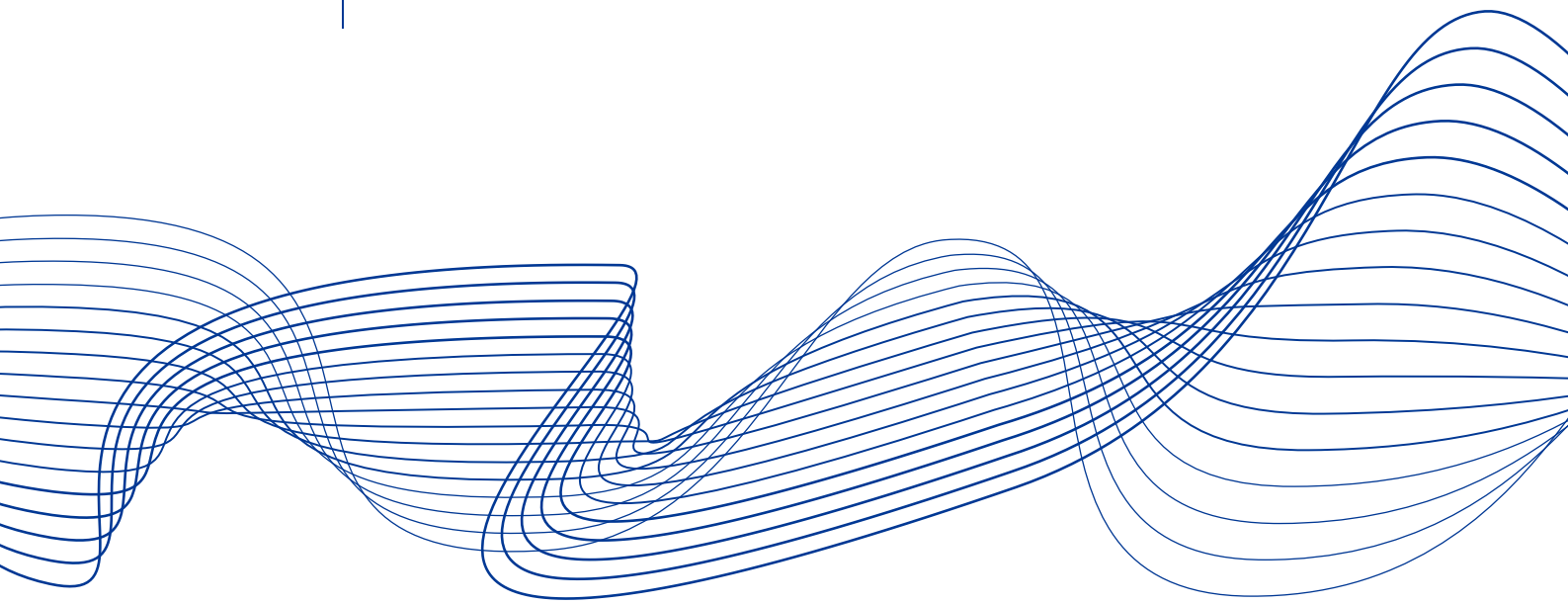
# Advancing macroprudential tools for cyber resilience – Operational policy tools

**April 2024**

A review of national and pan-European frameworks



ESRB
European Systemic Risk Board
European System of Financial Supervision

# Contents

# Executive summary

**Cyber threats continue to pose significant risks to financial stability in the EU and beyond.** The persistently heightened cyber threat environment in Europe is evidenced by the sabotage of undersea telecommunications cables, the disruptions to systems in large banks and third-party providers, and the increased sophistication of cyberattacks and the skills of hackers[1]. This shows how even financial institutions with mature cybersecurity and tested disaster plans are not immune to cyber risk. It also highlights that financial institutions need to assess their own third-party providers' cybersecurity fitness in the interests of overall financial stability. Incidents like the ransomware attacks on the ION Group and ICBC Financial Services in 2023 show that key economic functions such as securities trading and the US Treasury market impact financial markets (see **Box 1**). Also, if contingencies and mitigants had not been available or had not worked effectively, these incidents could have been amplified and could have had a significant impact on firms, with potentially systemic financial stability impacts. Recovery from a serious ransomware attack takes time and if a key node in the financial system is affected (such as a financial market infrastructure, FMI) it will be likely to crystallise systemic impacts and require the authorities to take action to prevent financial stability contagion.

