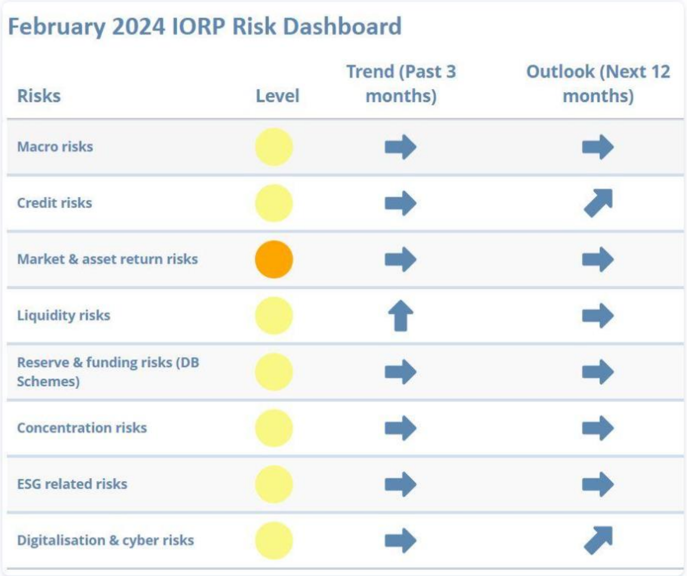
Solvency 2 News, February 2024

The European Insurance and Occupational Pensions Authority (EIOPA) published its first Risk Dashboard on Institutions for occupational retirement provisions (IORPs).

Based on individual occupational pensions regulatory reporting, EIOPA's IORP Risk Dashboard summarises the main risks and vulnerabilities in the IORPs sector of the European Economic Area (EEA) for the different schemes, i.e. defined contributions (DC) and defined benefits (DB).



February 2024 IORP Risk Dashboard

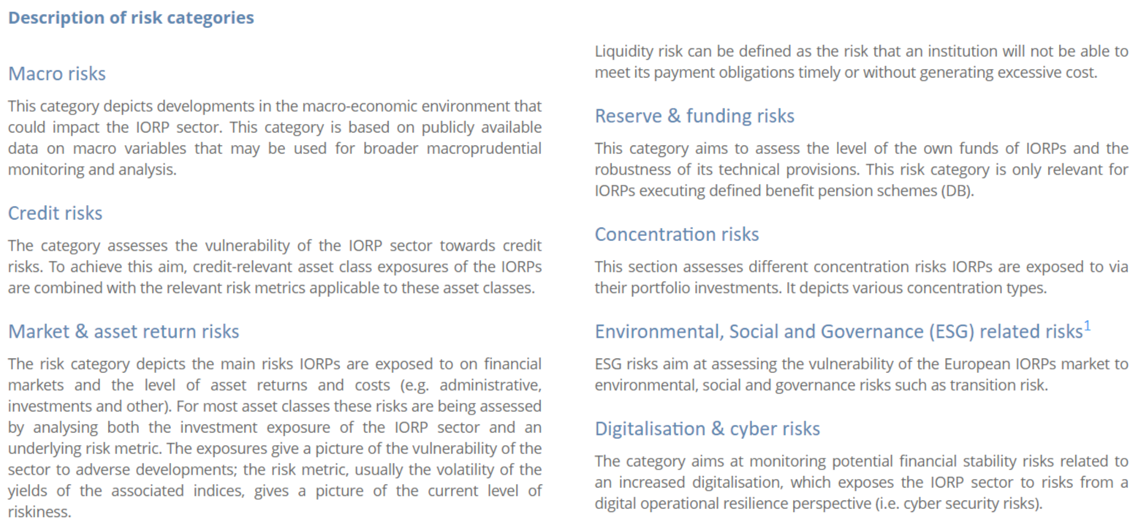
Risks	Level	Trend (Past 3 months)	Outlook (Next 12 months)
Macro risks	🟡	→	→
Credit risks	🟡	→	↗
Market & asset return risks	🟠	→	→
Liquidity risks	🟡	↑	→
Reserve & funding risks (DB Schemes)	🟡	→	→
Concentration risks	🟡	→	→
ESG related risks	🟡	→	→
Digitalisation & cyber risks	🟡	→	↗

It includes a set of risk indicators covering traditional risk categories, such as market and credit risks, liquidity risks, reserve & funding risks, as well as emerging threats like ESG and cyber risks.

The risk dashboard was developed in cooperation with National Competent Authorities with the objective to systematically:

- monitor and assess the risks and evolution thereof in the IORP sector from a macroprudential perspective; and

- analyse the potential vulnerabilities of IORPs' financial position and their implication to financial stability at the EEA level.



Description of risk categories

Macro risks

This category depicts developments in the macro-economic environment that could impact the IORP sector. This category is based on publicly available data on macro variables that may be used for broader macroprudential monitoring and analysis.

Credit risks

The category assesses the vulnerability of the IORP sector towards credit risks. To achieve this aim, credit-relevant asset class exposures of the IORPs are combined with the relevant risk metrics applicable to these asset classes.

Market & asset return risks

The risk category depicts the main risks IORPs are exposed to on financial markets and the level of asset returns and costs (e.g. administrative, investments and other). For most asset classes these risks are being assessed by analysing both the investment exposure of the IORP sector and an underlying risk metric. The exposures give a picture of the vulnerability of the sector to adverse developments; the risk metric, usually the volatility of the yields of the associated indices, gives a picture of the current level of riskiness.

Liquidity risk can be defined as the risk that an institution will not be able to meet its payment obligations timely or without generating excessive cost.

Reserve & funding risks

This category aims to assess the level of the own funds of IORPs and the robustness of its technical provisions. This risk category is only relevant for IORPs executing defined benefit pension schemes (DB).

Concentration risks

This section assesses different concentration risks IORPs are exposed to via their portfolio investments. It depicts various concentration types.

Environmental, Social and Governance (ESG) related risks[1]

ESG risks aim at assessing the vulnerability of the European IORPs market to environmental, social and governance risks such as transition risk.

Digitalisation & cyber risks

The category aims at monitoring potential financial stability risks related to an increased digitalisation, which exposes the IORP sector to risks from a digital operational resilience perspective (i.e. cyber security risks).

Results

The first edition shows that the IORPs' exposure to market & asset return risks is currently at a high level, making this the most relevant risk category for the sector given the still high volatility in bond markets.

Macro risks are at a medium level: there are positive developments related to a reduction in forecasted inflation, partially offset by a GDP growth outlook that remains weak by historical standards.

Liquidity risks are at a medium level but show an increasing trend compared to the previous quarter, driven by developments in derivative positions.

The net asset value of IORP's derivative positions went further into negative territory due to the continued increase of interest rates in Q3-2023.

All other risk categories are currently assessed at a medium level, with increases expected for credit risks as well as digitalisation and cyber risks over the next 12 months.

Key observations:

IORPs' exposure to market & asset return risks is currently at a high level, making this the most relevant risk category for the sector given the still high volatility in bond markets.

Macro risks are at a medium level: there are positive developments related to a reduction in forecasted inflation, partially offset by a GDP growth outlook that remains weak by historical standards.

Liquidity risks are at a medium level but show an increasing trend compared to the previous quarter, driven by developments in derivative positions. The net asset value of IORP's derivative positions went further into negative territory due to the continued increase of interest rates in Q3-2023.

All other risk categories are currently assessed at a medium level, with increases expected for credit risks as well as digitalisation and cyber risks over the next 12 months.

To read more: https://www.eiopa.europa.eu/eiopas-newly-launched-iorp-risk-dashboard-highlights-market-and-asset-return-risks-main-concerns-2024-02-01_en

ESAs recommend steps to enhance the monitoring of BigTechs' financial services activities

The European Supervisory Authorities (EBA, EIOPA and ESMA – the ESAs) published a report setting out the results of a stocktake of BigTech direct financial services provision in the EU.

