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, March 2023

Dear members and friends,

We will strart with the joint ESAs-ECB Statement on disclosure on climate change for structured finance products.

The European Supervisory Authorities (ESAs) and the ECB are committed to contributing to the transition towards a more sustainable economy within their respective mandates.

As investment in financial products meeting high environmental, social and governance (ESG) standards is increasingly important in the European Union (EU), it has also become a priority for structured finance products to disclose climate-related information on the underlying assets.

ESMA, with the contribution of EBA, EIOPA and the ECB, is hence working towards enhancing disclosure standards for securitised assets by including new, proportionate and targeted climate change-related information.

The ESAs and the ECB also call on issuers, sponsors and originators of such assets at EU level to proactively collect high-quality and

comprehensive information on climate-related risks during the origination process.

This call for improved disclosure concerns all funding instruments that are backed by the same type of underlying assets.

Enhanced climate related data are needed for securitised assets

Securitisation transactions are often backed by assets that could be directly exposed to physical or transition climate-related risks, such as real estate mortgages or auto loans.

Since the value of these underlying assets could be affected by climate-related events, the ESAs and the ECB share the view that the reporting on existing climate-related metrics needs to improve, and that additional metrics are necessary.

Additional climate related data will allow investors to better identify climate change-related risks while avoiding overreliance on estimates from external sources.

The lack of climate-related data on the assets underlying structured finance products not only poses a problem for properly assessing and addressing climate-related risks but also impedes the classification of products and services as sustainable under the EU Taxonomy Regulation and Sustainable Finance Disclosure Regulation (SFDR).

The ESAs and the ECB are committed to supporting better and targeted disclosures for structured finance products

The ESAs are committed to promoting transparency and robust disclosure requirements for financial institutions and financial products.

The ESAs have been developing advice and Regulatory Technical Standards under the EU Taxonomy Regulation and the Sustainable Finance Disclosure Regulation.

They are also currently reviewing the SFDR Delegated Regulation to enhance ESG disclosures by financial market participants, including to require additional disclosures on decarbonisation targets.

Sustainable finance is a key priority of the ESAs, and further deepening the integration of ESG factors across their activities will be a focus for their action in the coming months and years.

Enhanced climate-related disclosure requirements for securitised assets are also essential to the ECB.

Assets-backed securities constitute one of the most important asset classes mobilised by counterparties as collateral in Eurosystem credit operations. Moreover, the Eurosystem, with its asset backed securities purchase programme (ABSPP), has also become one of the largest investors in such assets in the euro area.

In July 2022 the ECB announced that it was taking further steps to include climate change considerations in its purchase programmes and collateral framework with the aims to better take into account climate-related financial risk in monetary policy implementation and – within its mandate – to support the green transition of the economy in line with the EU's climate neutrality objectives.

In this context, the ECB is committed to acting as a catalyst, engaging closely with the relevant EU authorities to support better and harmonised disclosure of climate-related data for assets mobilised as collateral.

Proportionate, standardised and readily accessible data Substantial efforts are already underway to improve sustainability-related transparency in securitisations.

The ESAs have been developing templates for voluntary sustainability-related disclosures for "simple, transparent and standardised" (STS) securitisations.

In March 2022, the EBA also provided guidance on how ESG standards could be implemented in the context of securitisation.

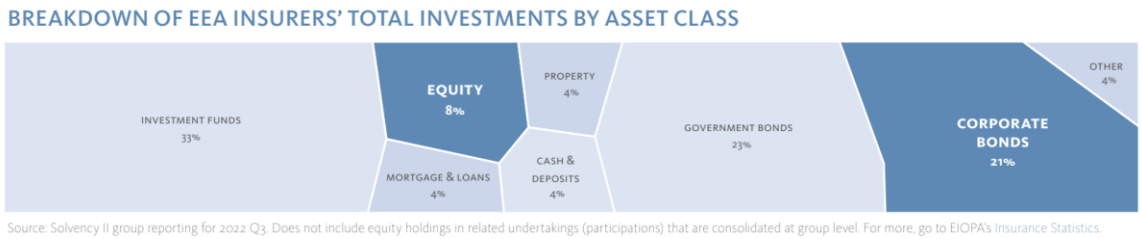
To read more: https://www.eiopa.europa.eu/system/files/2023-03/ESAs-ECB-Joint-Statement-on-disclosures-for-securitisations-6%20March-2023.pdf

Insurers green investments

European Insurance and Occupational Pensions Authority

To meet the EU's climate targets and help speed up society's transition to a net-zero economy, investments in sustainable activities are needed. As long-term investors with an overall balance sheet of around €8 trillion, insurers in the European Economic Area (EEA) can play a significant role in putting our economies on a more sustainable track.

Based on the EU Taxonomy of sustainable activities and using the NACE classification framework, EIOPA analyzed how much of EEA insurers' investments can be considered environmentally sustainable at present.



To read more: https://www.eiopa.europa.eu/system/files/2023-02/Factsheet%20-%20Green%20investments%202023v5.pdf

Proposal for a regulation on Markets in Crypto-assets (MiCA)

This proposal seeks to provide legal certainty for crypto-assets not covered by existing EU financial services legislation and establish uniform rules for crypto-asset service providers and issuers at EU level. The proposed Regulation will replace existing national frameworks applicable to crypto-assets not covered by existing EU financial services legislation and also establish specific rules for so-called 'stablecoins', including when these are e-money. The proposed Regulation is divided into nine Titles.

Title I sets the subject matter, the scope and the definitions. Article 1 sets out that the Regulation applies to crypto-asset service providers and issuers, and establishes uniform requirements for transparency and disclosure in relation to issuance, operation, organisation and governance of crypto-asset service providers, as well as establishes consumer protection rules and measures to prevent market abuse.

Article 2 limits the scope of the Regulation to crypto-assets that do not qualify as financial instruments, deposits or structured deposits under EU financial services legislation.

Article 3 sets out the terms and definitions that are used for the purposes of this Regulation, including 'crypto-asset', 'issuer of crypto-assets', 'asset-referenced token' (often described as 'stablecoin'), 'e-money token' (often described as 'stablecoin'), 'crypto-asset service provider', 'utility token' and others.

Article 3 also defines the various crypto-asset services. Importantly, the Commission may adopt delegated acts to specify some technical elements of the definitions, to adjust them to market and technological developments.

Title II regulates the offerings and marketing to the public of crypto-assets other than asset-referenced tokens and e-money tokens.