**This report reviews operational policy tools used to address systemic cyber crises across the membership of the European Systemic Risk Board (ESRB) at both the national and the supra-national levels.** It complements a report published by the ESRB in 2023 that included a review of financial policy tools such as capital buffers.[2] While the later stages of a systemic cyber crisis can resemble a more traditional financial crisis and can therefore be mitigated using traditional financial policy tools such as capital buffers, moratorium powers and ad hoc bank holidays, or central bank liquidity provisions, any impairment of the financial system's operability remains unaddressed. Operational policy tools can help mitigate the impact before, during and after an incident – they focus on preserving the underlying processes and systems on which the functioning of the financial system relies. They also focus on the information-flow channel, coordination functions and emergency/backup systems. Operational policy tools are therefore likely to be used in conjunction with financial policy tools. Beyond incident response, more holistic cybersecurity practices, including preventing new incidents and learning from past incidents, are needed across the entire financial sector and all agents in the sector. The overarching objective of all the tools reviewed is to ensure the European financial system is resilient and that systemic cyber crises are mitigated or, ideally, prevented.

To strengthen the financial system's overall resilience, the ESRB focuses on three distinct but interacting groups of operational tools.

- **Tools for gathering, sharing and managing information provide timely and high-quality data.** These are essential for systemic cyber risk monitoring, tool calibration and the ex post

1 See ENISA (2023b), **ENISA Threat Landscape 2023**, October.

2 Financial policy tools are reviewed in ESRB (2023), **Advancing macroprudential tools for cyber resilience**, February.

management of systemic cyber crises. The tools can provide valuable insights into the patterns of current threats and vulnerabilities.

- **Coordination tools help to mitigate potential negative effects on financial stability.** Financial institutions as well as authorities need to bear in mind that severe incidents may occur and should be prepared to implement crisis management plans. Financial authorities should enhance their capabilities to interact across jurisdictions with other financial and cyber authorities in coordination networks.

- **Emergency and backup systems can help to ensure the sustained provision of critical economic functions.** These are a new set of macroprudential tools that address systemic cyber risk, even in worst-case cyber incident scenarios.[3] The tools are put in place in advance and take effect after an incident has occurred, the aim being to foster overall resilience and temporarily ensure the continuation of key economic functions. Such tools have only been introduced in a few countries at a system-wide level.

**The three groups of tools discussed in this report cater to the second and third layers of defence and aim to foster system-wide resilience.**[4] The first layer of cyber defence is an institution's own detection and defence capabilities. Strengthening these capabilities is a key component of the significant ongoing efforts made by the EU to implement the Digital Operational Resilience Act (DORA).[5] The ESRB's focus, however, lies in the systemic nature of cyber risk and the financial system's resilience as a whole and addresses response and recovery capabilities (second layer) and the coordination and action capabilities of the authorities (third layer).

**Against this background, the ESRB evaluated the aforementioned types of tools as follows.**

- **The ESRB encourages financial institutions and authorities to improve their information management and information-sharing efforts.** The effectiveness of existing information-sharing tools and incident reporting centres in a major cyber incident depends largely on the format and the scope of the respective tool in place and whether it can be used across jurisdictions and sectors. In certain cases, market information and media coverage act as a source of information which can be misleading and inaccurate. This makes a clear case for employing structured and harmonised tools which can be used to gather, manage and share information. The use of information-sharing tools and incident reporting centres is critical to a functioning EU-wide information-sharing mechanism.

- **The ESRB advocates for national and EU-level crisis management and coordination practices in line with European and international standards.** This helps to address the

3 For readability purposes, we use the term "macroprudential tools" as shorthand for tools that serve macroprudential objectives, even if the tools themselves may be operational in nature.

4 Three layers of defence were identified in ESRB (2023), **Advancing macroprudential tools for cyber resilience**, February.

5 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022, p. 1.)

entire crisis management lifecycle of readiness, response and recovery[6]. Although Member States have national crisis management coordination mechanisms in place, resource constraints mean that 24/7 availability is often difficult to achieve. Secure communication channels are needed for responses to be effective, while response speed could be improved through targeted training and by conducting exercises involving decision-makers. The complexity of the response process requires effective coordination among all stakeholders.[7] This will be improved with the establishment and implementation of DORA as a first step at the national level and the pan-European systemic cyber incident coordination framework (EU-SCICF) at the EU level.[8]

- **The ESRB would consider the pros and cons of system-wide contingency options and backup arrangements.** This is because there may be systemic incidents that cannot be solved by the business continuity measures individual institutions have in place. It is primarily the responsibility of each individual institution to ensure its (time-) critical activities are functioning, although maintaining critical financial activities and functions in society is also a priority for the authorities. Moreover, the existence and use of a contingency option or backup system can also help maintain confidence in the affected financial institution. However, the costs and risks associated with developing, maintaining and using backup systems are likely to increase with the scope of an emergency system. Such systems are currently only in place at the national level. A European-level emergency system – or a framework for coordinating national backup systems – would require extensive discussion with national institutions and a careful evaluation of its benefits and any potential implications at both the system-wide and the national level. It would also require effective coordination across all institutions.