The Report identifies the types of financial services currently carried out by BigTechs in the EU pursuant to EU licences and highlights inherent opportunities, risks, regulatory and supervisory challenges.

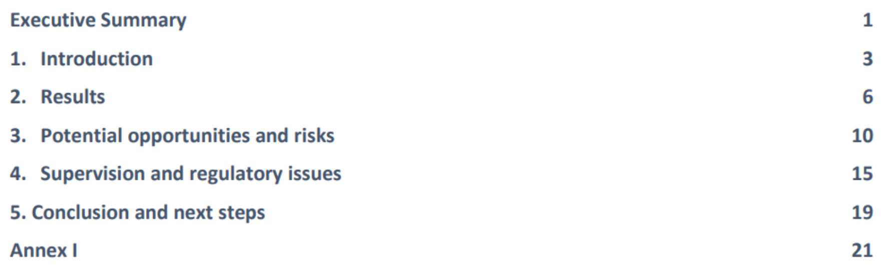
The ESAs will continue to strengthen the monitoring of the relevance of BigTech in the EU financial services sector, including via the establishment of a new monitoring matrix.

In 2023 the ESAs, via the European Forum for Innovation Facilitators (EFIF), conducted a cross-sectoral stocktake of BigTech subsidiaries providing financial services in the European Union (EU) as a follow-up to the ESAs' 2022 response to the European Commission's Call for Advice on Digital Finance.

The stocktake showed that BigTech subsidiary companies currently licenced to provide financial services pursuant to EU law mainly provide services in the payments, e-money and insurance sectors and, in limited cases, the banking sector. However, the ESAs have yet to observe their presence in the market for securities services.

To further strengthen the cross-sectoral mapping of BigTechs' presence and relevance to the EU's financial sector, the ESAs propose to set-up a data mapping tool within the EFIF.

This tool is intended to provide a framework that supervisors from the National Competent Authorities would be able to use to monitor on an ongoing and dynamic basis the BigTech companies' direct and indirect relevance to the EU financial sector.



The ESA will also continue the cross-disciplinary exchanges in the setting of the EFIF to further foster the exchange of information between EFIF members and other relevant financial and non-financial sector authorities involved in the monitoring of BigTechs' activities (e.g., data protection and consumer protection authorities).

Background

For the purpose of this Report, BigTechs are large technology companies with extensive customer networks, which include firms with core businesses in social media, internet search, software, online retail and telecoms.

The Report published today was one of the EFIF's work priorities for 2023, and extends the analysis conducted for the 2022 Joint ESAs Response to the European Commission 2021 Call for Advice on Digital Finance and related issues, which proposed recommendations in relation to the regulation and supervision of more fragmented or non-integrated value chains, platforms and bundling of various financial services, and risks of groups combining different activities.

The EFIF provides a platform for supervisors to regularly share experiences from their engagement with firms through innovation facilitators, to exchange technological expertise, and to reach common views on the regulatory treatment of innovative products, services and business models.

The EFIF was established following the 2019 Joint ESAs report on regulatory sandboxes and innovation hubs which identified the need for greater coordination and cooperation between innovation facilitators to support the scaling up of FinTech across the EU single market. The findings of the report have been updated in the ESAs Report on Innovation Facilitators published in December 2023.

Members of the EFIF include representatives of each innovation hub and regulatory sandbox established by national and European supervisors within the EEA. The EFIF unites representatives from all 30 countries in the EEA, covering the banking/payments, insurance and securities/markets sectors. More information about the EFIF can be found here.

For the purpose of this report, BigTechs are large technology companies with extensive customer networks, which include firms with core businesses in social media, internet search, software, online retail and telecoms.

To read more: https://www.eba.europa.eu/publications-and-media/press-releases/esas-recommend-steps-enhance-monitoring-bigtechs-financial

Proposed Insurance Circular Letter

NEW
YORK
STATE

TO: All Insurers Authorized to Write Insurance in New York State, Licensed Fraternal Benefit Societies, and the New York State Insurance Fund

RE: Use of Artificial Intelligence Systems and External Consumer Data and Information Sources in Insurance Underwriting and Pricing

I. Purpose and Background

The New York State Department of Financial Services ("Department") is committed to innovation and the responsible use of technology to improve financial access and contribute to the safety and stability of insurance markets. The Department expects that insurers use of emerging technologies such as artificial intelligence will be conducted in a manner that complies with all applicable federal and state laws, rules, and regulations.

The use of external consumer data and information sources ("ECDIS") and artificial intelligence systems ("AIS") can both benefit insurers and consumers alike by simplifying and expediting insurance underwriting and pricing processes, and potentially result in more accurate underwriting and pricing of insurance.

At the same time, ECDIS may reflect systemic biases and its use can reinforce and exacerbate inequality. This raises significant concerns about the potential for unfair adverse effects or discriminatory decision-making. ECDIS may also have variable accuracy and reliability and may come from entities that are not subject to regulatory oversight and consumer protections.

Furthermore, the self-learning behavior of AIS increases the risks of inaccurate, arbitrary, capricious, or unfairly discriminatory outcomes that may disproportionately affect vulnerable communities and individuals or otherwise undermine the insurance marketplace in New York.

Therefore, it is critical that insurers who utilize such technologies establish a proper governance and risk management framework to mitigate the potential harm to consumers and comply with all relevant legal obligations.

The purpose of this circular letter ("Circular Letter") is to identify DFS's expectations that all insurers authorized to write insurance in New York State, licensed fraternal benefit societies, and the New York State Insurance Fund (collectively, "insurers") develop and manage their use of ECDIS, artificial intelligence systems, and other predictive models in underwriting and pricing insurance policies and annuity contracts.

For purposes of this Circular Letter, AIS means any machine-based system designed to perform functions normally associated with human intelligence, such as reasoning, learning, and self-improvement, that is used – in whole or in part – to supplement traditional medical, property or casualty underwriting or pricing, as a proxy for traditional medical, property or casualty underwriting or pricing, or to establish "lifestyle indicators" that may contribute to an underwriting or pricing assessment of an applicant for insurance coverage.

For purposes of this Circular Letter, ECDIS includes data or information used – in whole or in part – to supplement traditional medical, property or casualty underwriting or pricing, as a proxy for traditional medical, property or casualty underwriting or pricing, or to establish "lifestyle indicators" that may contribute to an underwriting or pricing assessment of an applicant for insurance coverage.

For the purposes of this Circular Letter, ECDIS does not include an MIB Group, Inc. member information exchange service, a motor vehicle report, or a criminal history search. An insurer conducting a criminal history search for insurance underwriting and pricing purposes must comply with Executive Law § 296(16). See e.g., Insurance Circular Letter No. 13 (2022).

An insurer may deploy ECDIS and AIS in a variety of ways throughout the underwriting and pricing process. The Department recognizes there is no one-size-fits-all approach to managing data and decisioning systems.

Therefore, insurers should take an approach to developing and managing their use of ECDIS and AIS that is reasonable and appropriate to each insurer's business model and the overall complexity and materiality of the risks inherent in using ECDIS and AIS.

This Circular Letter is not intended to provide an exhaustive list of potential issues that could arise from the use of ECDIS or AIS and is not intended to suggest that an insurer's due diligence in assessing ECDIS or AIS should be limited to the concerns enumerated below.

This Circular Letter also is not intended to address phases of the insurance product lifecycle other than underwriting and pricing.
The Department may audit and examine an insurer's use of ECDIS and AIS, including within the scope of regular or targeted examinations pursuant to New York Insurance Law ("Insurance Law") § 309, or a request for special report pursuant to Insurance Law § 308.

