enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY


# EU CYBERSECURITY INITIATIVES IN THE FINANCE SECTOR

MARCH 2021

# ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

## CONTACT

For contacting the authors please use resilience@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

## AUTHORS

Rossen Naydenov, Marianthi Theocharidou – European Union Agency for Cybersecurity

## LEGAL NOTICE



## COPYRIGHT NOTICE



ISBN: 978-92-9204-497-8 – DOI: 10.2824/15644

# TABLE OF CONTENTS

# 1. INTRODUCTION

The finance sector is a heavily regulated sector, and cybersecurity provisions are already included in multiple EU policies and legislations (e.g. PSD 2[1], MIFID II[2]). EU institutions, agencies, bodies, regulators and other groups of stakeholders run several initiatives dedicated to improving the cybersecurity of financial entities. This brief document outlines such European cybersecurity initiatives in the sector and it is a first depiction of the complex landscape of initiatives related to cybersecurity at an EU level.

## 1.1 SCOPE, TARGET AUDIENCE AND OBJECTIVES

In this document, we have included initiatives of European scope, i.e. ones that are implemented in at least two EU Member states. This document focusses on financial entities, EU institutions, bodies and agencies of the Finance sector, as well as the finance community at large. The document was created in an effort to shed light on the initiatives and to guide interested parties in engaging with them and benefit from their produced results. Furthermore, it aims to make cooperation between the initiatives and their different groups work more seamless. The document may facilitate future assessments on the complementarity, overlaps and gaps of the respective initiatives and identify synergies.

ENISA's references in different sections reflect what ENISA is already doing in that particular area, as well as the mandate that the Agency has received through the Cybersecurity Act.

## 1.2 METHODOLOGY

The initiatives were collected during 2020 based on various sources, namely:

1. Desktop research conducted by ENISA,
2. Information gathered via a survey conducted in 2020 targeted to financial stakeholders,
3. Feedback during the validation of this report by relevant entities such as the European Commission (EC), European Banking Authority (EBA), European Central Bank (ECB), and ENISA's Expert Group on Finance (EGFI), as well as the other entities who contributed to the survey.

The selected topics are organised on the articles of the cybersecurity act[3] and are the following:

- Policy development and implementation (article 5)
- Information sharing and capacity building (articles 6, 9)
- Cyber crisis management and operational cooperation (article 7, 12)
- Awareness raising (article 10)
- Standardization and certification (article 8)
- Research and Innovation (article 11)

The list of initiatives included is not exhaustive and will be updated further as more initiatives develop or come to the attention of ENISA. This is a living document and will be updated regularly by ENISA to reflect the developments in the sector and to allow for changes or updates on current or new initiatives. Should the reader wishes to bring to the attention of ENISA other EU initiatives in the Finance sector, please contact resilience@enisa.europa.eu.

[1] DIRECTIVE (EU) 2015/2366 on payment services in the internal market https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366
[2] DIRECTIVE 2014/65/EU on markets in financial instruments https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0065
[3] REGULATION (EU) 2019/881 Cybersecurity Act https://eur-lex.europa.eu/eli/reg/2019/881/oj

# 2. EU CYBER INITIATIVES IN THE FINANCE SECTOR

## 2.1 DEVELOPMENT AND IMPLEMENTATION OF POLICY

The European Commission plays an active role in developing the EU's overall strategy and in designing and implementing EU policies for the financial sector. It evaluates and reports on these policies on a regular basis. These initiatives fall under the responsibility of **the European Commission**.

The European Commission issued the **Fintech action plan**[4] in 2018, which purpose is to achieve stronger cyber resilience. It does this by:

- Facilitating information sharing on cyber threats among market participants;
- Promoting higher supervisory convergence and enforcement of IT risk management;
- Increasing EU coordination in cyber threat testing using a common threat-intelligence lead method, such as TIBER-EU.

In 2020, the **digital finance strategy**[5] sets out general lines on how Europe can support the digital transformation of finance in the coming years, while regulating its risks. The strategy sets out four main priorities:

- removing fragmentation in the Digital Single Market,
- adapting the EU regulatory framework to facilitate digital innovation,
- promoting data-driven finance,
- addressing the challenges and risks with digital transformation, including enhancing the digital operational resilience of the financial system.