It indicates that an issuer shall be entitled to offer such crypto-assets to the public in the Union or seek an admission to trading on a trading platform for such crypto-assets if it complies with the requirements of Article 4, such as the obligation to be established in the form of a legal person or the obligation to draw up a crypto-asset white paper in accordance with Article 5 (with Annex I) and the notification of such a crypto-asset white paper to the competent authorities (Article 7) and its publication (Article 8).

Once a whitepaper has been published, the issuer of crypto-assets can offer its crypto-assets in the EU or seeks an admission of such crypto-assets to trading on a trading platform (Article 10).

Article 4 also includes some exemptions from the publication of a whitepaper, including for small offerings of crypto-assets (below €1 million within a twelve-month period) and offerings targeting qualified investors as defined by the Prospectus Regulation (Regulation EU 2017/1129).

Article 5 and Annex I of the proposal set out the information requirements regarding the crypto-asset white paper accompanying an offer to the public of crypto-assets or an admission of crypto-assets to a trading platform for crypto-assets, while Article 6 imposes some requirements related to the marketing materials produced by the issuers of crypto-assets, other than asset-referenced tokens or e-money tokens.

The crypto-asset white paper will not be subject to a pre-approval process by the national competent authorities (Article 7). It will be notified to the national competent authorities with an assessment whether the crypto-asset at stake constitutes a financial instrument under the Markets in Financial Instruments Directive (Directive 2014/65/EU), in particular.

After the notification of the crypto-asset white paper, competent authorities will have the power to suspend or prohibit the offering, require the inclusion of additional information in the crypto-asset white paper or make public the fact that the issuer is not complying with the Regulation (Article 7).

Title II also includes specific provisions on the offers of crypto-assets that are limited in time (Article 9), the amendments of an initial crypto-asset white paper (Article 11), the right of withdrawal granted to acquirers of crypto-assets (Article 12), the obligations imposed on all issuers of crypto-assets (Article 13) and on the issuers' liability attached to the crypto-asset white paper (Article 14).

Title III, Chapter 1 describes the procedure for authorisation of asset-referenced token issuers and the approval of their crypto-asset white paper by national competent authorities (Articles 16 to 19 and Annexes I and II). To be authorised to operate in the Union, issuers of asset-referenced tokens shall be incorporated in the form of a legal entity established in the EU (Article 15).

Article 15 also indicates that no asset-referenced tokens can be offered to the public in the Union or admitted to trading on a trading platform for crypto-assets if the issuer is not authorised in the Union and it does not publish a crypto-asset white paper approved by its competent authority.

Article 15 also includes exemptions for small-scale asset-referenced tokens and for asset-referenced tokens that are marketed, distributed and exclusively held by qualified investors. Withdrawal of an authorisation is detailed in Article 20 and Article 21 sets out the procedure for modifying the crypto-asset white paper.

Title III, Chapter 2 sets out the obligations for issuers of asset-referenced tokens. It states they shall act honestly, fairly and professionally (Article 23). It lays down the rules for the publication of the crypto-asset white paper and potential marketing communications (Article 24) and the requirements for these communications (Article 25). Further, issuers are subject to ongoing information obligations (Article 26) and they are required to establish a complaint handling procedure (Article 27).

They shall also comply with other requirements, such as rules on conflicts of interest (Article 28), notification on changes to their management body to its competent authority (Article 29), governance arrangements (Article 30), own funds (Article 31), rules on the reserve of assets backing the asset-referenced tokens (Article 32) and requirements for the custody of the reserve assets (Article 33).

Article 34 explains that an issuer shall only invest the reserve assets in assets that are secure, low risk assets. Article 35 also imposes on issuers of asset-referenced tokens the disclosure of the rights attached to the asset-referenced tokens, including any direct claim on the issuer or on the reserve of assets.

Where the issuer of asset-referenced tokens does not offer direct redemption rights or claims on the issuer or on the reserve assets to all holders of asset-reference tokens, Article 35 provides holders of asset-referenced tokens with minimum rights. Article 36 prevents issuers of asset-referenced tokens and crypto-asset service providers from granting any interest to holders of asset-referenced tokens.

Title III, Chapter 4, sets out the rules for the acquisition of issuers of asset-referenced tokens, with Article 37 detailing the assessment of an intended acquisition, and Article 38 the content of such an assessment.

Title III, Chapter 5, Article 39 sets out the criteria that EBA shall use when determining whether an asset-referenced token is significant. These criteria are: the size of the customer base of the promoters of the asset-referenced tokens, the value of the asset-referenced tokens or their market capitalisation, the number and value of transactions, size of the reserve of assets, significance of the issuers' cross-border activities and the interconnectedness with the financial system.

Article 39 also includes an empowerment for the Commission to adopt a delegated act in order to specify further the circumstances under which and thresholds above which an issuer of asset-referenced tokens will be considered significant. Article 39 includes some minimum thresholds that the delegated act shall in any case respect.

Article 40 details the possibility for an issuer of an asset-referenced token to classify as significant at the time of applying for an authorisation on their own initiative. Article 41 lists the additional obligations applicable to issuers of significant asset-referenced tokens, such as additional own funds requirements, liquidity management policy and interoperability.

Tittle III, Chapter 6, Article 42 obliges the issuer to have a procedure in place for an orderly wind-down of their activities.

Title IV, Chapter 1 describes the procedure for authorisation as an issuer of e-money tokens. Article 43 describes that no e-money tokens shall be offered to the public in the Union or admitted to trading on a crypto-asset trading platform unless the issuer is authorised as a credit institution or as an 'electronic money institution' within the meaning of Article 2(1) of Directive 2009/110/EC. Article 43 also states that 'e-money tokens' are deemed electronic money for the purpose of Directive 2009/110/EC.

Article 44 describes how holders of e-money tokens shall be provided with a claim on the issuer: e-money tokens shall be issued at par value and on the receipt of funds, and upon request by the holder of e-money tokens, the issuers must redeem them at any moment and at par value. Article 45 prevents issuers of e-money tokens and crypto-asset service providers from granting any interest to holders of e-money tokens.

Article 46 and Annex III sets out the requirements for the crypto-asset white paper accompanying the issuance of e-money tokens, for example: description of the issuer, detailed description of the issuer's project, indication of whether it concerns an offering of e-money tokens to the public or admission of these to a trading platform, as well as information on the risks relating to the e-money issuer, the e-money tokens and the implementation of any potential project.

