ratings are available here.

To read more: https://www.sec.gov/files/2023-ocr-staff-report.pdf

Chart 1. Table of NRSROs

NRSRO	Categories of Credit Ratings	Principal Office
A.M. Best Rating Services, Inc. (AMB)	(ii), (iii), and (iv)	U.S.
DBRS, Inc. (DBRS)	(i) through (v)	U.S.
Demotech, Inc. (Demotech)	(ii)	U.S.
Egan-Jones Ratings Company (EJR)	(i) through (iii)	U.S.
Fitch Ratings, Inc. (Fitch)	(i) through (v)	U.S.
HR Ratings de México, S.A. de C.V. (HR)	(i), (iii), and (v)	Mexico
Japan Credit Rating Agency, Ltd. (JCR)	(i), (ii), (iii), and (v)	Japan
Kroll Bond Rating Agency, LLC (KBRA)	(i) through (v)	U.S.
Moody's Investors Service, Inc. (Moody's)	(i) through (v)	U.S.
S&P Global Ratings (S&P)	(i) through (v)	U.S.

As Required by Section 6 of the Credit Rating Agency Reform Act of 2006
and Section 15E(p)(3)(C) of the Securities Exchange Act of 1934

Phishing Resistance – Protecting the Keys to Your Kingdom

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

If you own a computer, watch the news, or spend virtually any time online these days you have probably heard the term “phishing.” Never in a positive context…and possibly because you have been a victim yourself.

Phishing refers to a variety of attacks that are intended to convince you to forfeit sensitive data to an imposter.

These attacks can take a number of different forms; from spear-phishing (which targets a specific individual within an organization), to whaling (which goes one step further and targets senior executives or leaders).

Furthermore, phishing attacks take place over multiple channels or even across channels; from the more traditional email-based attacks to those using voice – vishing – to those coming via text message – smishing.

Regardless of the type or channel, the intent of the attack is the same – to exploit human nature to gain control of sensitive information.

These attacks typically make use of several techniques including impersonated websites, attacker-in-the-middle, and relay or replay to achieve their desired outcome.

Due to their effectiveness and simplicity, phishing attacks have rapidly become the tool of choice for baddies everywhere.

As a tactic, it is used by everyone from low level criminals looking to commit fraud, to the sophisticated nation state attackers seeking a foothold within an enterprise network. And, while almost any kind of information can be targeted, often the most damaging attacks focus on your password, pin, or one-time passcodes – the keys to your digital realm.

The combination can be catastrophic. The Verizon 2022 Data Breach Investigations Report lists phishing and stolen credentials (which may be harvested during phishing attacks) as two of the four “key pathways” that organizations must be prepared to address in order to prevent breaches.

In recognition of the threat posed by phishing – the Office of Management and Budget’s Memo 22-09 “Moving the U.S. Government Toward Zero Trust Cybersecurity Principles” prioritizes implementation of phishing resistant authenticators.

You may visit: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

January 26, 2022

M-22-09

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Acting Director

SUBJECT: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

This memorandum sets forth a Federal zero trust architecture (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024 in order to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns. Those campaigns target Federal technology infrastructure, threatening public safety and privacy, damaging the American economy, and weakening trust in Government.

So – how do you keep your keys from falling into the wrong hands? What constitutes a phishing resistant authenticator?

NIST Special Publication DRAFT 800-63-B4 defines it as "the ability of the authentication protocol to detect and prevent disclosure of authentication secrets and valid authenticator outputs to an impostor relying party without reliance on the vigilance of the subscriber." To achieve this, phishing resistant authenticators must address the following attack vectors associated phishing:

1. Impersonated Websites – Phishing resistant authenticators prevent the use of authenticators at illegitimate websites (known as verifiers) through multiple cryptographic measures.

This is achieved through the establishment of authenticated protected channels for communications and methods to restrict the context of an authenticator's use.
For example, this may be achieved through name binding – where an authenticator is only valid for a specific domain (I can only use this for one website). It may also be achieved through binding to a communication channel – such as in client authenticated TLS (I can only use this over a specific connection).

2. Attacker-in-the Middle - Phishing resistant authenticators prevent an attacker-in-the-middle from capturing authentication data from the user and relaying it to the relying website.

This is achieved through cryptographic measures, such as leveraging an authenticated protected channel for the exchange of information and digitally signing authentication data and messages.