II. Fairness Principles

An insurer should not use ECDIS or AIS for underwriting or pricing purposes unless the insurer can establish that the data source or model, as applicable, does not use and is not based in any way on any class protected pursuant to Insurance Law Article 26. Moreover, an insurer should not use ECDIS or AIS for underwriting or pricing purposes if such use would result in or permit any unfair discrimination or otherwise violate the Insurance Law or any regulations promulgated thereunder.

A. Data Actuarial Validity

As with any other variables employed in underwriting and pricing, insurers should be able to demonstrate that the ECDIS are supported by generally accepted actuarial standards of practice and are based on actual or reasonably anticipated experience, including, but not limited to, statistical studies, predictive modeling, and risk assessments.

The underlying analyses should demonstrate a clear, empirical, statistically significant, rational, and not unfairly discriminatory relationship between the variables used and the relevant risk of the insured.

Insurers must be able to demonstrate that the ECDIS employed for underwriting and pricing are not prohibited by the Insurance Law or regulations promulgated thereunder and should be able to demonstrate that they do not serve as a proxy for any protected classes that may result in unfair or unlawful discrimination.

B. Unfair and Unlawful Discrimination

State and federal law prohibits insurers from unlawfully discriminating against certain protected classes of individuals and from engaging in unfair discrimination, including the ability of insurers to underwrite based on certain criteria.

An insurer should not use ECDIS or AIS in underwriting or pricing unless the insurer has determined that the ECDIS or AIS does not collect or use criteria that would constitute unfair or unlawful discrimination or an unfair trade practice.

When using ECDIS or AIS as part of their insurance business, insurers are responsible for complying with these anti-discrimination laws irrespective of whether they themselves are collecting data and directly underwriting consumers, or relying on ECDIS or AIS of external vendors that are intended to be partial or full substitutes for direct underwriting or pricing.

An insurer may not use ECDIS or AIS to collect or use information that the insurer would otherwise be prohibited from collecting or using directly.

An insurer may not rely solely on a vendor’s claim of non-discrimination or a proprietary third-party process to determine compliance with anti-discrimination laws. The responsibility to comply with anti-discrimination laws remains with the insurer at all times.

An insurer should not use ECDIS or AIS in underwriting or pricing unless the insurer can establish through a comprehensive assessment that the underwriting or pricing guidelines are not unfairly or unlawfully discriminatory in violation of the Insurance Law. A comprehensive assessment of whether an underwriting or pricing guideline derived from ECDIS or AIS unfairly discriminates between similarly situated individuals or unlawfully discriminates against a protected class should, at a minimum, include the following steps:

- assessing whether the use of ECDIS or AIS produces disproportionate adverse effects in underwriting and/or pricing on similarly situated insureds, or insureds of a protected class. If there is no prima facie showing of a disproportionate adverse effect, then the insurer may conclude its evaluation.

- if there is prima facie showing of such a disproportionate adverse effect, further assessing whether there is a legitimate, lawful, and fair explanation or rationale for the differential effect on similarly situated insureds. If no legitimate, lawful, and fair explanation or rationale can account for the differential effect on similarly situated insureds, the insurer should modify its use of such ECDIS or AIS and evaluate the modified use of ECDIS or AIS.

- if a legitimate, lawful, and fair explanation or rationale can account for the differential effect, further conducting and appropriately documenting a search and analysis for a less discriminatory alternative variable(s) or methodology that would reasonably meet the insurer's legitimate business needs. If a less discriminatory alternative exists, the insurer should modify its use of ECDIS or AIS accordingly.

To read more:
https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2024_nn_proposed

ENISA Single Programming Document 2024 – 2026

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

Strategy

EMPOWERING COMMUNITIES

Cybersecurity is a shared responsibility. Europe strives for a cross sectoral, all-inclusive cooperation framework. ENISA plays a key role in stimulating active cooperation between the cybersecurity stakeholders in MSs and the EU institutions and agencies.

It strives to ensure the complementarity of common efforts, by adding value to the stakeholders, exploring synergies and effectively using limited cybersecurity expertise and resources. Communities should be empowered to scale up the cybersecurity model.

CYBERSECURITY POLICY

Cybersecurity is the cornerstone of digital transformation and the need for it permeates all sectors, therefore it needs to be considered across a broad range of policy fields and initiatives.

Cybersecurity must not be restricted to a specialist community of technical cybersecurity experts. Cybersecurity must therefore be embedded across all domains of EU policies. Avoiding fragmentation and the need for a coherent approach while taking into account the specificities of each sector is essential.

OPERATIONAL COOPERATION

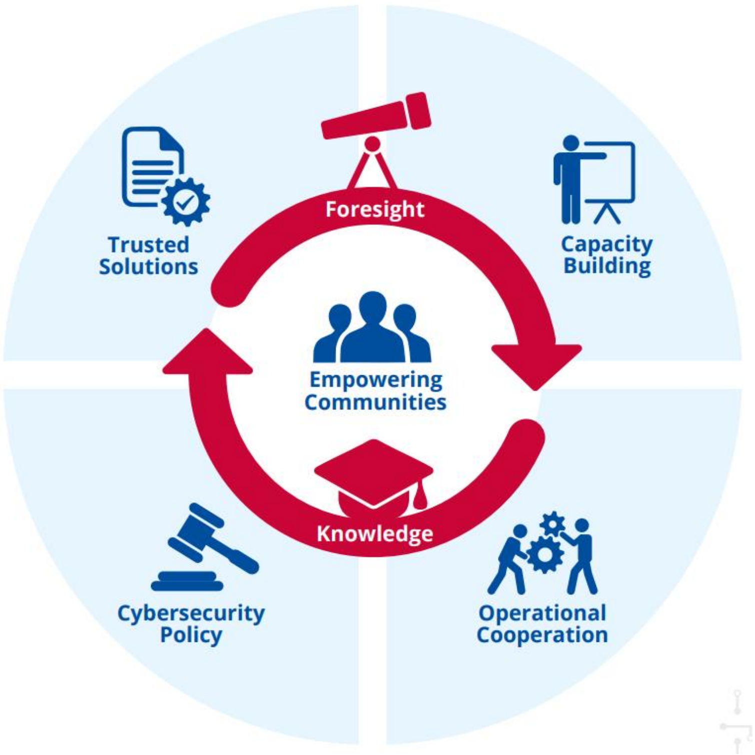
The benefits of the European digital economy and society can only be fully attained under the premise of cybersecurity. Cyberattacks know no borders. All layers of society can be impacted and the Union needs to be ready to respond to massive (large-scale and cross-border) cyber-attacks and cyber crisis.

Cross-border interdependencies have highlighted the need for effective cooperation between MSs and the EU institutions for faster response and proper coordination of efforts at all levels (strategic, operational, technical and communications).

CAPACITY BUILDING

The frequency and sophistication of cyberattacks is rising speedily, while at the same time the use of information and communications technology (ICT) infrastructures and technologies by individuals, organisations and industries is increasing rapidly. The needs for cybersecurity knowledge and competences exceeds the supply.

The EU has to invest in building competences and talents in cybersecurity at all levels, from the non-expert to the highly skilled professional. The investments should focus not only on increasing the cybersecurity skillset in the MSs but also on making sure that the different operational communities possess the appropriate capacity to deal with the cyber threat landscape.



