EUROPEAN CENTRAL BANK

EUROSYSTEM

October 2024

Eurosystem Cyber Resilience Strategy

- Short version -

Contents

1. Cyber Resilience Strategy[1]

1.1 Context

The safe and efficient operation of the payment system is a statutory task of the Eurosystem and encompasses the safe and efficient operation of financial market infrastructures (FMIs) under the Eurosystem oversight mandate. The smooth operation of these FMIs – many of which are systemic in nature and essential for the implementation of monetary policy – is key for maintaining and promoting financial stability and economic growth.

Due to their high level of interconnectivity, these entities can transmit financial shocks across both domestic and international markets in case of adverse events. Therefore, a cyber-attack against such entities may pose a significant threat to financial stability and the smooth functioning of the payment system and raise risks for financial stability and monetary policy implementation given that cyber-attacks are increasingly sophisticated and pervasive in nature. Cyber risk is moreover accentuated due to its dynamic, evolving, and borderless nature.

FMIs also rely on the resilience of their participants, ICT third parties[2] and other interconnected financial entities. Failure of even one of these stakeholders in managing cyber risks may impact the own functioning of FMIs and could lead to the above-mentioned consequences for the broader financial ecosystem. Accordingly, it is of utmost importance that entities under the scope of the Eurosystem Cyber Resilience Strategy (‘the Strategy’’) maintain an adequate high level of cyber resilience and this also pertains to connections to service providers, participants etc. A high level of cyber resilience ensures an FMI’s own security and contributes in this way to the security of the ecosystem as a whole.

The current updated version of the Eurosystem Cyber Resilience Strategy also acknowledges the growing role of payment schemes and arrangements in the payments ecosystem and their coverage under Eurosystem oversight; accordingly, the Strategy aims to encompass these entities in a proportionate manner.

Although the Strategy is to be applied by the Eurosystem, cyber threats are borderless, and collaboration is recommended. Therefore, non-euro central banks are also invited to consider adopting and implementing tools from the Strategy.

1.2 Purpose

The initial Eurosystem Cyber Resilience Strategy was approved by the Governing Council in 2017 with the aim to provide a consistent approach[3] in addressing cyber risk and implementing the CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures[4] (‘‘the CPMI-IOSCO Cyber Guidance’) across the Eurosystem, by setting out an oversight strategy for cyber resilience for FMIs which fall within the legal framework of the Eurosystem central banks.

The current document provides an update of the 2017 Strategy considering the evolving threat landscape since then and leveraging industry best practices, lessons learnt from the application of the tools included in the initial Strategy and the practical application of the CPMI-IOSCO Cyber Guidance. The updated

[1] A number of key definitions of relevance to the current Strategy are taken from the FSB Cyber Lexicon (2023) – the definitions concerned (including the term “**cyber resilience**” are set out in Annex 1. Moreover, the EU Digital Operational Resilience Act (DORA) introduced the term **digital operational resilience** as “the ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions” and thus for the purpose of the Strategy the terms cyber resilience and digital operational resilience are considered to be analogous.
[2] ICT third-parties, in the context of the Strategy, refers to service providers using ICT means and may range from outsourcing of critical or important functions to provision of software/hardware that underpin or may affect these functions.
[3] https://www.ecb.europa.eu/paym/cyber-resilience/fmi/html/index.en.html.
[4] http://www.bis.org/cpmi/publ/d146.pdf.

Strategy also draws on the various Fundamental Elements of cybersecurity for the financial sector, developed by the G7 Cyber Expert Group (G7 CEG), which contain a concise set of best practice principles on various aspects of cybersecurity for the financial sector[5].

The Strategy also takes into account aspects of recent EU regulation, namely the "Digital Operational Resilience Act "(DORA). While DORA does not apply to payment systems, payment schemes or ICT third-party service providers that are subject to central bank oversight, it applies to some type of FMIs which are covered by this Strategy, e.g. central securities depositories (CSDs) and central counterparties (CCPs). In case a tool of the Strategy is (partially) covered by supervisory tools and other requirements deriving from DORA (and/or its RTS) then those tools and requirements must be taken into account for the entities in scope of DORA; central banks however may opt to use tool(s) of the Strategy in a complementary manner to DORA insofar as feasible.

To address the increase in cyber threats from the advancement in the capabilities of threat actors, the Strategy furthermore addresses emerging threats and vulnerabilities linked to geopolitical tensions or technological innovation (e.g. Artificial Intelligence, Quantum Computing).