Article 47 includes provision on the liability attached to such crypto-asset white paper related to e-money tokens. Article 48 sets requirements for potential marketing communications produced in relation to an offer of e-money tokens and Article 49 states that any funds received by an issuer in exchange for e-money tokens, shall be invested in assets denominated in the same currency as the one referenced by the e-money token.

Title IV, Chapter 2, Article 50 states that the EBA shall classify e-money tokens as significant on the basis of the criteria listed in Article 39. Article 51 details the possibility of an issuer of an e-money token to classify as significant at the time of applying for an authorisation on their own initiative. Article 52 contains the additional obligations applicable to issuers of significant e-money tokens.

Issuers of significant e-money tokens must apply Article 33 on the custody of the reserve assets and Article 34 on the investment of these assets instead of Article 7 of Directive 2009/110/EC, Article 41, paragraphs 1, 2, and 3 on remuneration, interoperability and liquidity management, Article 41, paragraph 4 instead of Article 5 of Directive 2009/110/EC and Article 42 on an orderly wind-down of their activities.

To read more: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0593&from=EN

EBA publishes methodology and draft templates for the 2023 EU-wide stress test

The European Banking Authority (EBA) published the final methodology, draft templates and template guidance for the 2023 EU-wide stress test along with the milestone dates for the exercise.

The methodology and templates cover all relevant risk areas and have considered the feedback received from industry. The stress test exercise will be launched in January 2023 with the publication of the macroeconomic scenarios. The results will be published by the end of July 2023.

The 2023 EU-wide stress test uses a constrained bottom-up approach with some top-down elements. Balance sheets are assumed to be constant. Focus is on the assessment of the impact of adverse shocks on banks' solvency.

Banks are required to estimate the evolution of a common set of risks (credit, market, counterparty, and operational risk) under an adverse scenario. Banks are also asked to project the impact of the scenarios on main income sources.

For net fee and commission income, risk weights of securitisation, and the credit loss path of sovereign exposures, banks are required to make use of prescribed parameters. The methodology includes the sample of banks participating in the exercise.

The stress test templates along with a template guidance are published in their draft versions as they can still be subject to minor technical adjustments before their final publication.

Milestone for the 2023 EU-wide stress test

1. Launch of the exercise at the end of January 2023;
2. First submission of results to the EBA at the beginning of April 2023;
3. Second submission to the EBA in mid-May 2023;
4. Third submission to the EBA at the end of June 2023;
5. Final submission to the EBA in mid-July 2023;

6. Publication of results by end-July 2023.

ECB-PUBLIC

ESRB
European Systemic Risk Board
European System of Financial Supervision

Macro-financial scenario for the 2023 EU-wide banking sector stress test

To read more: https://www.eba.europa.eu/eba-publishes-methodology-and-draft-templates-2023-eu-wide-stress-test

FSB Chair's letter to G20 Finance Ministers and Central Bank Governors

This letter was submitted to G20 Finance Ministers and Central Bank Governors (FMCBG) ahead of the G20's meeting on 24-25 February.

FSB FINANCIAL STABILITY BOARD

THE CHAIR

20 February 2023

To G20 Finance Ministers and Central Bank Governors

The financial stability outlook remains challenging. While expectations of a 'soft landing' for the global economy have grown, the outlook remains clouded by uncertainty.

The combination of near record-high levels of debt, rising debt service costs and stretched asset valuations in some key markets can pose serious threats to financial stability.

The letter lays out the FSB's work during 2023 to monitor and address these conjunctural vulnerabilities, as well as a number of structural vulnerabilities.

The letter introduces the reports the FSB is delivering to the February G20 FMCBG meeting, which cover:

The financial stability aspects of commodity markets, which forms part of the FSB's work programme to strengthen the resilience of the NBFI sector.

The financial stability risks of decentralised finance (DeFi), a fast-growing segment of the crypto-asset ecosystem. The report forms part of the FSB's work programme, jointly with sectoral standard setters, for the delivery of a consistent and comprehensive regulatory framework for crypto-assets.

Priority actions for achieving the G20 targets for enhancing cross-border payments. The report contains a detailed set of next steps to achieve the G20 cross-border payments roadmap's goals and is being accompanied by

the establishment of two new taskforces to work in partnership with the private sector.

The letter also outlines forthcoming work to enhance cyber and operational resilience; and to address climate-related financial risks, through the FSB's climate roadmap.

Crypto-assets and decentralised finance

The events of the past year, such as the collapse of FTX, have highlighted the intrinsic volatility and structural vulnerabilities of crypto-assets.

We have now seen first-hand that the failure of a key intermediary in the crypto-asset ecosystem can quickly transmit risks to other parts of that ecosystem. And, if linkages to traditional finance grow, risks from crypto-asset markets could spill over onto the broader financial system.

The G20 has charged the FSB with coordinating the delivery of an effective and comprehensive regulatory framework for cryptoassets, for which we and the sectoral standard setters have jointly put forth an ambitious 2023 work programme.

This year, the FSB will finalise its recommendations for the regulation, supervision and oversight of crypto-assets and markets and its recommendations targeted at global stablecoin arrangements, which have characteristics that may make threats to financial stability more acute.

The recommendations for global stablecoin arrangements include guidance to strengthen governance frameworks, clarify and strengthen the redemption rights and the need to maintain effective stabilisation mechanisms, among other revisions.

Importantly, the FSB's work concludes that many existing stablecoins would not currently meet these high-level recommendations, nor would they meet the international standards and supplementary, more detailed BIS Committee on Payments and Market Infrastructures-International Organization of Securities Commissions guidance.

Collectively, these recommendations seek to promote the comprehensiveness and international consistency of regulatory and supervisory approaches, recognizing that many crypto-asset activities and markets are currently not compliant with applicable regulations or are unregulated. We are working with our members, including the sectoral standard-setting bodies, to complete this critical work.

Additionally, we will deliver a joint paper with the IMF later this year that synthesises the policy findings from IMF work on macroeconomic and monetary issues and FSB work on supervisory and regulatory issues associated with cryptoassets.

We will also explore how to address the cross-border risks specific to EMDEs. Publication of the FSB's recommendations will only be the beginning of the next phase of work in this area, as the standard-setting bodies will need to make their own, more detailed, recommendations, and member jurisdictions will need to implement the recommendations.

The FSB will continue to coordinate that work, as necessary, and going forward will monitor implementation of the recommendations together with the standard-setters.