TRUSTED SOLUTIONS

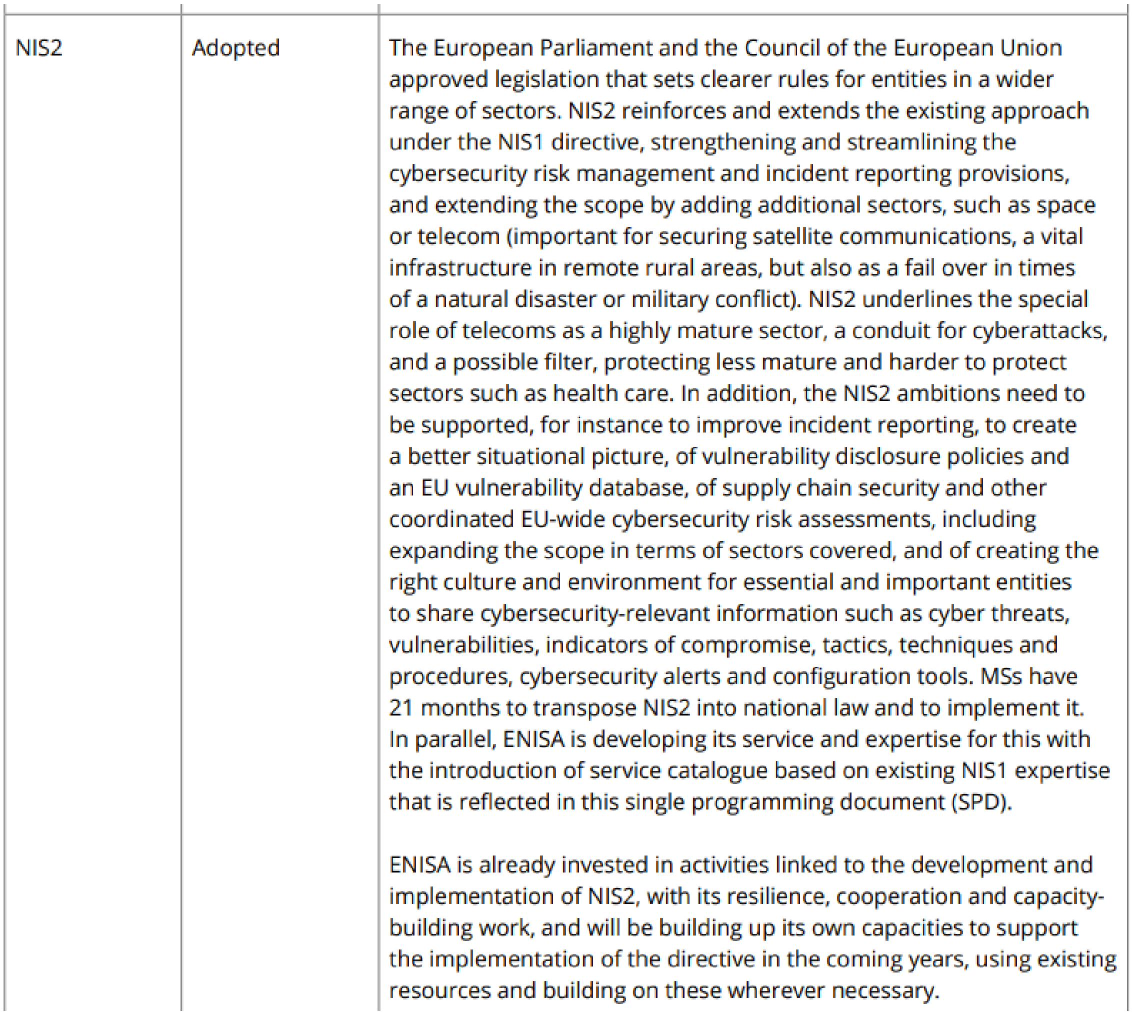
Digital products and services bring benefits as well as risks, and these risks must be identified and mitigated. In the process of evaluating the security of digital solutions and ensuring their trustworthiness, it is essential to adopt a common approach, with the goal to strike a balance between societal, market, economic and cybersecurity needs. A neutral entity acting in a transparent manner will increase customer trust in digital solutions and the wider digital environment.

FORESIGHT

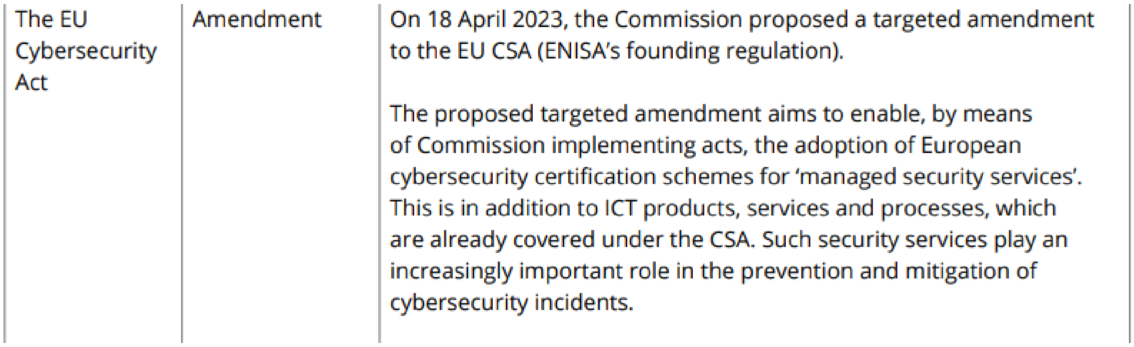
Numerous new technologies, still in their infancy or close to mainstream adoption, would benefit from the use of foresight methods. Through a structured process enabling dialogue among stakeholders, decision- and policymakers would be able to define early mitigation strategies that improve the EU's resilience to cybersecurity threats and find solutions to address emerging challenges.

KNOWLEDGE

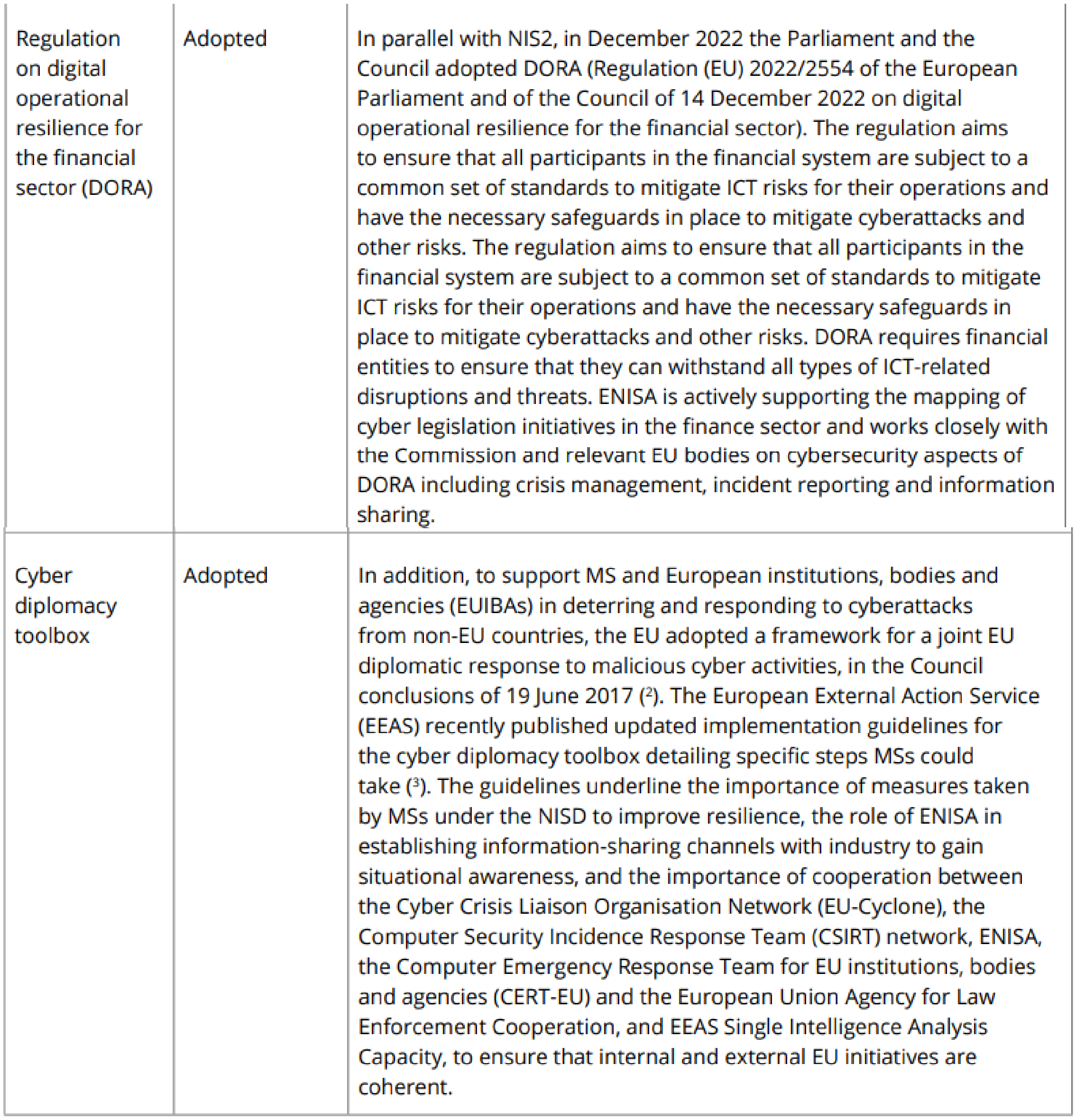
The energy that fuels the mill of cybersecurity is information and knowledge. For cybersecurity professionals to be efficient at tackling objectives, to work in a constantly moving environment – in terms of digital developments as well as with regard to actors – to face the challenges of our time, a continuous process of collecting, organising, summarising, analysing, communicating, and maintaining cybersecurity information and knowledge is clearly needed. All phases are essential to ensure that information and knowledge is shared and expanded within the EU cybersecurity ecosystem.