Overall, the purpose of the updated Strategy is to ensure a comprehensive, holistic, and integrated approach that enables entities in its scope to continuously adapt and respond to the constantly evolving cyber threat landscape, and to enhance the ability to protect systems from cyber attacks and to resume business operations quickly in case of a successful cyber-attack.

1.3 Objectives

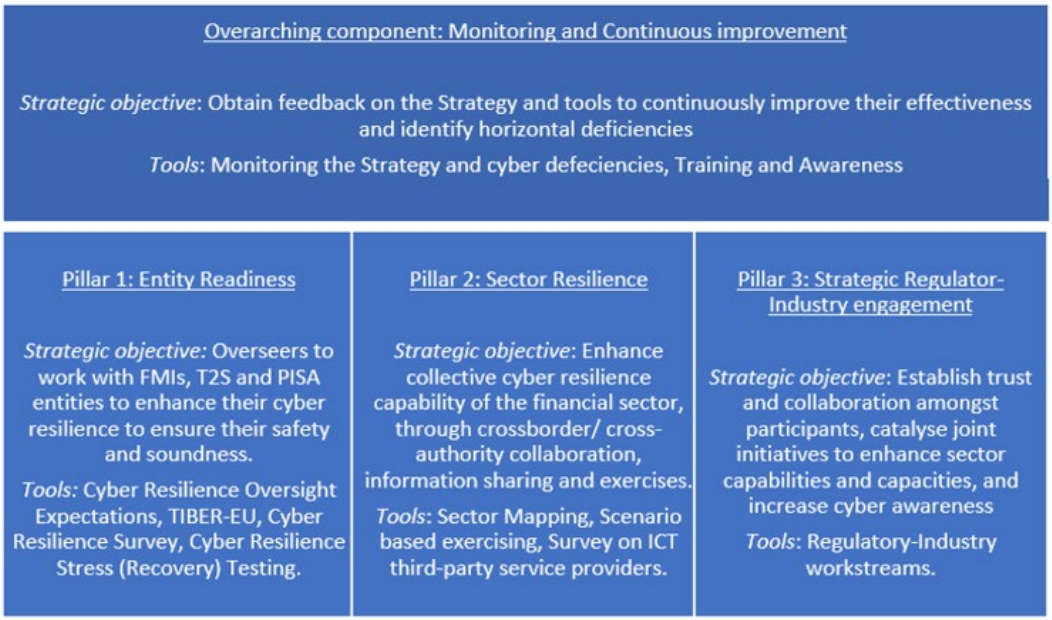
The overarching objective for the Eurosystem cyber resilience strategy is articulated as:

"ensuring the cyber resilience of the euro area financial ecosystem by enhancing FMI and payment entities' cyber readiness, fostering sectoral resilience and collaboration in a landscape of increasing interdependencies, sophisticated cyber threat actors, geopolitical tensions and emerging threats."

1.4 Structure

The Strategy continues to be organised according to the three pillars of the initial cyber resilience strategy[6]. A new addition to the Strategy is an overarching component that details monitoring and continuous improvement, thereby ensuring that progress is tracked, fostering harmonized implementation in each jurisdiction and allowing for proper adjustments to maintain the effectiveness of the tools.

[5] See for the relevant C7 CEG publications: https://www.ecb.europa.eu/paym/cyber-resilience/fmi/html/index.en.html.
[6] The 2017 Strategy comprised three pillars: FMI readiness, Sector resilience, Strategic regulator-industry engagement.



The Strategy specifies a set of tools for each pillar consisting of existing tools that will be updated and some new ones that will be established for the Strategy implementation.

The **1st pillar of the Strategy** covers "**Entity Readiness**". This refers to the cyber resilience of an individual entity (e.g. FMI, payment entity) and is one of the cornerstones of the Strategy. To enhance the collective cyber resilience capability, the focus then expands from entity resilience to the sector, thus in the **2nd pillar**, "**Sector Resilience**", the Strategy promotes sectoral (incl. cross-border and cross-authority) collaboration, information sharing and joint cyber crisis simulation exercises. At the same time the financial ecosystem and authorities need to collaborate and cooperate in order to identify and subsequently mitigate cyber risks via collective actions, which are the goals of the **3rd pillar**: "**Strategic Regulator-Industry Engagement**".

1.5 Scope

The Strategy covers overseen FMIs and entities under the Eurosystem oversight framework for electronic payment instruments, schemes and arrangements (PISA Framework[7]). Specifically, it covers the following systems and entities: systemically important payment systems (SIPS), large-value payment systems (LVPS), prominently important retail payment systems (PIRPS), other retail payment systems (ORPS), TARGET2-Securities, CSDs, CCPs and overseen payment schemes and arrangements under the PISA framework (PISA entities). In the context of this Strategy, the term "**entity**" is used for ease of collective reference to the aforementioned FMIs as well as schemes/arrangements under the PISA framework.