Once the work is completed, the appropriate regulation of crypto-assets, based on the principle of 'same activity, same risk, same regulation' will provide the beginning of a strong basis for harnessing potential benefits associated with this form of financial innovation while containing its risks.

Within the crypto-asset ecosystem, so-called decentralised finance (DeFi) has emerged as a fast-growing segment, and we are delivering to this meeting a report on DeFi.

Our report points to the need for proactive monitoring, filling data gaps, and exploring to what extent the cryptoasset recommendations may need to be enhanced to cover DeFi risks.

We will build on this work to examine whether additional policy recommendations are needed to deal with this growing segment.

The FSB continues to conduct forward-looking analysis to assess the implications of cryptoassets for financial stability.

This year we are undertaking in-depth analysis of the large cryptoasset intermediaries that provide a wide range of services to the ecosystem.

We will also undertake analysis of the increasing trend toward the tokenisation of assets and how that could affect financial stability.

Enhancing cross-border payments

One factor that has helped spur the development of the crypto-asset ecosystem is dissatisfaction with the existing system of cross-border payments.

In 2020, G20 Leaders endorsed the Roadmap for Enhancing Cross-border Payments, in order to address the frictions that such payments currently face and thereby achieve faster, cheaper, more transparent and more inclusive cross-border payment services.

Last year we reported to the G20 that this work had reached the next phase, focused on implementation.

For this meeting, the FSB is delivering a report with detailed next steps under the new phase of the Roadmap, comprising high-priority, practical steps to achieve the Roadmap's goals.

This is being accompanied by the setting up of two new taskforces to work in partnership with the private sector as we take the work forward. Continued G20 support remains vital here.

To read more: https://www.fsb.org/wp-content/uploads/P200223-1.pdf

European Parliament resolution on the adequacy of the protection afforded by the EU-US Data Privacy Framework

European Parliament
2019-2024

Committee on Civil Liberties, Justice and Home Affairs

DRAFT MOTION FOR A RESOLUTION, to wind up the debate on the statement by the Commission pursuant to Rule 132(2) of the Rules of Procedure on the adequacy of the protection afforded by the EU-US Data Privacy Framework (2023/2501(RSP)) Juan Fernando López Aguilar, on behalf of the Committee on Civil Liberties, Justice and Home Affairs

The European Parliament,

– having regard to the Charter of Fundamental Rights of the European Union ('the Charter'), in particular Articles 7, 8, 16, 47 and 52 thereof,

– having regard to the judgment of the Court of Justice of 6 October 2015 in Case C-362/14 Maximillian Schrems v Data Protection Commissioner ('Schrems I'),

– having regard to the judgment of the Court of Justice of 16 July 2020 in Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ('Schrems II'),

– having regard to its enquiry into the revelations made by Edward Snowden on the electronic mass surveillance of EU citizens, including the findings in its resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs,

– having regard to its resolution of 26 May 2016 on transatlantic data flows,

– having regard to its resolution of 6 April 2017 on the adequacy of the protection afforded by the EU-US Privacy Shield,

– having regard to its resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield,

– having regard to its resolution of 20 May 2021 on the ruling of the CJEU of 16 July 2020 – Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ('Schrems II'), Case C-311/18,

– having regard to the Commission draft Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework,

– having regard to President of the United States' Executive Order 14086 of 7 October 2022 on Enhancing Safeguards For United States Signals Intelligence Activities,

– having regard to the Regulation on the Data Protection Review Court issued by the US Attorney General ('AG Regulation'),

– having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ('GDPR'), in particular Chapter V thereof,

– having regard to the Commission proposal of 10 January 2017 for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (COM(2017)0010), to the decision to enter into interinstitutional negotiations confirmed by Parliament's plenary on 25 October 2017, and to the Council's general approach adopted on 10 February 2021 (6087/21),

– having regard to the European Data Protection Board (EDPB) Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, and to the EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures,

– having regard to the EDPB Opinion of [to be added],

– having regard to Rule 132(2) of its Rules of Procedure,

A. whereas in the 'Schrems I' judgment, the Court of Justice of the European Union (CJEU) invalidated the Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, and pointed out that indiscriminate access by intelligence authorities to the content of electronic communications violates the essence of the fundamental right to confidentiality of communications provided for in Article 7 of the Charter;

B. whereas in the 'Schrems II' judgment, the CJEU invalidated Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield and concluded that it did not provide sufficient legal remedies against mass surveillance for non-US nationals and that this violates the essence of the fundamental right to a legal remedy as provided for in Article 47 of the Charter;

C. whereas on 7 October 2022, the President of the United States of America signed Executive Order 14086 on Enhancing Safeguards For United States Signals Intelligence Activities ('EO');

D. whereas on 13 December 2022 the Commission launched the process to adopt an adequacy decision for the EU-US Data Privacy Framework;

E. whereas, when examining the level of protection afforded by a third country, the Commission is obliged to assess the content of the rules applicable in that country deriving from its domestic law or its international commitments, as well as the practice designed to ensure compliance with those rules;

F. whereas the ability to transfer personal data across borders has the potential to be a key driver of innovation, productivity and economic competitiveness; whereas these transfers should be carried out in full respect for the right to the protection of personal data and the right to privacy; whereas one of the fundamental objectives of the EU is the protection of fundamental rights, as enshrined in the Charter;

G. whereas the GDPR applies to all companies processing the personal data of data subjects in the EU, where the processing activities are related to the offering of goods or services to such data subjects in the Union, or the monitoring of their behaviour as far as their behaviour takes place within the Union;

H. whereas mass surveillance, including the bulk collection of data, by state actors is detrimental to the trust of European citizens and businesses in digital services and, by extension, in the digital economy;
I. whereas controllers should always be accountable for compliance with data protection obligations, including demonstrating compliance for any data processing whatever its nature, scope, context, purposes and risks for data subjects;

J. whereas there is no federal privacy and data protection legislation in the United States (US); whereas the EU and the US have differing definitions

of key data protection concepts such as principles of necessity and proportionality;

1. Recalls that privacy and data protection are legally enforceable fundamental rights enshrined in the Treaties, the Charter and the European Convention of Human Rights, as well as in laws and case-law; emphasises that they must be applied in a manner that does not unnecessarily hamper trade or international relations, but can be balanced only against other fundamental rights and not against commercial or political interests;