NIS2	Adopted	The European Parliament and the Council of the European Union approved legislation that sets clearer rules for entities in a wider range of sectors. NIS2 reinforces and extends the existing approach under the NIS1 directive, strengthening and streamlining the cybersecurity risk management and incident reporting provisions, and extending the scope by adding additional sectors, such as space or telecom (important for securing satellite communications, a vital infrastructure in remote rural areas, but also as a fail over in times of a natural disaster or military conflict). NIS2 underlines the special role of telecoms as a highly mature sector, a conduit for cyberattacks, and a possible filter, protecting less mature and harder to protect sectors such as health care. In addition, the NIS2 ambitions need to be supported, for instance to improve incident reporting, to create a better situational picture, of vulnerability disclosure policies and an EU vulnerability database, of supply chain security and other coordinated EU-wide cybersecurity risk assessments, including expanding the scope in terms of sectors covered, and of creating the right culture and environment for essential and important entities to share cybersecurity-relevant information such as cyber threats, vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools. MSs have 21 months to transpose NIS2 into national law and to implement it. In parallel, ENISA is developing its service and expertise for this with the introduction of service catalogue based on existing NIS1 expertise that is reflected in this single programming document (SPD). ENISA is already invested in activities linked to the development and implementation of NIS2, with its resilience, cooperation and capacity-building work, and will be building up its own capacities to support the implementation of the directive in the coming years, using existing resources and building on these wherever necessary.



The EU Cybersecurity Act	Amendment	On 18 April 2023, the Commission proposed a targeted amendment to the EU CSA (ENISA's founding regulation). The proposed targeted amendment aims to enable, by means of Commission implementing acts, the adoption of European cybersecurity certification schemes for 'managed security services'. This is in addition to ICT products, services and processes, which are already covered under the CSA. Such security services play an increasingly important role in the prevention and mitigation of cybersecurity incidents.



Regulation on digital operational resilience for the financial sector (DORA)	Adopted	In parallel with NIS2, in December 2022 the Parliament and the Council adopted DORA (Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector). The regulation aims to ensure that all participants in the financial system are subject to a common set of standards to mitigate ICT risks for their operations and have the necessary safeguards in place to mitigate cyberattacks and other risks. The regulation aims to ensure that all participants in the financial system are subject to a common set of standards to mitigate ICT risks for their operations and have the necessary safeguards in place to mitigate cyberattacks and other risks. DORA requires financial entities to ensure that they can withstand all types of ICT-related disruptions and threats. ENISA is actively supporting the mapping of cyber legislation initiatives in the finance sector and works closely with the Commission and relevant EU bodies on cybersecurity aspects of DORA including crisis management, incident reporting and information sharing.
Cyber diplomacy toolbox	Adopted	In addition, to support MS and European institutions, bodies and agencies (EUIBAs) in deterring and responding to cyberattacks from non-EU countries, the EU adopted a framework for a joint EU diplomatic response to malicious cyber activities, in the Council conclusions of 19 June 2017 [2]. The European External Action Service (EEAS) recently published updated implementation guidelines for the cyber diplomacy toolbox detailing specific steps MSs could take [3]. The guidelines underline the importance of measures taken by MSs under the NISD to improve resilience, the role of ENISA in establishing information-sharing channels with industry to gain situational awareness, and the importance of cooperation between the Cyber Crisis Liaison Organisation Network (EU-Cyclone), the Computer Security Incidence Response Team (CSIRT) network, ENISA, the Computer Emergency Response Team for EU institutions, bodies and agencies (CERT-EU) and the European Union Agency for Law Enforcement Cooperation, and EEAS Single Intelligence Analysis Capacity, to ensure that internal and external EU initiatives are coherent.

To read more: https://www.enisa.europa.eu/publications/corporate-documents/enisa-single-programming-document-2024-2024

The first set of final draft technical standards under the Digital Operational Resilience Act (DORA).

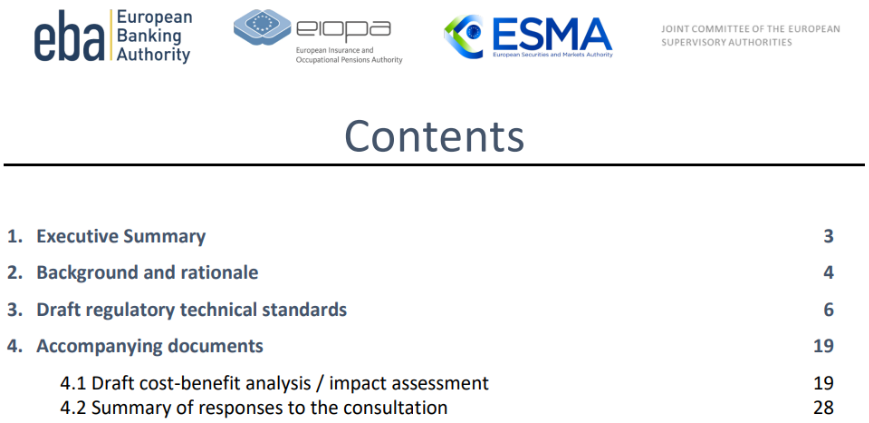
The three European Supervisory Authorities (EBA, EIOPA and ESMA – the ESAs) published the first set of final draft technical standards under the Digital Operational Resilience Act (DORA) aimed at enhancing the digital operational resilience of the EU financial sector by strengthening financial entities' Information and Communication Technology (ICT) and third-party risk management and incident reporting frameworks. The joint final draft technical standards include:

1. Final report, Draft Regulatory Technical Standards to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Contents

2. Final report on Draft Regulatory Technical Standards to specify the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers as mandated by Regulation (EU) 2022/2554.