3. User Entry – Phishing resistant authenticators eliminate the need for a user to type or manually input authentication data over the internet.

This is achieved through the use of cryptographic keys for authentication that are unlocked locally through a biometric or pin. No user entered information is exchanged between the relying website and the authenticator itself.

4. Replay – Phishing resistant authenticators prevent attackers from using captured authentication data at a later point in time.

Supporting cryptographic controls for restricting context and to prevent attacker-in-the-middle scenarios are also preventative of replay attacks, particularly digitally signed and time-stamped authentication and message data.

As complicated as this may seem, there are several practical examples of phishing resistant authenticators in place today.

For U.S. federal employees, the most ubiquitous form of phishing resistant authenticator is the Personal Identity Verification (PIV) card; they leverage public-key cryptography to protect authentication events.

Commercially, FIDO authenticators paired with W3C's Web Authentication API are the most common form of phishing resistant authenticators widely available today.

These can take the form of separate hardware keys or be embedded directly into platforms (for example your phone or laptop).
Availability, practicality, and security of these "platform authenticators" increasingly puts strong, phishing resistant authenticators into user's hands without the need for additional form factors or dongles.

Not every transaction requires phishing resistant authenticators. However, for applications that protect sensitive information (such as health information or confidential client data) or for users that have elevated privileges (such as admins or security personnel) organizations should be enforcing, or at least offering, phishing resistant authenticators.

Individuals should explore the security settings for their more sensitive online accounts to see if phishing resistant authenticators are available and make use of them if they are. In reality, these tools are often easier, faster, and more convenient than the MFA – such as SMS text codes – they may currently be using.

In the end, phishing resistant authenticators are a critical tool in personal and enterprise security that should be embraced and adopted. They are not, however, a silver bullet.

Phishing resistant authenticators only address one focus of phishing attacks – the compromise and re-use of authenticators such as passwords and one-time passcodes.

They do not mitigate phishing attempts that may have alternative goals such as installing malware or compromising personal information to be used elsewhere.

Phishing resistant authenticators should be paired with a comprehensive phishing prevention program that includes user awareness and training, email protection controls, data loss prevention tools, and network security capabilities.

To read more: https://www.nist.gov/blogs/cybersecurity-insights/phishing-resistance-protecting-keys-your-kingdom

The NIS 2 Directive of the EU

EUR-Lex
Access to European Union law

Network and information systems have developed into a central feature of everyday life with the speedy digital transformation and interconnectedness of society, including in cross-border exchanges.

That development has led to an expansion of the cyber threat landscape, bringing about new challenges, which require adapted, coordinated and innovative responses in all Member States.

The number, magnitude, sophistication, frequency and impact of incidents are increasing, and present a major threat to the functioning of network and information systems.

As a result, incidents can impede the pursuit of economic activities in the internal market, generate financial loss, undermine user confidence and cause major damage to the Union's economy and society.

Cybersecurity preparedness and effectiveness are therefore now more essential than ever to the proper functioning of the internal market.

Moreover, cybersecurity is a key enabler for many critical sectors to successfully embrace the digital transformation and to fully grasp the economic, social and sustainable benefits of digitalisation.

The cybersecurity requirements imposed on entities providing services or carrying out activities which are economically significant vary considerably among Member States in terms of type of requirement, their level of detail and the method of supervision.

Those disparities entail additional costs and create difficulties for entities that offer goods or services across borders.

Requirements imposed by one Member State that are different from, or even in conflict with, those imposed by another Member State, may substantially affect such cross-border activities.

Furthermore, the possibility of the inadequate design or implementation of cybersecurity requirements in one Member State is likely to have repercussions at the level of cybersecurity of other Member States, in particular given the intensity of cross-border exchanges.
The review of Directive (EU) 2016/1148 has shown a wide divergence in its implementation by Member States, including in relation to its scope, the

delimitation of which was very largely left to the discretion of the Member States.

Directive (EU) 2016/1148 also provided the Member States with very wide discretion as regards the implementation of the security and incident reporting obligations laid down therein.

Those obligations were therefore implemented in significantly different ways at national level.

There are similar divergences in the implementation of the provisions of Directive (EU) 2016/1148 on supervision and enforcement.