A harmonized approach in the implementation of the Strategy by central banks is desirable and shall be promoted also through the new overarching component for monitoring the implementation (and continuous improvement) of the Strategy.

2. Entity readiness

2.1 Preface

Entities need to have strong cyber resilience capabilities to protect themselves against the unpredictable and increasingly sophisticated cyber threat landscape. Hence, the strategic objective of this pillar is for overseers to work with these entities to enhance their cyber resilience. To achieve this objective, the

[7] https://www.ecb.europa.eu/paym/pdf/consultations/ecb.PISApublicconsultation202111_1.en.pdf

Eurosystem has developed several tools that collectively aim to help increase the cyber resilience of entities and allow overseers to:

- assess cyber resilience of the entities using a set of expectations aligned with the CPMI-IOSCO Cyber Guidance: the Eurosystem Cyber resilience oversight expectations (**CROE**)**;**
- have a general, timely insight on the level of maturity of those entities in terms of cyber resilience: **the Cyber Resilience Survey**; and
- realistically test the cyber resilience posture of the entities according to a framework that requires a sufficient level of security and quality in the management of the test: **the TIBER-EU framework.**

In addition, a new tool is also included, namely:

- **Cyber Resilience Stress Testing**, to assess the effectiveness of entities in recovering and resuming business operations if a cyber-attack is successful.

2.2 Cyber Resilience Oversight Expectations (CROE)

The CROE serves three key purposes:

- it provides entities with detailed steps on how to operationalise the CPMI-IOSCO Cyber Guidance, ensuring they are able to foster improvements and enhance their cyber resilience over a sustained period of time;
- it provides overseers with clear expectations to assess payment systems and other entities under their responsibility; and
- it provides the basis for a meaningful discussion between the entities and their respective overseers.

The cyber threat landscape is continuously evolving, with new threats emerging daily and threat actors improving their capabilities. To deal with this increasingly sophisticated threat landscape and realising that cyber resilience is not static but a process of continuous improvement, **the CROE establishes a maturity model outlined in three levels of expectations: evolving, advancing and innovating**. Each level includes practices that build on top of each other.

Although the CROE was created to provide entities with detailed and specific expectations on how to implement the CPMI-IOSCO Cyber Guidance, it also incorporates proportionality given that entities vary in nature, size, complexity and systemic importance. The CROE utilises a maturity model where the minimum level to be achieved by each entity will be different depending on the respective criticality of the entity concerned for the financial system. The purpose of the three levels is to enable the FMIs to enhance their respective capabilities in a layered manner over a longer period of time. Entities under PISA will be expected to adopt the CROE after the PISA assessment methodology is adapted in this respect, also taking into account elements of proportionality as relevant for such entities.

2.3 Threat Intelligence led Ethical Red Teaming (TIBER-EU)

In 2018, the ECB published the TIBER-EU framework. TIBER-EU enables European financial entities to conduct threat intelligence based ethical red teaming, led by competent authorities, also commonly referred to as threat-led penetration testing (TLPT). TLPT is a form of testing to model adversarial behaviour, where an attacking team (the red team) challenges the defending team (the blue team) with the aim to anticipate, as much as possible, the impact that a real attack could have on an entity. .

TIBER-EU is a framework designed to test a financial entity's live production systems underpinning critical or important functions. The testing is conducted under the monitoring of the TIBER Cyber Team (TCT), established by the authority that has implemented the TIBER-EU framework in its jurisdiction. The aim of this test is to improve the entity's knowledge of its own weaknesses and strengths when dealing with a cyber-attack and identify those measures that may enable it to enhance its cyber resilience.

DORA requires the mandatory execution of Threat Led Penetration Tests as a form of advanced operational resilience testing for significant financial entities[8] in the EU. The **ECB published a legal opinion on DORA**[9], which states that ***any regulatory technical standards (RTS) for TLPT under DORA need to be drafted in accordance with TIBER-EU***. Thus, the DORA RTS TLPT has been drafted in accordance with the TIBER-EU framework and in agreement with the ECB[10].

The **TIBER-EU Knowledge Centre (TKC)** is a forum hosted by the ECB in which national and European TIBER cyber teams coordinate and discuss initiatives and share details of their experiences. The TKC may as needed:

- propose updates to the TIBER-EU framework
- propose updates to the TIBER-EU Service Procurement Guidelines, TIBER-EU White Team Guidance, TIBER-EU guidance and templates and the TIBER-EU Purple Teaming Best Practices;
- suggest the publication of any other guidance as relevant.