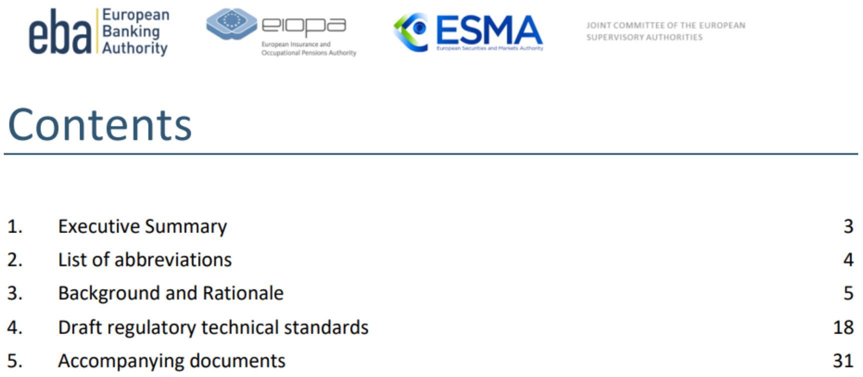


JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Contents

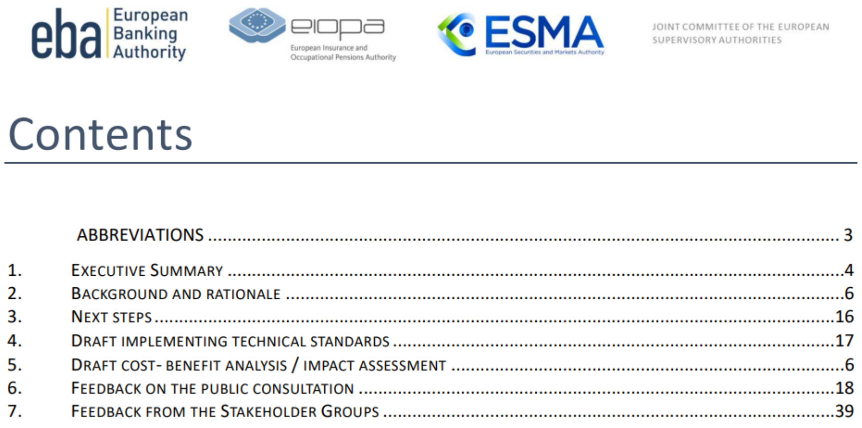
3. Final report on Draft Regulatory Technical Standards specifying the criteria for

the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under Regulation (EU) 2022/2554.


eba European Banking Authority
eiopa European Insurance and Occupational Pensions Authority
ESMA European Securities and Markets Authority
JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Contents

4. Final Report On Draft Implementing Technical Standards on the standard templates for the purposes of the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers under Article 28(9) of Regulation (EU) 2022/2554


eba European Banking Authority
eiopa European Insurance and Occupational Pensions Authority
ESMA European Securities and Markets Authority
JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Contents

To read more: https://www.eba.europa.eu/publications-and-media/press-releases/esas-publish-first-set-rules-under-dora-ict-and-third-party

We carefully monitor the developments at: https://www.digital-operational-resilience-act.com

This website belongs to Cyber Risk GmbH, a sister entity of the IARCP.

The Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554 solves an important problem in the EU financial regulation. Before DORA, financial institutions managed the main categories of operational risk mainly with the allocation of capital, but they did not manage all components of operational resilience.

After DORA, they must also follow rules for the protection, detection, containment, recovery and repair capabilities against ICT-related incidents. DORA explicitly refers to ICT risk and sets rules on ICT risk-management, incident reporting, operational resilience testing and ICT third-party risk monitoring.

This Regulation acknowledges that ICT incidents and a lack of operational resilience have the possibility to jeopardise the soundness of the entire financial system, even if there is "adequate" capital for the traditional risk categories.

Italian Data Protection Authority
ChatGPT: Italian DPA notifies breaches of privacy law to OpenAI

GPDP | GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

The Italian DPA (Garante per la protezione dei dati personali) notified breaches of data protection law to OpenAI, the company behind ChatGPT's AI platform.

Following the temporary ban on processing imposed on OpenAI by the Garante on 30 March of last year, and based on the outcome of its fact-finding activity, the Italian DPA concluded that the available evidence pointed to the existence of breaches of the provisions contained in the EU GDPR.

OpenAI may submit its counterclaims concerning the alleged breaches within 30 days.

The Italian Garante will take account of the work in progress within the ad-hoc task force set up by the European Data Protection Framework in its final determination on the case.

To read more: https://garanteprivacy.it/home/docweb/-/docweb-display/docweb/9978020#english

The temporary ban (*31 March 2023)*

The Italian SA imposed an immediate temporary limitation on the processing of Italian users' data by OpenAI, the US-based company developing and managing the platform. An inquiry into the facts of the case was initiated as well.

A data breach affecting ChatGPT users' conversations and information on payments by subscribers to the service had been reported on 20 March. ChatGPT is the best known among relational AI platforms that are capable to emulate and elaborate human conversations.

In its order, the Italian SA highlights that no information is provided to users and data subjects whose data are collected by Open AI; more importantly, there appears to be no legal basis underpinning the massive collection and processing of personal data in order to 'train' the algorithms on which the platform relies.

As confirmed by the tests carried out so far, the information made available by ChatGPT does not always match factual circumstances, so that inaccurate personal data are processed.

Finally, the Italian SA emphasizes in its order that the lack of whatever age verification mechanism exposes children to receiving responses that are absolutely inappropriate to their age and awareness, even though the service is allegedly addressed to users aged above 13 according to OpenAI's terms of service.

OpenAI is not established in the EU, however it has designated a representative in the European Economic Area. It will have to notify the Italian SA within 20 days of the measures implemented to comply with the order, otherwise a fine of up to EUR 20 million or 4% of the total worldwide annual turnover may be imposed.

The temporary ban: https://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870847#english

Judgment of the Court in Case C-118/22

Right to erasure: the general and indiscriminate storage of biometric and genetic data of persons convicted of criminal offences, until their death, is contrary to EU law

COURT OF JUSTICE
OF THE EUROPEAN UNION

In Bulgaria, an entry was made in the police records concerning a person in the course of a criminal investigation for failing to tell the truth as a witness.

That person was ultimately found guilty of that offence and given a one year suspended sentence.

After serving that sentence, that person was legally rehabilitated. He subsequently applied to be removed from the police records.

Under Bulgarian law, the data relating to him are retained in those records and may be processed by the authorities, who have access to them without any time limit other than his death.

His application was rejected on the ground that a final criminal conviction, even after legal rehabilitation, is not one of the grounds for removal of the entry from the police records.

On appeal, the Bulgarian Supreme Administrative Court referred questions to the Court of Justice.

In its judgment, the Court of Justice holds that the general and indiscriminate storage of biometric and genetic data of persons convicted of an intentional offence, until their death, is contrary to EU law.

The Court notes that the personal data stored in the police records in Bulgaria include, amongst other things, fingerprints, a photograph and a DNA sample taken for profiling purposes.

The records also contain data relating to the criminal offences committed by the data subject and to his or her convictions in that regard.

Those data may be essential for the purposes of verifying whether the data subject is involved in criminal offences other than that in respect of which he or she was convicted by final judgment.

However, such persons do not all present the same degree of risk of being involved in other criminal offences, justifying a uniform period of storage of the data relating to them. Thus, factors such as the nature and seriousness of the offence committed or the absence of recidivism may mean that the risk represented by the convicted person does not necessarily justify the storage of the data relating to that person in the police records until his or her death.

Consequently, that time limit is appropriate only in specific circumstances which duly justify it. That is not the case where it is applicable generally and indiscriminately to any person convicted by final judgment of an intentional offence.