The EC recently published its legislative **proposal on Digital Operational Resilience Act ('DORA')**[6]. The ever-increasing dependency of the financial sector on software and digital processes means that information communication technologies (ICT) risks are inherent in finance.

The Commission, therefore, proposes that all financial entities ensure they can withstand all types of ICT-related disruptions and threats. Credit institutions, payment and e-money institutions, insurance companies and other financial entities will have to respect strict standards to prevent and limit the impact of ICT-related incidents. The EC also sets an oversight framework on service providers (such as Big Techs) which provide critical ICT services to financial entities.

The main task of the **European Banking Authority** (EBA)[7] is to contribute to the creation of the **European Single Rulebook**[8], aiming at providing a single set of harmonised prudential rules for financial institutions throughout the EU. On ICT/cyber-related topics, the EBA has produced a number of regulatory documents including guidelines, recommendations, opinions and other

**POLICY DEVELOPMENT AND IMPLEMENTATION**

Drafting, revising and issuing or advising in the drafting of policies and legislations

Monitor, audit, assess and monitor the implementation of policies and legislations related to or including cybersecurity provisions

[4] COM/2018/0109, FinTech Action plan https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0109
[5] COM(2020) 591, Digital Finance Strategy for the EU https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0591
[6] Financial services – improving resilience against cyberattacks (new rules) https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act
[7] EBA Mission and Tasks https://eba.europa.eu/about-us/missions-and-tasks
[8] EBA Single Rulebook https://www.eba.europa.eu/regulation-and-policy/single-rulebook

non-regulatory public statements. The EBA develops **technical standards, guidelines, opinions and other legal instruments** aimed at enhancing the cyber resilience of credit institutions, payment institutions, investment firms, and electronic money institutions.

The **EBA** has established two relevant structures, which are working on cyber-related matters. The first is the **Sub-Committee on Payment Services**, which is working on PSD2 related aspects and involves experts from the competent authorities. The second structure is the **Task Force on IT Supervision** (TFIT). TFIT involves ICT experts from Member States who are assisting in areas related to convergence of supervisory practices for supervision of IT and IT related risks. Additionally, it helps in developing a consistent and effective framework for the assessment of IT risks and other prudential risks, which may arise from the use of innovative technologies (FinTech) in supervised institutions

The EBA **Guidelines on ICT and security risk management**[9] establish requirements for credit institutions, investment firms, payment institutions and electronic money institutions in the EU/EEA on the mitigation and management of their information and communication technology (ICT) risks and aim to ensure a consistent and robust approach across the Single Market. In November 2019, the EBA published Guidelines on ICT and security risk management (EBA/GL/2019/04), which require management and mitigation of ICT and security risks through the establishment of sound internal governance and the use of an internal control framework setting clear responsibilities for financial institutions' staff, including for the management bodies.

The **EU Delegated Regulation on strong customer authentication**[10] is based on the EBA's Regulatory Technical Standards on strong customer authentication and secure communication and is applicable to credit institutions, payment institutions, and electronic money institutions. The requirements cover a range of security measures, which aim at enhancing customer protection, increase the security of electronic payments and decreasing the risk of fraud. The requirements also cover standards for secure communication between third party providers and account servicing payment service providers established in the EU/EEA in the process of provision of payment initiation services or account information services. The Regulation was developed by the EBA in close cooperation with the ECB.

The **EBA Guidelines on incident reporting under PSD2**[11] set out the criteria, thresholds and methodology to be used by credit institutions, payment institutions, and electronic money institutions in the EU/EEA. The guidelines determine whether an operational or security incident related to the provision of payment services, should be considered major and, therefore, be notified to the competent authority in the home Member State. The guidelines were developed by the EBA in close cooperation with the ECB.

**EBA Guidelines on the reporting of retail payment fraud under PSD2**[12]. The Guidelines aimed at contributing to the objective of PSD2 of enhancing the security of retail payments in the EU by requiring credit institutions, payment institutions and electronic money institutions to collect and report data on payment transactions and fraudulent payment transactions.