2. Acknowledges the efforts made in the EO to lay down limits on US Signals Intelligence Activities, by referring to the principles of proportionality and necessity, and providing a list of legitimate objectives for such activities; points out, however, that these principles are long-standing key elements of the EU data protection regime and that their substantive definitions in the EO are not in line with their definition under EU law and their interpretation by the CJEU; points out, furthermore, that for the purposes of the EU-US Data Privacy Framework, these principles will be interpreted solely in the light of US law and legal traditions; points out that the EO requires that signals intelligence must be conducted in a manner proportionate to the 'validated intelligence priority', which appears to be a broad interpretation of proportionality;

3. Regrets the fact that the EO does not prohibit the bulk collection of data by signals intelligence, including the content of communications; notes that the list of legitimate national security objectives can be expanded by the US President, who can determine not to make the relevant updates public;

4. Points out that the EO does not apply to data accessed by public authorities via other means, for example through the US Cloud Act or the US Patriot Act, by commercial data purchases, or by voluntary data sharing agreements;

5. Points out that the decisions of the Data Protection Review Court ('DPRC') will be classified and not made public or available to the complainant; points out that the DPRC is part of the executive branch and not the judiciary; points out that a complainant will be represented by a 'special advocate' designated by the DPRC, for whom there is no requirement of independence; points out that the redress process provided by the EO is based on secrecy and does not set up an obligation to notify the complainant that their personal data has been processed, thereby undermining their right to access or rectify their data; notes that the proposed redress process does not provide for an avenue for appeal in a federal court and therefore, among other things, does not provide any

possibility for the complainant to claim damages; concludes that the DPRC does not meet the standards of independence and impartiality of Article 47 of the Charter;

6. Notes that, while the US has provided for a new mechanism for remedy for issues related to public authorities' access to data, the remedies available for commercial matters under the adequacy decision are insufficient; notes that these issues are largely left to the discretion of companies, which can select alternative remedy avenues such as dispute resolution mechanisms or the use of companies' privacy programmes;

7. Notes that European businesses need and deserve legal certainty; stresses that successive data transfer mechanisms, which were subsequently repealed by the CJEU, created additional costs for European businesses; notes that continuing uncertainty and the need to adapt to new legal solutions is particularly burdensome for micro, small and medium-sized enterprises;

8. Points out that, unlike all other third countries that have received an adequacy decision under the GDPR, the US still does not have a federal data protection law; points out that the EO is not clear, precise or foreseeable in its application, as it can be amended at any time by the US President; is therefore concerned about the absence of a sunset clause which could provide that the decision would automatically expire four years after its entry into force;

9. Emphasises that adequacy decisions must include clear and strict mechanisms for monitoring and review in order to ensure that decisions are future proof and that EU citizens' fundamental right to data protection is guaranteed;

Conclusions

10. Recalls that, in its resolution of 20 May 2021, Parliament called on the Commission not to adopt any new adequacy decision in relation to the US, unless meaningful reforms were introduced, in particular for national security and intelligence purposes;

11. Concludes that the EU-US Data Privacy Framework fails to create actual equivalence in the level of protection; calls on the Commission to continue negotiations with its US counterparts with the aim of creating a mechanism that would ensure such equivalence and which would provide the adequate level of protection required by Union data protection law and the Charter as interpreted by the CJEU; urges the Commission not to adopt the adequacy finding;

12. Instructs its President to forward this resolution to the Council, the Commission and the President and Congress of the United States of America.

Advancing macroprudential tools for cyber resilience

ESRB
European Systemic Risk Board
European System of Financial Supervision

The ESRB worked in 2022 within the context of a substantially heightened cyber threat environment across Europe.

The cyber activity resulting from Russia's invasion of Ukraine have affected both Ukraine and EU Member States directly and indirectly.

Furthermore, an increase in cyber attacks and the active sabotage of power and telecommunications infrastructure in EU Member States – which the financial sector relies on – present significant threats to financial stability.

The ESRB responded to this heightened cyber threat environment by:

1. Enhancing the exchange of information across jurisdictions and authorities.

2. Focusing on the tools and elements needed to advance cyber resilience and strengthen preparedness for potential cyber incidents.

3. Advancing a cyber resilience scenario testing (CyRST) approach: the ESRB completed further work on this approach, which could support authorities in:

(i) testing the response and recovery capacity of the financial system against severe but plausible scenarios involving a cyber incident,

(ii) evaluating their impact on financial and operational stability, and

(iii) identifying areas where further work is required to mitigate cyber risks.

4. Developing the concept for a systemic impact tolerance objective (SITO): the ESRB worked on developing SITOs, which can assist in identifying and measuring the impacts of cyber incidents on the financial system, and evaluating when they are likely to breach tolerance levels and cause significant disruption.

5. Reviewing current financial crisis management tools: the ESRB evaluated whether these tools are sufficient for adequately responding to system-wide cyber incidents.

The heightened cyber threat environment across Europe calls for a step change in enhancing system-wide cyber resilience.

The resistance and detection capabilities of individual entities constitute a first layer of defence against cyber incidents.

The Digital Operational Resilience Act (DORA) is part of an ongoing effort at the EU level to improve the cyber resilience of individual entities.

Threat-led penetration tests outlined by DORA, such as the European Framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU), provide a way of testing this first layer of defence.

However, further layers of defence are needed to increase the resilience of the financial system as a whole against cyber incidents.

Against this background, the ESRB has three key areas of focus.

1. The ESRB encourages authorities to use the CyRST approach to pilot system-wide cyber resilience scenario testing as soon as possible.

Such pilots can complement other analytical tools that the authorities might be using and deepen their understanding of CyRST and of the risks to system-wide cyber resilience.

This is important and urgent, given the increased likelihood that a cyber attack will strike the European financial sector and because it will take time to pilot CyRST, identify the risks and implement appropriate mitigating measures.

The ESRB will continue to work in this area as a hub for sharing progress and good practice, and will update the conceptual approach based on what the authorities learn from their more detailed work in the pilots.

2. The ESRB advocates the use of SITOs and will continue to transition from a conceptual approach to a practical basis for implementing them.