Under EU law, national legislation must lay down an obligation for the data controller to review periodically whether that storage is still necessary and to grant the data subject the right to have those data erased if that is no longer the case.

To read more: https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-01/cp240020en.pdf

https://curia.europa.eu/juris/documents.jsf?num=C-118/22

Artificial intelligence in central banking

Douglas Araujo, Sebastian Doerr, Leonardo Gambacorta, Bruno Tissot

Key takeaways

1. Central banks have been early adopters of machine learning techniques for statistics, macro analysis, payment systems oversight and supervision, with considerable success.

2. Artificial intelligence brings many opportunities in support of central bank mandates, but also challenges – some general and others specific to central banks.

3. Central bank collaboration, for instance through knowledge-sharing and pooling of expertise, holds great promise in keeping central banks at the vanguard of developments in artificial intelligence.

Long before artificial intelligence (AI) became a focal point of popular commentary and widespread fascination, central banks were early adopters of machine learning methods to obtain valuable insights for statistics, research and policy (Doerr et al (2021), Araujo et al (2022, 2023)).

The greater capabilities and performance of the new generation of machine learning techniques open up further opportunities. Yet harnessing these requires central banks to build up the necessary infrastructure and expertise.

Central banks also need to address concerns about data quality and privacy as well as risks emanating from dependence on a few providers.

This Bulletin first provides a brief summary of concepts in the machine learning and AI space. It then discusses central bank use cases in four areas:

(i) information collection and the compilation of official statistics;

(ii) macroeconomic and financial analysis to support monetary policy;

(iii) oversight of payment systems; and (iv) supervision and financial stability.

The Bulletin also summarises the lessons learned and the opportunities and challenges arising from the use of machine learning and AI.

It concludes by discussing how central bank cooperation can play a key role going forward.

Overview of machine learning methods and AI

Broadly speaking, machine learning comprises the set of techniques designed to extract information from data, especially with a view to making predictions.

Machine learning can be seen as an outgrowth of traditional statistical and econometric techniques, although it does not rely on a pre-specified model or on statistical assumptions such as linearity or normality.

The process of fitting a machine learning model to data is called training.

The criterion for successful training is the ability to predict outcomes on previously unseen (“out-of-sample”) data, irrespective of how the models predict them.

This section describes some of the most common techniques used in central banks, based on the regular stocktaking exercises organised in the central banking community under the umbrella of the BIS Irving Fisher Committee on Central Bank Statistics (IFC).

To read more: https://www.bis.org/publ/bisbull84.pdf

BIS Bulletin

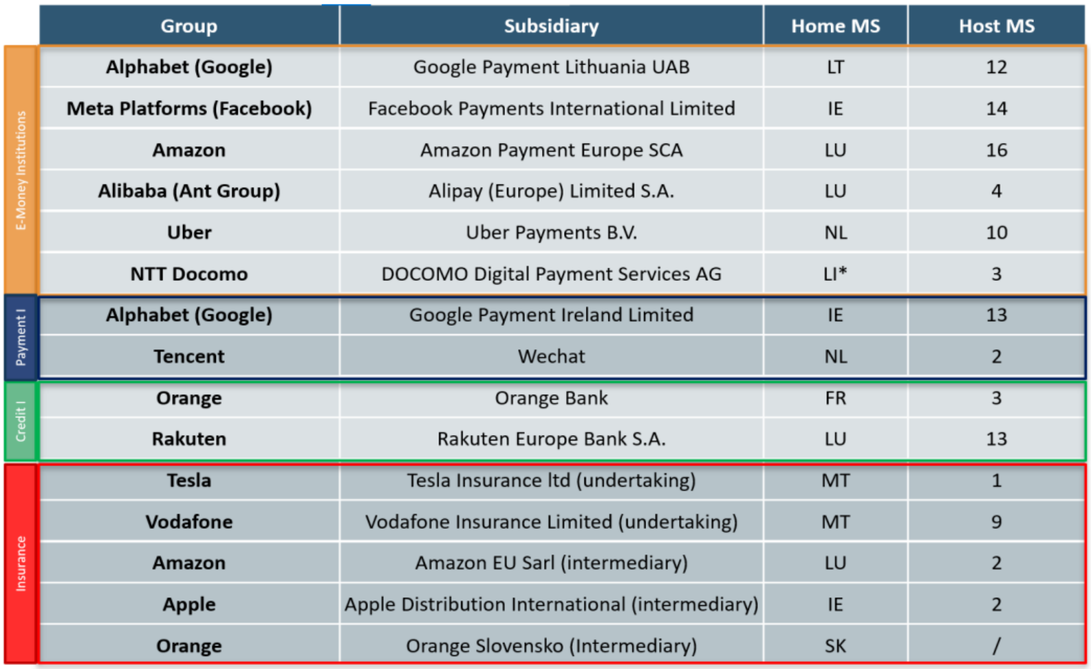
No 84

Artificial intelligence in central banking

The European Supervisory Authorities (ESAs) recommend steps to enhance the monitoring of BigTechs' financial services activities

The European Supervisory Authorities (EBA, EIOPA and ESMA) published a Report setting out the results of a stocktake of BigTech direct financial services provision in the EU.

Table 1: Stocktake results: MAGs as electronic money institutions (EMI), payment institutions (PI), credit institutions (CI), insurance intermediaries/undertakings.



	Group	Subsidiary	Home MS	Host MS
E-Money Institutions	**Alphabet (Google)**	Google Payment Lithuania UAB	LT	12
	Meta Platforms (Facebook)	Facebook Payments International Limited	IE	14
	Amazon	Amazon Payment Europe SCA	LU	16
	Alibaba (Ant Group)	Alipay (Europe) Limited S.A.	LU	4
	Uber	Uber Payments B.V.	NL	10
	NTT Docomo	DOCOMO Digital Payment Services AG	LI*	3
Payment I	**Alphabet (Google)**	Google Payment Ireland Limited	IE	13
	Tencent	Wechat	NL	2
Credit I	**Orange**	Orange Bank	FR	3
	Rakuten	Rakuten Europe Bank S.A.	LU	13
Insurance	**Tesla**	Tesla Insurance ltd (undertaking)	MT	1
	Vodafone	Vodafone Insurance Limited (undertaking)	MT	9
	Amazon	Amazon EU Sarl (intermediary)	LU	2
	Apple	Apple Distribution International (intermediary)	IE	2
	Orange	Orange Slovensko (Intermediary)	SK	/

*LI: until 1 June 2022

The Report identifies the types of financial services currently carried out by BigTechs in the EU pursuant to EU licences and highlights inherent opportunities, risks, regulatory and supervisory challenges.

The ESAs will continue to strengthen the monitoring of the relevance of BigTech in the EU financial services sector, including via the establishment of a new monitoring matrix.

In 2023 the ESAs, via the European Forum for Innovation Facilitators (EFIF), conducted a cross-sectoral stocktake of BigTech subsidiaries providing financial services in the European Union (EU) as a follow-up to the ESAs' 2022 response to the European Commission's Call for Advice on Digital Finance.

The stocktake showed that BigTech subsidiary companies currently licenced to provide financial services pursuant to EU law mainly provide services in the payments, e-money and insurance sectors and, in limited cases, the banking sector. However, the ESAs have yet to observe their presence in the market for securities services.

European Banking Authority

eiopa European Insurance and Occupational Pensions Authority

ESMA European Securities and Markets Authority

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

JC 2024 02

01/02/2024

Report on 2023 stocktaking of BigTech direct financial services provision in the EU

Joint-ESA Report

To further strengthen the cross-sectoral mapping of BigTechs' presence and relevance to the EU's financial sector, the ESAs propose to set-up a data mapping tool within the EFIF.