The **European Insurance and Occupational Pensions Authority** (EIOPA) [13] undertakes initiatives to make regulation for both insurance and pensions sectors. EIOPA focuses on the impact of new technology enabled business models and the use of new technologies for

[9] EBA/GL/2019/04, https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management
[10] OJ L 69, 13.3.2018, RTS on strong customer authentication and common and secure open standards of communication https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R0389.
[11] For further info, see: https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2
[12] For further info, see: https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-fraud-reporting-under-psd2
[13] EIOPA https://www.eiopa.europa.eu/

supervisory purposes. The Agency also contributes to the establishment of a common European approach towards technological innovation and promotes the exchange of information on cybersecurity and cyber-attacks.

EIOPA recently published a **strategy on cyber underwriting**[14]. It takes into account the acceptance of cyber risks and the following possibilities:

- The losses that might come out of cyber-attacks;
- The responses and recovery from a cyber-attack;
- Sharing good practices in cyber risk management;
- Encourage investment in risk reduction premiums.

The importance of outsourcing functions to cloud service providers has increased rapidly in many industries, especially in the finance sector. In fact, the EBA, EIOPA and ESMA have all issued **outsourcing guidelines**.

The **EBA** has issued a **report on outsourcing arrangements[15],** which have integrated the EBA recommendations on outsourcing to cloud service providers (December 2017). The recommendations aimed at overcoming the high level of uncertainty regarding supervisory expectations on outsourcing to cloud service providers and at removing the barriers that this uncertainty caused for institutions proceeding with using cloud services. The recommendations have been now integrated in the EBA Guidelines on outsourcing arrangements.

**EIOPA** has also issued **outsourcing guidelines**[16]. These guidelines apply to the different Cloud services being offered. The purpose of these guidelines is provide clarification and transparency to market participants avoiding potential regulatory arbitrages. Additionally, they aim to foster supervisory convergence regarding the expectations and processes applicable in relation to cloud outsourcing.

Similarly, **ESMA** has **published outsourcing guidelines**[17], which are addressing specifically Cloud providers. These guidelines refer to the risks assessment that should be performed by the entities when engaging with Cloud service providers. In addition, requirements are included in relation to how the governance, organisational and control structure should look like, as well as the possible exit clauses. Additionally, the contractual obligations are defined in the notification mechanism for getting into a contractual agreement with Cloud service providers. The competent authorities in their supervision of cloud outsourcing arrangements could also use the guidelines.

The **Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB)[18]** is a forum for strategic discussions between financial market infrastructures. Its objectives are to:

- Raise awareness of the topic of cyber resilience;
- Catalyse joint initiatives to develop effective solutions for the market;
- Provide a place to share best practices and foster trust and collaboration.

The ECRB is composed of representatives of pan-European financial market infrastructures and of their critical service providers. Additionally, several national central banks, as well ECB are

[14] Cyber underwriting strategy https://www.eiopa.europa.eu/content/cyber-underwriting-strategy_en
[15] EBA Guidelines on outsourcing arrangements, EBA/GL/2019/02, 25 February 2019 https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf?retry=1
[16] Guidelines on outsourcing to cloud service providers, EIOPA-BoS-20-002, https://www.eiopa.europa.eu/content/guidelines-outsourcing-cloud-service-providers_en
[17] Guidelines on outsourcing to cloud service providers (CSPs), ESMA50-157-2403, https://www.esma.europa.eu/press-news/esma-news/esma-publishes-cloud-outsourcing-guidelines
[18] Euro Cyber Resilience Board for pan-European Financial Infrastructures https://www.ecb.europa.eu/paym/groups/euro-cyber-board/html/index.en.html

active participants, without taking a position for final decisions. Furthermore, the EC, ENISA, EBA, Single Supervisory Mechanism (SSM), ESMA, and Europol are participating as observers.

**ENISA** supports policy development and implementation by carrying out a regularly updated stocktaking of ongoing and future EU policy initiatives with cybersecurity implications and make this information available to the European Commission and national cybersecurity competent authorities. It focuses in particular on policies related to the sectorial dimension of the NIS Directive, which includes the Finance sector, and on policies dedicated to cybersecurity (e.g. DSM, security certification, crisis cooperation, education and training, information hub). ENISA offers cybersecurity expert advice to the European Commission and other relevant EU institutions on policy developments.