The TIBER-EU framework will be updated to align with the DORA RTS. The updated TIBER-EU framework and supplementary guidance will be fundamental in order to assist authorities in implementing/running TLPT across Europe. In particular, these documents serve to:

- improve the TLPT practices in the respective jurisdiction;
- provide adequate guidance to the tested entities;
- contextualise the requirements for TI and RT providers (and internal testers);
- enable TLPT knowledge sharing between NCAs via the TKC for the authorities that adopt TIBER-EU.

2.4 Cyber Resilience Survey

The purpose of the Survey is to obtain a periodic overview of individual entities' cyber resilience maturity and to identify in a quick manner the effectiveness of the practices deployed by these entities, as well as form an aggregated view on cyber resilience level at the sector level. The results serve as a tool to identify main vulnerabilities in the systems and processes of the respective entities and serve as a basis to engage with the individual entity and develop remediation plans.

The Survey helps the overseer and the relevant stakeholders of the Strategy to:

- benchmark the level of cyber resilience amongst the entities;
- monitor progress made by the sector in the implementation of the CPMI-IOSCO Cyber Guidance;
- leverage the Survey as a tool of improvement for the cyber resilience posture of the sector.

2.5 Cyber Resilience Stress Testing

The core purpose of the Cyber Resilience Stress Testing tool is to assess an entity's level of readiness with respect to the continuity of critical functions under plausible cyber-attack scenarios, leveraging on the work of the European Systemic Cyber Group (ESCG) under the European Systemic Risk Board (ESRB)[11] and

[8] Only entities under DORA deemed significant by their respective CAs.

[9] "There is no need for the development of a new advanced cyber resilience testing framework as Member States have already widely adopted TIBER-EU, the only such framework in the EU at present" and that "the regulatory and implementing technical standards, which are to be drafted for TLPT under the proposed regulation, should be in accordance with TIBER-EU." https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021AB0020.

[10] On 26 June 2024 the Governing Council decided that the draft RTS on threat-led penetration testing (TLPT) prepared in accordance with Article 26(11) of Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) were also in accordance with the European Framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU). https://www.ecb.europa.eu/press/govcdec/otherdec/2024/html/ecb.gc240719~dde12c2121.en.html

[11] https://www.esrb.europa.eu/news/pr/date/2024/html/esrb.pr240416~bd1b9fc086.en.html

G7 guidance[12]. The results may identify vulnerabilities in the recovery process at entity level, but could also be used to evaluate the recovery readiness of the sector,

The Cyber Resilience Stress Testing aims to help the relevant stakeholders:

- understand the continuity capabilities of an entity;
- identify which plausible scenarios are challenging for an entity from a recovery perspective;
- determine from which scenarios entities can generally recover in a satisfactory manner;
- determine for which scenarios financial entities generally need to improve upon;
- identify factors that can hinder or boost individual and collective recovery.

3. Sector Resilience

Even though entities may attain a high level of cyber resilience, the levels of interconnectedness and interdependency have significantly increased across the financial ecosystem over the last years, exposing each entity to impacts of events that may have affected other entities, including third parties and ICT service providers with which they are connected.

Occurrence of cyber incidents related to third-party products and cyber threats more generally increased in recent years. Equally, the digitalisation of the financial sector is accelerating, with new technologies like Distributed Ledger Technology (DLT) and Artificial Intelligence (AI) on the rise, and a potential threat from quantum computing on the horizon.

Two major oversight tools exist to assess cyber risk and supply-chain risk at sector level: i) the previously mentioned **Cyber Resilience Survey**, a self-assessment that facilitates overseers to evaluate the level of cyber resilience of entities, in order to help identify areas of strength or weakness based on sector-wide assessments, and ii) the Eurosystem's **Critical Service Provider Survey (CSP survey)** that enables overseers to identify service providers that can be classified as critical, based on a self-assessment by the entities.

The updated Strategy aims to develop and maintain a broader set of tools that includes, among others, the following:

- a Sector Mapping to identify critical nodes and interdependencies within the European financial ecosystem;
- Scenario-based exercising to assess industry-wide preparedness including response, resumption and recovery practices including governance arrangements and communication plans based on the simulation of extreme but plausible cyber-attack;
- a Survey on ICT service providers to enhance the existing CSP Survey.