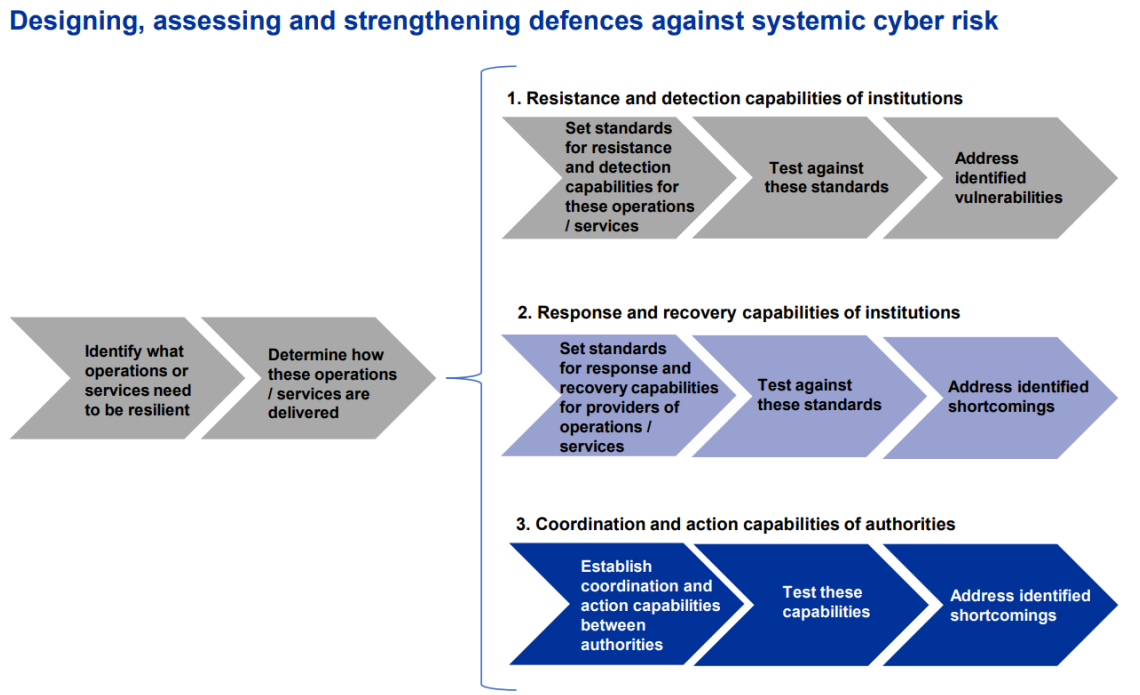
Specifically, the ESRB will identify a key economic function3 where disruptions have cross-border implications and define appropriate SITOs at EU level so as to ensure consistency across the region/sector and authorities.

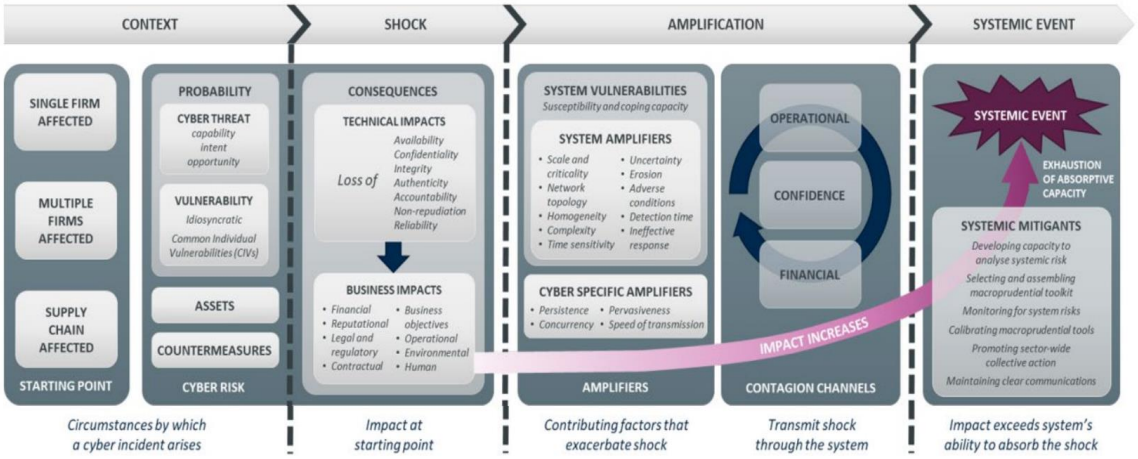
The ESRB will work with authorities across the EU to identify where a consistent approach is required and to decide on the approach for setting SITOs where there are crossborder implications.

The ESRB recognises that where disruptions have no or few cross-border implications, SITOs may differ across jurisdictions to reflect national specificities.

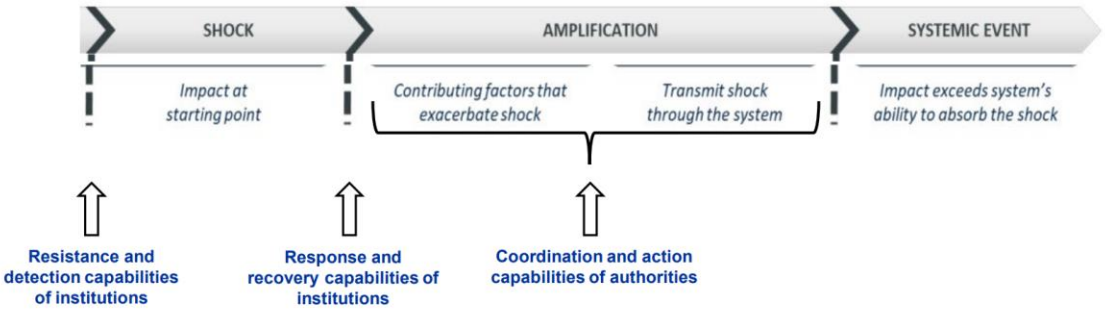
3. The ESRB will consider which operational policy tools are most effective in responding to a system-wide cyber incident and identify gaps across operational and financial policy tools.

This work will build on the analysis of financial crisis management tools described in this report.