ENISA also supports the cooperation between national competent authorities in order to work together towards the implementation of already agreed EU policies (legislation). It thus allows the sharing of national views and experience, and helps build upon those to draw and agree on recommendations. ENISA focuses on the NISD (in particular on requirements for operators of essential services e.g. identification, security requirements, incident reporting) and on the eIDAS Regulation as well as on NIS aspects of the General Data Protection Regulation (GDPR) (and more generally data protection) and the draft ePrivacy Regulation. Additionally, ENISA participates in the working groups of **Forum on the Security of Retail Payments** (SecuRe Pay)[19], by providing advice and recommendations for harmonization of the policy implementation.

## 2.2 INFORMATION SHARING AND CAPACITY BUILDING

**TIBER-EU**[20] is the European framework for threat intelligence-based ethical red teaming. It is the first EU-wide guide on how authorities, financial entities, threat intelligence and red-team providers should work together to test and improve the cyber resilience of entities by carrying out a controlled cyberattack. The TIBER-EU foresees the possibility for cooperation not only among different regulators from different sectors, but also among regulators from different countries. This is one of the first initiatives to foresee such capability.

The **ECRB** launched the **Cyber Information and Intelligence Sharing Initiative (CIISI-EU)**[21] on 27 February 2020. CIISI-EU brings together a community of public and private entities with the aim of sharing intelligence and exchanging best practices. The core objectives of CIISI-EU are to:

- Protect the financial system by preventing, detecting and responding to cyberattacks;
- Facilitate the sharing of information, intelligence and best practices between financial infrastructures; and
- Raise awareness of cybersecurity threats.

The CIISI-EU community is a market-driven initiative. It consists of pan-European financial infrastructures, central banks (in their operational capacity), critical service providers, ENISA and EUROPOL, as represented in the ECRB. Authorities in their capacity as regulators, overseers and/or supervisors are not part of the CIISI-EU Community. Regulatory reporting on cyber incidents and data breaches are outside the scope of information and intelligence sharing within the CIISI-EU Community[22].

**INFORMATION SHARING AND CAPACITY BUILDING**

Exchange of information regarding threats, vulnerabilities, incidents, trends, good practices.

Between competent authorities/CSIRTs, law enforcement and defence.

[19] Forum on the Security of Retail Payments – SecuRe Pay https://www.ecb.europa.eu/paym/pol/forum/html/index.en.html
[20] TIBER-EU framework https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html
[21] Major European financial infrastructures join forces against cyber threats https://www.ecb.europa.eu/press/pr/date/2020/html/ecb.pr200227_1~062992656b.en.html
[22] More information on the initiative is available at: https://www.ecb.europa.eu/paym/groups/euro-cyber-board/shared/pdf/ciisi-eu_practical_example.pdf

The **G7**[23] set up a **Cyber Expert Group** (CEG), a group of cybersecurity experts that meets regularly to facilitate progress on major international debates and that reports to G7 ministers and governors. This group is chaired by the United Kingdom and the United States. The objectives of the CEG are to identify the main cybersecurity risks in the financial sector and to propose actions to be taken in this area.

The CEG also works on other topics such as the identification of vulnerabilities, penetration testing, the risks of contagion resulting from relations with third parties, and cooperation between the public and private sectors.

The **Association for Financial Markets in Europe** (AFME)[24] is actively engaged in coordinating the effort to support a safe, secure, resilient information infrastructure within the financial sector, which provides security and privacy of customer information and efficient, reliable execution of transactions. AFME continually works with industry and government leaders to identify and communicate cybersecurity best practices and capabilities to educate the industry on evolving threats and appropriate responses. Cybersecurity being cross-border in nature, AFME is pro-actively engaged through the GFMA (Global Financial Markets Association[25]), with sister trade organisations (SIFMA[26] and ASIFMA[27]) on cybersecurity related issues.

On November 7 2019, SIFMA held a global cyber exercise **'Quantum Dawn V' (QDV)**[28]. QDV brought together key participants from the global financial community, attracting public and private sector institutions from many jurisdictions and professionals representing a broad range of roles and responsibilities. The exercise helped identify the roles and responsibilities of key participants in managing global crises with cross-border impacts. The exercise scenario emphasized cross-jurisdiction communication and coordination between member firms and regulatory agencies in North America, Europe, and Asia.