4. Regulator-Industry Engagement

Whilst the first two pillars focus on preparing cyber readiness and cyber capabilities of individual entities and the financial sector as a whole, the major stakeholders involved in these processes are authorities (central banks, supervisory authorities), market actors (e.g. FMIs and their CSPs) and the cybersecurity sector. Consequently, it is critical that there is a forum which brings these stakeholders together. Such a forum catalyses a European cybersecurity sector and helps develop effective solutions for the market.

[12] https://www.ecb.europa.eu/paym/pol/shared/pdf/November_2020-G7-fundamental-elements-of-cyber-exercise-programmes.en.pdf

For this reason, the ECB set up the Euro Cyber Resilience Board (ECRB) in 2017, consisting of the pan European FMIs, their critical service providers and other critical stakeholders in the EU[13]. At national level, central banks may set up similar arrangements to facilitate local engagement.

Given the continuously evolving threat landscape, the ECRB is a forum where all the relevant stakeholders can come together to exchange ideas at a strategic and Board level on how best to tackle the emerging challenges, share best practices and tools, encourage information sharing, and identify gaps and weaknesses in the ecosystem which require collaborative thinking to catalyse effective solutions.

The ECRB continues to work with a view on finding solutions together with the market on the cyber challenges that the financial sector and the respective ecosystem is facing. In addition, central banks should promote the creation of such fora on a local level so that the respective financial ecosystems can work together to solve the existing cyber challenges and upcoming cyber threats.

Moreover, the ECRB continues to work on areas such as Eurosystem recovery, Information Sharing (e.g. further enhancing the ECRB Cyber Intelligence and Information Sharing Initiative (CIISI-EU)) Crisis Coordination, Third-party risk and Training and Awareness. Additionally, recognizing the importance of collaboration and knowledge sharing in the field of cybersecurity, the ECRB should be open and prepared to engage with other similar fora.

5. Monitoring and continuous improvement

The Strategy outlines a variety of tools that aim to bolster the cyber resilience of individual entities and of the financial sector as a whole. It is imperative that the Strategy has a feedback loop by which it brings together reactions and lessons learned from all the tools, as they are applied at entity level and in the various countries, in order to understand the effectiveness of the tools and whether any changes are needed. This feedback loop also enables the aggregation of results from the tools which can identify what deficiencies exist on a sector wide level, to raise awareness and possibly create new tools where needed.

The feedback loop is to be effected through a **survey on the implementation of the Strategy and cyber deficiencies.** Every 2 years a survey will be circulated to the central banks to understand the status of work on the implementation of the strategy and the type of cyber deficiencies that exist across the market infrastructure ecosystem. The **first part of the survey** shall focus on the tools of the strategy and the extent of their implementation and perceived effectiveness by the central banks. The **second part of the survey** shall focus on the cyber deficiencies identified by the respective central banks through the tools that they have implemented. This will be done using a common taxonomy / reference to enable the central banks to quickly discern which areas seem to be deficient on a broad basis across the various entities.

Finally, there needs to be regular training on cyber topics across the central bank community in order to ensure ongoing education of overseers and cultivate deep awareness of the Strategy.

All these actions will help the implementation of the Strategy and further ensure a successful and harmonized implementation of the tools throughout the Eurosystem.

[13] https://www.ecb.europa.eu/paym/groups/euro-cyber-board/html/index.en.html.

Annex 1: Overview of tools per pillar and their potential application to entities under the scope of the Cyber Resilience Strategy

(*As indicated previously, central banks have flexibility in the implementation and application of the tools to their overseen entities*)

Pillar	Tool/Type of entity	PS and T2S	CSD	CCP	Payment Schemes	Payment Arrangements	ICT Critical Service Providers[14]
1	CROE[15]	X	*	*	X[16]	X[17]	
1	Cyber Resilience Survey	X	X	X	X	X	
1	TIBER-EU	X	*	*			
1	Cyber Resilience Stress Testing	X	X	X			
2	Sector Mapping	X	X	X	X	X	
2	Scenario based exercising	X	X	X	X	X	X
2	Survey on ICT Service Provider	X	X	X	X	X	
3	Regulatory Industry-engagement	X	X	X	X	X	X

*CSDs/CCPs are also subject to corresponding requirements in DORA.

The above table may serve as a guide for the implementation of the Strategy. A central bank may choose to implement and apply tools beyond those proposed in the table.

[14] Insofar these ICT Third-Parties underpin (or may adversely affect critical function for entities under the scope of the Strategy.
[15] The application of CROE for overseen PISA entities will be limited to the evolving level with the twofold objective of pursuing a harmonised approach while maintaining an adequate level of flexibility in relation to their nature and regulatory landscape.
[16] After the assessment methodology of the CROE is developed.
[17] After the assessment methodology of the CROE is developed.