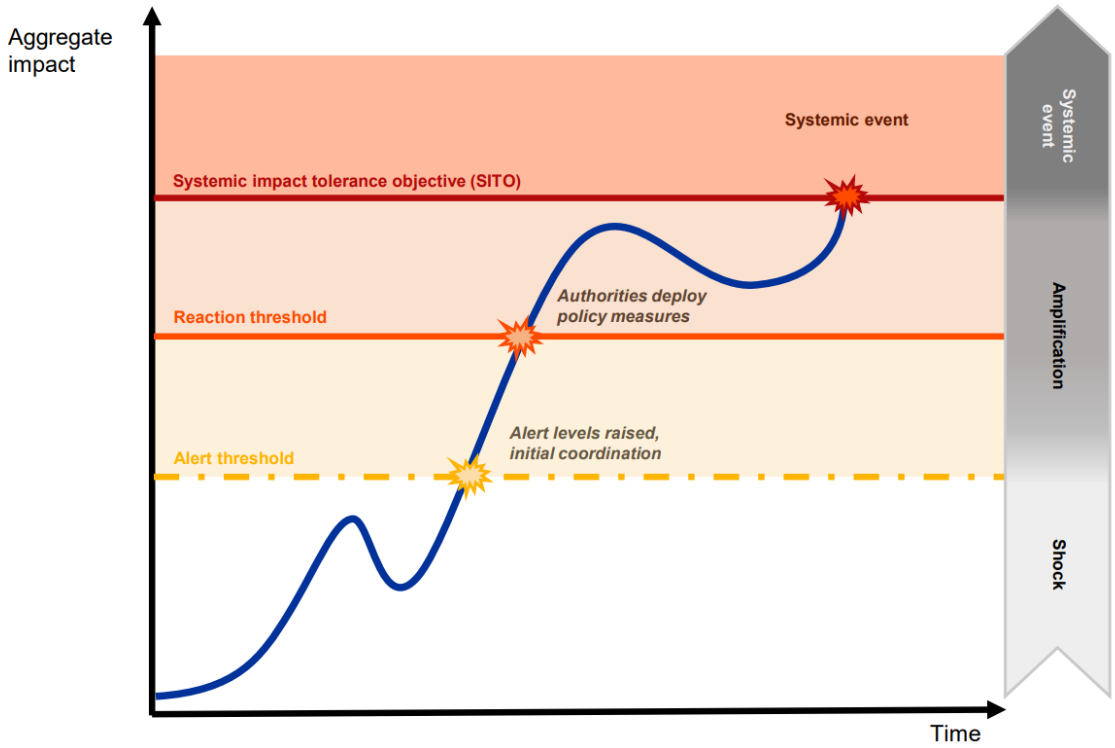




Stylised representation of the layers of defence



Cyber incident impact and tolerance for different impact levels



To read more:
https://www.esrb.europa.eu/pub/pdf/reports/esrb.macroprudentialtoolscyberresilience220214~984a5ab3a7.en.pdf?888a06fcb36d2c1ce41594efd67a4c88

The quick and the dead - building up cyber resilience in the financial sector

Fabio Panetta, Member of the Executive Board of the European Central Bank, at the meeting of the Euro Cyber Resilience Board for pan-European Financial Infrastructures, Frankfurt am Main.

The proliferation of cyber threat actors combined with an increase in remote working and greater digital interconnectedness is raising the risk, frequency and severity of cyberattacks.

Increasingly, cyber criminals are launching ransomware attacks and demanding payment in crypto. Cyberattacks related to geopolitical developments – Russia's aggression against Ukraine in particular – have also become a more common feature of the cyber-threat landscape.

The Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB) has played a key role in protecting the security and integrity of the financial system from these threats.

You may visit: https://www.ecb.europa.eu/paym/groups/euro-cyber-board/shared/pdf/ECRB_mandate.pdf

EUROPEAN CENTRAL BANK
EUROSYSTEM

ECB-PUBLIC
26 January 2018

Mandate of the Euro Cyber Resilience Board for pan-European Financial Infrastructures

The last three years have shown that we can work under adverse conditions towards a common goal. Our financial infrastructures have proven their resilience to cyber threats. But this does not mean we can become complacent or any less vigilant in the face of cyber threats. We simply cannot afford to fall behind the curve: cybersecurity must be the backbone of digital finance.

Today I will take stock of the ECRB's work. I will then discuss current cyber threats and emerging risks before outlining the implications for our work in the future.

The contribution of the Euro Cyber Resilience Board

The ECRB brings together private and public stakeholders across pan-European financial infrastructures, critical service providers, central banks and other authorities.

This offers a unique prism through which the ECRB can identify and fix any weaknesses which cyberattacks could potentially exploit in order to propagate, which in turn would cause systemic ripples throughout the European financial ecosystem.

Let me give three examples of why the ECRB is such a useful forum for cooperation.

First, in the area of information sharing, the ECRB's Cyber Information and Intelligence Sharing Initiative (CIISI-EU) allows members to exchange information about cyber threats and mitigation in a secure and trusted group environment.

Second, the ECRB has established a crisis coordination protocol that facilitates cooperation and coordination, allowing members to exchange and respond to major cyber threats and incidents.

Third, in the area of training and awareness, the ECRB conducts joint assessments and training sessions to increase common knowledge and understanding.

A key pillar of the ECB's cyber strategy for financial infrastructures is the TIBER-EU framework for threat-led penetration testing, also known as red teaming. In June 2022 the ECRB organised a dedicated roundtable on TIBER-EU where members shared their experience of these kinds of exercises.

In view of their systemic role in the financial system, we will continue to focus on pan-European financial infrastructures. Nonetheless, financial infrastructures are increasingly interdependent through horizontal and vertical links and common participants.

They are also reliant on information and communication technology and on third-party service providers. As a result, these infrastructures are exposed to common risks and vulnerabilities through which cyberattacks could propagate swiftly if they are not rigorously managed. The ECRB allows us to join forces to address these risks on a sector-wide level.

Adapting to a constantly changing cyber threat landscape

Let me now turn to the cyber threat landscape.

Threats are becoming increasingly complex. Recent attacks call for constant vigilance at an operational level, and the continuous reassessment of regulatory and oversight frameworks to see whether they need to be updated. Significant but unpredictable shifts can occur at any time. We must therefore be prepared to understand them and to adapt quickly in order to mitigate the financial ecosystem's susceptibility to cyberattacks.

The ECRB has identified supply chain attacks and ransomware as key threats in the current environment, and artificial intelligence (AI) as an emerging threat. We have also witnessed how geopolitical developments, most recently Russia's aggression against Ukraine, have weaponised cyberspace. The most prominent examples are distributed denial-of-service (DDoS) attacks against government and financial entities.

Let me discuss the key current and emerging threats in more detail.

Supply chain attacks

The financial ecosystem's reliance on third-party products and services is a key risk, especially when financial entities outsource critical functions to them. An attack on these third parties or on their products and services can disrupt and harm the financial infrastructures that rely on them, with spillovers to interconnected entities.