All those divergences entail a fragmentation of the internal market and can have a prejudicial effect on its functioning, affecting in particular the cross-border provision of services and the level of cyber resilience due to the application of a variety of measures.

Ultimately, those divergences could lead to the higher vulnerability of some Member States to cyber threats, with potential spill-over effects across the Union.

This Directive aims to remove such wide divergences among Member States, in particular by setting out minimum rules regarding the functioning of a coordinated regulatory framework, by laying down mechanisms for effective cooperation among the responsible authorities in each Member State, by updating the list of sectors and activities subject to cybersecurity obligations and by providing effective remedies and enforcement measures which are key to the effective enforcement of those obligations.

Therefore, Directive (EU) 2016/1148 should be repealed and replaced by this Directive.

With the repeal of Directive (EU) 2016/1148, the scope of application by sectors should be extended to a larger part of the economy to provide a comprehensive coverage of sectors and services of vital importance to key societal and economic activities in the internal market.

In particular, this Directive aims to overcome the shortcomings of the differentiation between operators of essential services and digital service providers, which has been proven to be obsolete, since it does not reflect the importance of the sectors or services for the societal and economic activities in the internal market.

To read more: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

27.12.2022 EN Official Journal of the European Union L 333/80

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

(Text with EEA relevance)

EBA issues Opinion to the European Commission on the draft European Sustainability Reporting Standards

- The EBA believes that the draft standards are a good basis for the implementation of the Corporate Sustainability Reporting Directive (CSRD), although a few aspects should deserve further consideration.

- Interoperability of the draft standards with the EBA Pillar 3 disclosures, together with the data that credit institutions need from a risk management perspective, are central considerations of this Opinion.

The European Banking Authority (EBA) published an Opinion on the draft European Sustainability Reporting Standards (ESRS) developed by the European Financial Reporting Advisory Group (EFRAG).


OPINION ON THE EUROPEAN SUSTAINABILITY REPORTING STANDARDS

EBA/Op/2023/01

26 January 2023

Opinion of the European Banking Authority on the draft European Sustainability Reporting Standards (ESRS)

In this Opinion, addressed to the European Commission, the EBA acknowledges that, overall, the draft ESRS are consistent with international standards and any other relevant EU Regulation.

In addition, the EBA very much welcomes the level of alignment with the Pillar 3 disclosure requirements reached at this stage. The EBA also highlights a few aspects that should deserve further consideration by the European Commission.

In particular, the EBA acknowledges the significant improvement of the draft ESRS prepared by EFRAG compared to the versions put out for consultation.

Overall, the EBA welcomes the consistency of ESRS with international standards and relevant EU Regulation, and a better alignment with the disclosure requirements under the EBA Pillar 3 framework.

As regards proportionality, the EBA believes that the draft standards offer a well-balanced approach with the relevant phasing-in provisions in place.

A few aspects should deserve further consideration by the European Commission, including the timetable for the development of the sector-specific standards for credit institutions.

The European Commission also requested an Opinion from the European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA). The ESMA communication is available here and the EIOPA communication is available here.

Legal basis and background

This Opinion is based on Article 16a(4) of Regulation (EU) No 1093/2010 ('EBA Regulation'), which mandates the EBA to issue opinions in its area of competence as requested by the European Commission.

In addition, Article 49(3b) of Directive 2013/34/EU (Accounting Directive), as amended by the Corporate Sustainability Reporting Directive (CSRD), lays down the conditions for the adoption by the European Commission of the delegated acts on the European Sustainability Reporting Standards (ESRS), including the need to request an opinion to the EBA.

The draft ESRS set out the rules and requirements for companies to report on sustainability-related aspects under the Corporate Sustainable Reporting Directive (CSRD).

On 28 July 2022, the EBA submitted its comment letter to EFRAG on exposure drafts ESRS 1, ESRS 2 and ESRS E1.

Following this public consultation, the first set of standards was submitted by EFRAG to the European Commission last November, in line with the Commission's mandate.

Following this submission, the European Commission requested the opinion of the EBA on the technical advice provided by EFRAG, as required by the CSRD.

To read more:
https://www.eba.europa.eu/sites/default/documents/files/document_libr

ary/Publications/Opinions/2023/1051231/EBA-Op-2023-01%20%28Opinion%20of%20the%20EBA%20on%20the%20draft%20ESRS%29.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.