The **Pan European Insurance Forum** (PEIF) [29] is involved in the promotion of greater transparency of cyber-related incidents to make a solid base of data available to the cyber insurance underwriting community. Greater transparency is intended both in quantitative terms (i.e., increasing the amount of information currently produced and exchanged within the European market, and giving access to these information to a wider group of economic agents) and in qualitative terms (i.e., the development of a common language and a standard set of data points to be collected and shared).

Additionally, the following structures also contribute to information sharing and cooperation:

- The European Savings and Retail Banking Group[30] (ESBG) is involved in monitoring policy development, organising exchanges with policymakers and sharing best practices.
- The European Payments Council (EPC)[31], through its Payment Scheme Fraud Prevention Working Group (PSFPWG) focuses on fraud data collection and analysis, information sharing and prevention measures.
- The European Association for Secure Transactions[32] (EAST) uses its membership platforms to provide country and European updates on payments and terminal fraud (fraud types, fraud origins and due diligence), for the gathering, collation and

[23] Role of the G7 https://ec.europa.eu/info/food-farming-fisheries/farming/international-cooperation/international-organisations/g7_en
[24] https://www.afme.eu/
[25] https://www.gfma.org/
[26] https://www.sifma.org/
[27] https://www.asifma.org/
[28] https://www.sifma.org/resources/general/cybersecurity-exercise-quantum-dawn-v/
[29] https://www.peif.eu/
[30] https://www.wsbi-esbg.org/
[31] https://www.europeanpaymentscouncil.eu/
[32] https://www.association-secure-transactions.eu/

dissemination of related information, trends and general statistics across all geographies. Sharing also includes fraud definitions and preventive measures. At the international level, EAST maintains an active global Public-Private Partnership Network that includes Europol, GCCPOL, ASEANAPOL, US Secret Service and INTERPOL. EAST is developing a network of Global Members (entities that operate across two or more regions) and has country representation from America, Africa, Eastern Europe and Pacific Asia.

- The Nordic Financial CERT[33] runs continuous information sharing in the member community and participates actively in information sharing and cooperation with government, police and international information-sharing organizations.

At the international level, the **Financial Services Information Sharing and Analysis Center** (FS-ISAC) [34] focuses on safe and effective information sharing among financial institutions. The particular initiative has members from across the globe, which includes many European members as well. The FS-ISAC online sharing platform provides a way to share information without attribution. The ISAC also offers secure chat rooms, email lists, communities of interest and other efforts to encourage sharing. It also maintains an active Public-Private Partnership Network that includes Europol, National cybersecurity centres in the Netherlands and the United Kingdom. The ISAC offers guidelines and recommendations, Info sharing (IOCs, TTPs, etc.), Threat Intelligence, Industry papers, Opinion Papers, Playbooks and preparedness benchmarking.

**ENISA** contributes to the initiatives by supporting the establishment of information sharing and analysis centres (ISACs) in various sectors by providing information on best practice and guidance on available tools and procedures, as well as by appropriately addressing regulatory issues related to information sharing. ENISA is part of the established European ISAC in Finance. The **European Financial Institutes – Information Sharing and Analysis Centre (FI-SAC)[35]** is an independent organisation that was founded in 2008. Membership consists of country representatives coming from the financial sector, national CERT's (GovCerts) and Law Enforcement Agencies (LEAs). Other organisations represented are ENISA, Europol, the European Central Bank (ECB), the European Payments Council (EPC) and the European Commission. ENISA actively supports European FI-ISAC.

This information exchange helps each member and the banks in its member state, to raise awareness on potentials risks, and provides an early warning on new threats and MO's. The mission of the European FI-ISAC is information exchange on electronic and mobile channel, credit/debit cards, central systems and all ICT related topics including:

- Cyber-criminal activity affecting the financial community
- Vulnerabilities, technology trends and threats
- Incidents and case-studies

The members share information via meetings (biannually, hosted by members, in different European cities), via forwarding continuously relevant information to the EU FI-ISAC list server and via direct individual communication between member organizations/individuals. Trusted relationships are key to successful co-operation and exchange between members. Members represent their country and should actively participate in the information exchange. The European FI-ISAC has signed a Memorandum of Understanding with Europol EC3, which is a step to improve cooperation between the European banking community and European Law Enforcement Agencies.