When such third-party products and services are widely used in the financial ecosystem, a cyberattack can have widespread, possibly systemic effects by having an impact on multiple financial entities at once. That is why cyber threat actors target these third parties. In so doing, they can compromise numerous financial entities simultaneously.

The recent cyberattack on the third-party provider ION Cleared Derivatives shows how an attack on one software provider may cascade onto their clients. In this specific case, the disruptions to the trading and clearing of financial derivatives remained limited, but we cannot ignore scenarios where the attacks could have propagated quickly, disrupting the financial system.

This case signalled the need for financial entities to review their third-party providers, the providers of these third-parties, their cyber resilience levels and the systemic impact that may ensue from a cyberattack on any of these providers.

In particular, it is vital to assess critical service dependencies on third-party products and services which could be disrupted or even terminated as a result of a cyberattack. Mitigating measures need to be put in place.

Against this background, the G7 recently updated its Fundamental Elements for Third-Party Cyber Risk Management in the Financial Sector. In addition, the ECRB set up a working group in 2022 to support third-party cyber risk management.

We must have a cyber resilience mindset at all times. The question we must ask is not if a cyberattack will happen, but whether we are ready to respond when it happens.

Over the past year, the ECRB has worked on a conceptual model for how the financial infrastructure ecosystem could manage such a crisis if it occurred. It has also developed protocols and networks aimed at supporting a collective, consistent and comprehensive response to a cyber crisis by stakeholders.

Ransomware

The proliferation of ransomware is one of the most significant challenges currently facing financial entities. Not only may ransomware attacks result in financial loss, they may also severely disrupt operations.

Even after a ransom is paid, there is no guarantee the decryption key will actually work or that the stolen data will not be publicly disclosed or further misused to extort victims' customers, for example.

Ransomware attacks are growing more sophisticated and damaging, which in turn may enable ransomware threat actors to obtain even more resources. 2022 was one of the most active years for ransomware activity.

However, it was also the first year that the majority of victims of ransomware attacks decided not to pay up, which indicates that the approach towards ransomware attacks is changing.

Authorities globally are stepping up their efforts to counter ransomware. For instance, the G7 issued Fundamental Principles on Ransomware Resilience in October 2022.

We need to tackle ransomware attacks from various angles.

First, every firm must be ready to repel ransomware attacks, either through the use of proper cyber hygiene practices or by ensuring that data is backed up regularly and is kept up-to-date and tamper-proof.

Second, enforcement agencies need to conduct forensic analyses, locate attackers and join forces to prosecute them.

Third, crypto-assets – especially unbacked crypto-assets, which are used to make ransomware payments owing to the anonymity and money laundering possibilities they offer – need to be strictly regulated. Similarly, crypto-asset transfers must be traceable.

The proposed EU Regulation for Markets in Crypto-Assets (MiCA) and revision to the Regulation on information accompanying transfers of funds, which extends the "travel rule" to crypto-assets, are important steps. However, to be effective and prevent regulatory arbitrage, regulation must be stepped up globally.

Implementation of the Financial Action Task Force (FATF) guidance for crypto-assets and its enforcement at international level are therefore crucial.

In addition, all firms need to have the highest level of cyber controls in place to prevent attacks from being successful and to detect and recover from ransomware attacks.

Moreover, insurance firms can lend their support by obtaining assurances from their clients that they have high-level cyber resilience plans in place before providing cyber risk insurance policies, thus ensuring that these very same policies do not lower firms' incentives to prepare for cyberattacks.

Artificial Intelligence (AI)

Even if we do not realise it, the use of artificial intelligence (AI) is already widespread. We use AI every day, including on our phones, in our homes and at the workplace. And firms use it to harness big data.

AI can help to strengthen cybersecurity, for instance, by improving the detection of highly sophisticated cyberattacks through its ability to identify abnormal system behaviour compared with an established baseline. This is the kind of potential that we need to leverage.

But AI can also multiply cyber risks by, for instance, helping malicious individuals, even those who have limited or no technical skills, draft very convincing phishing emails or identify topics that will achieve the maximum engagement from those being targeted.

To make matters worse, AI can even create and fix code that can be used to exploit and compromise the endpoint.

This opens up new possibilities for malicious individuals to use AI to launch cyberattacks. Although AI development firms try to install safeguards to prevent its unethical use, they can be circumvented.

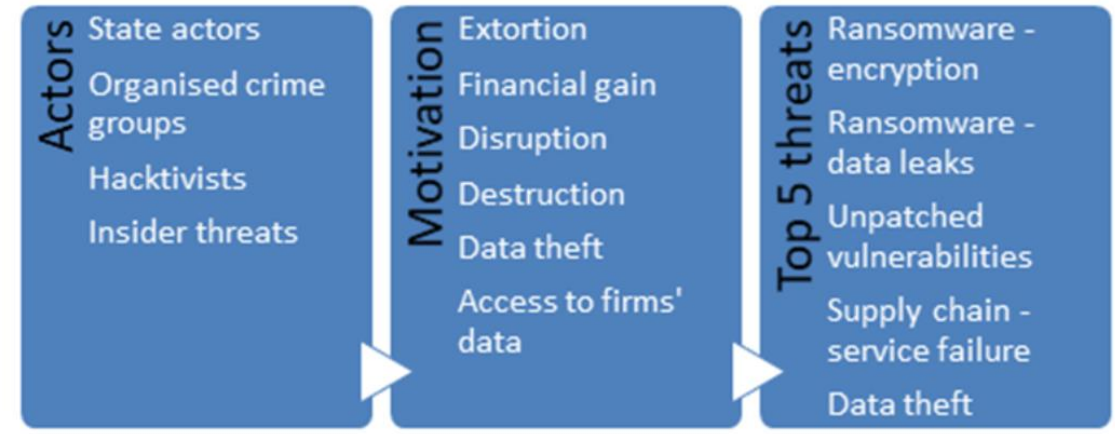
The risks from AI need to be clearly understood and addressed through regulation and oversight.

By exchanging information among its members and organising roundtables and training, the ECRB is in a strong position to raise awareness of risks at an early stage and accumulate knowledge of these types of threats.

For its part, the European Commission has proposed a Regulation on artificial intelligence that aims to address some of the key risks associated with AI.

Chart 1

Cyber threat landscape for financial market infrastructures in Europe



Note: Threats are arranged in descending order of estimated severity.

To read more:
https://www.ecb.europa.eu/press/key/date/2023/html/ecb.sp230308~92211cd1f5.en.html

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.