This tool is intended to provide a framework that supervisors from the National Competent Authorities would be able to use to monitor on an ongoing and dynamic basis the BigTech companies' direct and indirect relevance to the EU financial sector.

Figure 1: Potential opportunities arising from intragroup dependencies

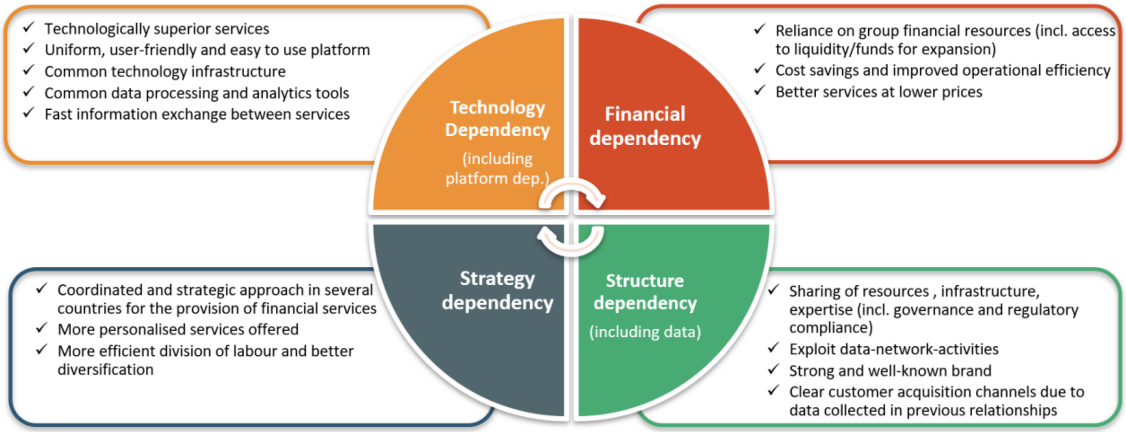
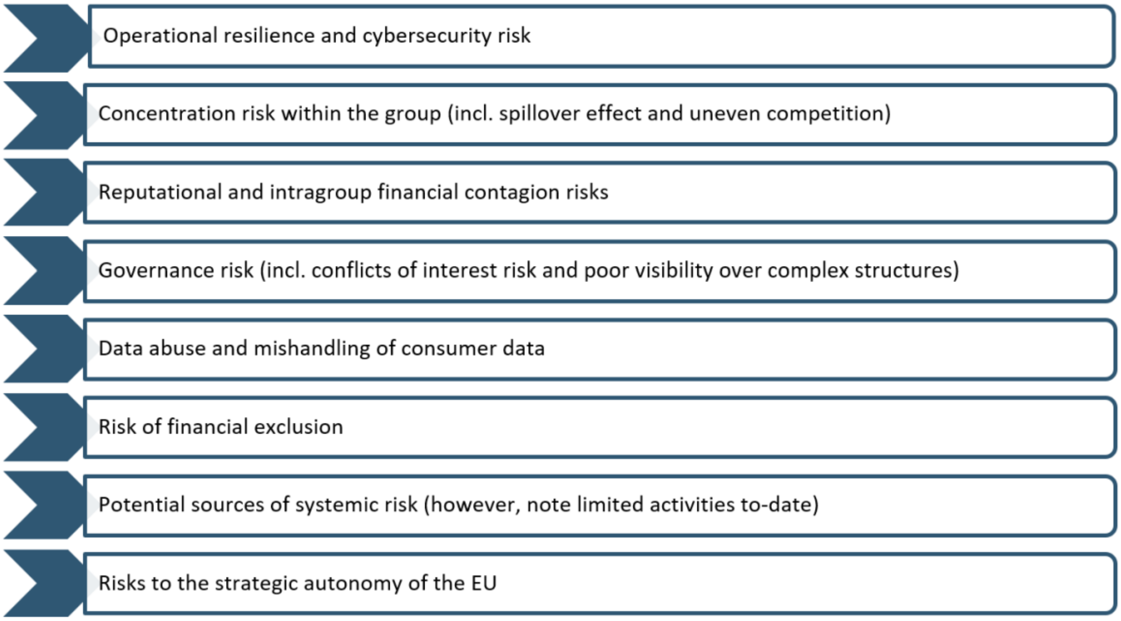

✓ Technologically superior services
✓ Uniform, user-friendly and easy to use platform
✓ Common technology infrastructure
✓ Common data processing and analytics tools
✓ Fast information exchange between services
Technology Dependency
(including platform dep.)
Financial dependency
✓ Reliance on group financial resources (incl. access to liquidity/funds for expansion)
✓ Cost savings and improved operational efficiency
✓ Better services at lower prices
✓ Coordinated and strategic approach in several countries for the provision of financial services
✓ More personalised services offered
✓ More efficient division of labour and better diversification
Strategy dependency
Structure dependency
(including data)
✓ Sharing of resources , infrastructure, expertise (incl. governance and regulatory compliance)
✓ Exploit data-network-activities
✓ Strong and well-known brand
✓ Clear customer acquisition channels due to data collected in previous relationships

Figure 2: Potential risks arising from intragroup dependencies



Operational resilience and cybersecurity risk

Concentration risk within the group (incl. spillover effect and uneven competition)

Reputational and intragroup financial contagion risks

Governance risk (incl. conflicts of interest risk and poor visibility over complex structures)

Data abuse and mishandling of consumer data

Risk of financial exclusion

Potential sources of systemic risk (however, note limited activities to-date)

Risks to the strategic autonomy of the EU

The ESA will also continue the cross-disciplinary exchanges in the setting of the EFIF to further foster the exchange of information between EFIF members and other relevant financial and non-financial sector authorities involved in the monitoring of BigTechs' activities (e.g., data protection and consumer protection authorities).

To read more: https://www.eiopa.europa.eu/system/files/2024-02/Joint%20ESAs%20Report%20-%20Stocktaking%20of%20BigTech%20direct%20financial%20services%20provision%20in%202023.pdf

Disclaimer

The Solvency II Association (hereinafter "Association") enhances public access to information. Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

The Association expressly disclaims all warranties, either expressed or implied, including any implied warranty of fitness for a particular purpose, and neither assumes nor authorizes any other person to assume for it any liability in connection with the information or training programs provided.

The Association and its employees will not be liable for any loss or damages of any nature, either direct or indirect, arising from use of the information provided, as these are general information, not specific guidance for an organization or a firm in a specific country.

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;

- is in no way constitutive of interpretative;

- 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.

We are not responsible for opinions and information posted by others. The inclusion of links to other web sites does not necessarily imply a recommendation or endorsement of the views expressed within them. Links to other web sites are presented as a convenience to users. The Association does not accept any responsibility for the content, accuracy, reliability, or currency found on external web sites.

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.

Readers that are interested in a specific topic covered in the newsletter, must download the official papers, must find more information, and must ask for legal and technical advice, before making any business decisions.

The Solvency ii Association

The Solvency ii Association is the largest Association of Solvency ii professionals in the world.

The Association is a business unit of Compliance LLC, incorporated in Wilmington, NC, and offices in Washington, DC, a provider of risk and compliance training in 57 countries.

Join us. Stay current. Read our monthly newsletter with news, alerts, challenges and opportunities. Get certified and provide independent evidence that you are a Solvency II expert.

Our reading room:
https://www.solvency-ii-association.com/Reading__Room.htm

Contact Us

Lyn Spooner
Email: lyn@solvency-ii-association.com

George Lekatis
President of the Solvency II Association
1200 G Street NW Suite 800,
Washington DC 20005, USA
Email: lekatis@solvency-ii-association.com
Web: www.solvency-ii-association.com
HQ: 1220 N. Market Street Suite 804
Wilmington DE 19801, USA