[33] https://www.nfcert.org/
[34] https://www.fsisac.com/
[35] European Financial Institutes – Information Sharing and Analysis Centre, A Public-Private Partnership https://www.enisa.europa.eu/topics/cross-cooperation-for-csirts/finance/european-fi-isac-a-public-private-partnership

## 2.3 CYBER CRISIS MANAGEMENT

ENISA plays an active role in the **EU coordinated response to cybersecurity incidents crises**, assisting the European Commission whenever required, notably in the framework of the Integrated Political Crisis Response (IPCR) arrangements.

ENISA works closely with the Member States to develop EU-level cyber crisis management procedures to improve situational awareness in the event of cross-border cyber incidents, to assist both national level and EU-level decision-makers in taking the right decisions. ENISA also runs several crisis simulations[36] and exercises and offers numerous trainings[37] on this topic.

Additionally, ENISA manages the programme of pan-European exercises named Cyber Europe[38] and offers the cyber exercises platform[39], which is a tool for managing complex exercises.

The following structures also contribute to the overall cyber crisis management:

- The European Association for Secure Transactions (EAST) performs incident identification and qualified response actions taken in different locations.
- The Nordic Financial CERT supports and assists members in incident handling, response and recovery.
- The European Payments Council, via its Payment Scheme Fraud Prevention Working Group (PSFPWG), facilitates the collaboration between Payment Service Providers on operational payment fraud prevention including cybersecurity incidents affecting the SEPA payment[40] schemes.
- FS-ISAC provides industry-wide crisis response and coordination calls, crisis communications channels and support staff.

**CYBER CRISIS MANAGEMENT**

Participation or having a specific assigned role in the coordinated operational response at Union and Member State level to a large-scale cyber incident.

Support in operational handling of cybersecurity incidents, including response and recovery by providing expertise and/or resources or by facilitating the operational collaboration between MS or public/private sectors.

## 2.4 AWARENESS RAISING AND TRAINING

The **European Banking Authority (EBA)** develops awareness for cyber resilience through its policy work and through supervisory convergence activities. These involve workshops and training for supervisors and regulators across the EU and some non-EU jurisdictions. On the supervisory side, the EBA raises awareness also by incorporating specific details on ICT and cybersecurity into supervision. As part of its mandate to assess risks and vulnerabilities in the EU banking sector, the EBA publishes regular **risk assessment reports**[41] with ICT and cybersecurity risks included on a regular basis. Similarly, the joint committee of the ESAs risks reports also include regularly aspects of cybersecurity. The EBA cooperates too with external stakeholders, including consultations, roundtables and workshops.

Under the umbrella of the EBA's **FinTech Knowledge Hub**, the EBA also provides training to competent authorities on the topics of ICT and security supervision, fostering common understanding, knowledge exchange and guidance on the application of policy products in day-to-day supervisory activities. In addition, the EBA develops workshops and training on cyber risks and other risks for national authorities responsible for the supervision of credit institutions, payment institutions and other legal entities. These include physical seminars and online training or webinars. Within the mandate of the FinTech Knowledge Hub, the EBA also

[36] https://www.enisa.europa.eu/topics/cyber-exercises
[37] https://www.enisa.europa.eu/topics/cyber-crisis-management/trainings
[38] https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme
[39] https://www.enisa.europa.eu/topics/cyber-exercises/cyber-exercises-platform
[40] Single euro payments area (SEPA) https://ec.europa.eu/info/business-economy-euro/banking-and-finance/consumer-finance-and-payments/payment-services/single-euro-payments-area-sepa_bg
[41] The Risk Assessment Reports provide an annual update on risks and vulnerabilities in the EU banking sector https://eba.europa.eu/risk-analysis-and-data/risk-assessment-reports

engages with industry on cyber risks and other FinTech related topics in order to enhance knowledge sharing between the industry, the EBA and the competent authorities.

The **European Banking Federation (EBF)** plans and implements activities to raise awareness on cybersecurity issues and to enhance cybersecurity skills for bank employees and customers. Through its **Cybersecurity Working Group**, the EBF is actively working on cyber risk awareness-raising campaigns and initiatives in order to enhance cybersecurity skills for both the workforce and EU citizens. In 2014, the EBF signed a MoU with EUROPOL's European Cybercrime Center (EC3) [42] on three levels, including awareness-raising. Since then, it has leveraged the network of its banking community throughout 32 countries to raise awareness on the latest cyber threats and solutions to mitigate the risks within the sector (employees, customers and board level). The EBF has jointly created with EC3 the **Cyber scams**[43] campaign and supports also the **European Money Mulling Action**[44] and **NoMoreRansom**[45]**.** Moreover, the EBF organizes annually the EBF Cybersecurity Conference, an annual event in Brussels on cybersecurity in the financial sector and the EBF Innovation & Cyber Thursdays, covering an array of topics in the domain of digital innovation, including a day dedicated to cybersecurity and resilience, which explores the rapidly evolving trends and challenges for banks. Both events take place in October, in the framework of the European Cybersecurity Month (ECSM), which the EBF actively supports.

Additionally, these stakeholders also participate in the awareness-raising actions at EU level:

- European Savings and Retail Banking Group (ESBG) through advocacy in the field of cybersecurity, targeting members and stakeholders.
- European Payments Council through its Payment Security Support Group (PSSG) provides advice and guidance on security issues affecting payments or payment-related services within the framework of the EPC's activities.
- ESBG through position papers, organisation of public events and seminars.
- FI-ISAC shares information on new threats and attacks among its constituency.
- EAST shares information on Payment Alerts, Fraud Alerts, Physical Attack Alerts, best practice and guidance information, and conducts Private and Public training activities

At the international level, the **FS-ISAC** engages in awareness-raising through conference speaking engagements, good practice briefings to stakeholder groups (e.g. industry federations). Awareness mostly focuses on network and cybercrime threats. These include daily alerts, metrics reporting, threat calls, briefs and other activities. The task of the Global Intelligence Office, based out of London, is to help financial institutions understand the threat landscape through research and analysis. The FS ISAC offers Intelligence training, support for workforce diversity through academic scholarships. They also offer cyber range exercises and hands-on training.

ENISA reinforces links between EU institutions and general awareness-raising campaigns through active engagement of EU institutions in the **European Cybersecurity Month (ECSM)**[46]. The ECSM carries out regular stocktaking of national awareness-raising initiatives. It also builds upon this stocktaking and analyses and provides recommendations and advice on best practice in awareness-raising, in particular about communication activities.

**TRAINING**

Coordinating the design and planning of training courses, creating training material and/or providing targeted training courses; address the lack of cyber experts across the EU by offering training, education and practical application or working with MS to include cybersecurity training in MS educational curricula.

**AWARENESS RAISING**

Ensure cybersecurity is a common responsibility by promoting cyber hygiene and making relevant stakeholders aware of the relevant risks, threats, good practices and own role detect and actively protecting themselves against attacks.

[42] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
[43] Take control of your digital life https://www.ebf.eu/ebf-media-centre/cyberscams/
[44] Global crackdown on money laundering https://www.ebf.eu/ebf-media-centre/422-arrested-and-4-031-money-mules-identified-in-global-crackdown-on-money-laundering/
[45] No More Ransom campaign https://www.ebf.eu/cybersecurity/nomoreransom/
[46] The European Cybersecurity Month, https://www.enisa.europa.eu/topics/cybersecurity-education/european-cyber-security-month

## 2.5 STANDARDIZATION AND CERTIFICATION

The **European Central Bank** (ECB) published the **Cyber Resilience Oversight Expectations (CROE)**[47] for financial market infrastructures (FMIs). The CROE defines Euro-system's regulator expectations in terms of cyber resilience, based on existing global guidance. It provides clear steps for the FMIs on how to comply with the guidelines.

The **Cyber Risk Institute**[48] **(CRI)** is engaged in the protection of the global economy. It does soby enhancing cybersecurity and resiliency through standardization. As a not-for-profit coalition of financial institutions and trade associations, CRI houses and maintains the **Financial Services Cybersecurity Profile ("the Profile")** [49]— the benchmark for cybersecurity and resiliency in the financial services industry. This ever-evolving and concise list of assessment questions is drawn based on the intersection of global regulations and cyber standards, such as the standards of ISO and NIST. The Profile also aims to create a common supervisory tool designed to improve the ability of authorities to benchmark firm practices.

The **EBA** published two regulatory **technical standards under the Payment Services Directive II**. The two technical standards are:

- Regulatory technical standard-setting technical requirements on development, operation and maintenance of the electronic central register and on access to the information contained therein, under Article 15(4) of PSD2
- Implementing technical standards on the details and structure of the information entered by competent authorities in their public registers and notified to the EBA under Article 15(5) of PSD2

The **Financial Stability Board**[50] (FSB) developed a **Cyber Lexicon**[51], which sets the terminology to be used in cybersecurity and cyber resilience in the financial sector. It supports the public and private sector in properly understanding each other when describing cyber-related terminology. It also promotes a common language and facilitates cross-jurisdictional communication on cyber risk.

The **Payment card industry (PCI) standards Council**[52]'s mission is to enhance global payment account data security by developing standards and supporting services driving education, awareness, and effective implementation by stakeholders. The **PCI Security Standards** are developed specifically to protect payment account data throughout the payment lifecycle and to enable technology solutions that devalue this data and remove the incentive for criminals to steal it. They include standards for merchants, service providers, and financial institutions on security practices technologies and processes, and standards for developers and vendors for creating secure payment products and solutions. The council produced 15 PCI Security Standards, which are to be used in different parts of the payment process.

The Regulation (EU) 2019/881 (Cybersecurity Act)[53], establishes a European cybersecurity certification framework for ICT products, services and processes. **ENISA** participates in this new framework, by preparing candidate certification schemes on the request of the **European Commission** or the **European Cybersecurity Coordination Group** (representation of Member

**STANDARDIZATION & CERTIFICATION**

Development of cybersecurity certification schemes, in the certification of products, services and processes based on existing cybersecurity certification schemes.

Development of standards related to cybersecurity for products, services or processes.

[47] Cyber resilience oversight expectations for financial market infrastructures https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf
[48] The Cyber Risk Institute https://cyberriskinstitute.org/
[49] The Profile is the benchmark for cyber risk assessment, https://cyberriskinstitute.org/the-profile/
[50] The Financial Stability Board (FSB) is an international body that monitors and makes recommendations about the global financial system https://www.fsb.org/
[51] FSB Cyber Lexicon, https://www.fsb.org/2018/11/cyber-lexicon/
[52] The PCI Security Standards, https://www.pcisecuritystandards.org/
[53] REGULATION (EU) 2019/881 Cybersecurity Act, OJ L 151, 7.6.2019 http://data.europa.eu/eli/reg/2019/881/oj

States). Additionally, ENISA analyses aspects of functional equivalence of existing certification schemes across the EU (at the MS as well as the EU level).

## 2.6 RESEARCH AND INNOVATION

**CONCORDIA**[54] is a Cybersecurity Competence Network with leading research, technology, industrial and public competences. CONCORDIA provides excellence and leadership in technology, processes and services to establish a user-centric EU-integrated cybersecurity ecosystem for a digital sovereign Europe. Bringing different stakeholders together, developing innovative solutions in various sectors such as the finance sector, providing leading research and innovation through virtual labs, training courses and cyber ranges, as well as giving expertise to European policymakers and industry are examples of CONCORDIA's services. Besides, CONCORDIA is building a European educational ecosystem and publishes on regular basis reports on cybersecurity skills certifications or threat landscape

Similarly, **Cybersecurity for Europe**[55] is a research project, working towards harmonising the development of software components. It covers real-world use cases that address cybersecurity challenges within the vertical sectors of digital infrastructure, finance, government and smart cities, healthcare and transportation. One of the work packages focuses specifically on the common research, development and innovation in next-generation cybersecurity technologies (including dual-use), applications and services with a focus on horizontal cybersecurity technologies and cybersecurity in critical sectors (e.g. finance).

**RESEARCH & INNOVATION**

Promote research & innovation by providing funding, designing, implementing and coordinating research & innovation funding programmes and identifying priorities for research & innovation funding.

[54] Concordia Ecosystem, https://www.concordia-h2020.eu/
[55] CyberSec4Europe, https://cybersec4europe.eu/

TP-01-21-086-EN-N

## ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

**ENISA**
European Union Agency for Cybersecurity

**Athens Office**
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

**Heraklion office**
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-497-8
DOI: 10.2824/15644