6 European and international standards for cybersecurity, which contain corresponding guidelines and are deployed in the financial sector, include the following: the **G7 Cyber Expert Group's family of "Fundamental Elements"**, the **CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures**, the **ISO/IEC 27000 family of standards on information security management systems** and the **NIST Cybersecurity Framework**. See also the European Banking Authority's **guidelines on ICT and security risk management**, the European Insurance and Occupational Pensions Authority's **guidelines on information and communication technology security and governance**, the Financial Stability Board's **cyber incident response and recovery toolkit** as well as the Basel Committee on Banking Supervision's principles for **operational resilience**, **sound management of operational risk** and **effective risk data aggregation and risk reporting**.

7 The use of standards contributes to the establishment of common taxonomies, terminology and conventions and the overall effectiveness of collaboration between the various actors. The **Traffic Light Protocol – FIRST Standards Definitions and Usage Guidance 2.0**, for example, "was created to facilitate greater sharing of potentially sensitive information and more effective collaboration".

8 The respective international and European standards fed into DORA and the complementing implementing acts such as the draft Regulatory Technical Standards developed under Article 15 and Article 16(3) of DORA. See EBA (2024), **Draft Regulatory Technical Standards**, EIOPA/ESMA, January. For information on standards and legislation referring to EU-wide crisis communication and coordination, see ENISA (2024), **Best Practices for Cyber Crisis Management**, February.

# 1 Introduction

**The risks to financial stability from cyber incidents, which had been identified by the ESRB as key risks in 2020, have increased in recent years.** This increase reflects several factors. First, the structural change arising from increased digitalisation has led to more complexity and homogeneity. This is because advances in telecommunications and information technology have given rise to new delivery channels and providers.[9] IT landscapes have become more heavily dependent on core infrastructures (such as the internet), standardised IT products with mass users (such as IT operating systems) and associated methods and technologies (such as encryption standards). This trend was accelerated by the coronavirus (COVID-19) pandemic and is likely to continue as profitability can typically be achieved through high levels of standardisation and scaling in the development of (ICT-)products.[10] Second, adversaries behave strategically. Not only do they continuously seek to overcome the latest IT security measures but, as a 2022 ECB study found, they also deliberately time attacks to strike when they expect targets to be at their weakest.[11] In 2023 the variety and number of cyberattacks grew significantly and ongoing geopolitical tensions could adversely impact the risk landscape further.[12] Recent incidents, including the physical sabotage of power and telecommunications infrastructure, underscore the financial system's need for broad operational resilience.[13] Direct attacks on financial institutions reveal how even large institutions can be harmed by breaches at fintechs and other third-party providers (**Box 1** below).

Box 1

## Recent examples of cyber incidents

A technological disruption due to a cyber incident may result in the loss of availability of a critical service and/or the loss of the confidentiality, integrity or reliability of data underlying a critical service. This in turn could affect the delivery of an important economic function. In the worst-case scenario the initial shock spills over from the operational channel to the financial and confidence transmission channels and is amplified through feedback loops.

Among multiple recent cases, we highlight how two "near miss" incidents evolved. To analyse them, we apply the ESRB's conceptual model for systemic cyber events.[14]

---

9 A rough distinction can be drawn between providers that operate either in competition or in cooperation with established institutions to deliver financial services (commonly referred to as fintechs and big techs) and ICT-providers that support the business operations of the above-mentioned financial services providers (e.g. cloud service providers).

10 See Beck, T. et al. (2022), "**Will video kill the radio star?– Digitalisation and the future of banking**", *Reports of the Scientific Advisory Committee*, No 12, ESRB, January.

11 See Fell, J. et al. (2022), "**Towards a framework for assessing systemic cyber risk**", *Financial Stability Review*, ECB, November.

12 See ENISA (2023b), **ENISA Threat Landscape 2023**, October.

13 Incidents like the sabotage of the sub-sea Nord Stream natural gas pipelines in 2022 have highlighted the need to further address the security of (submarine) physical infrastructures. Sub-sea cables are among the most important components of the global internet infrastructure, as an estimated 97% of the world's internet traffic is transmitted in this way. The risk of incidents affecting such infrastructure, leading to sector-wide outages, was recently reflected in a dedicated report. See ENISA (2023a), **Undersea cables**, August.

14 The ESRB has developed hypothetical scenarios that describe how a cyber incident can be amplified and cascade into a systemic event. See ESRB (2020),"**Systemic Cyber Risk**", February for detailed scenarios and the theoretical model.

**1 The ION Group ransomware attack**

In January 2023, the LockBit ransomware gang[15] targeted ION Group, a UK-based software company, which provides automation software to match both sides of exchange traded derivatives trades and their clearing, with lasting effects on derivatives trading.

- **Context:** Little information is available on how the cybercriminals infiltrated ION Group's systems, which vulnerabilities they exploited or if they engaged in a supply chain attack. The ransomware attack disabled ION Group's cleared derivatives front, middle and back office services for clients, with no other services affected. It forced the financial institution to take parts of their systems offline.
- **Shock:** The incident left over 40 banks, hedge funds and brokerages without the ability to process transactions and slowed down their operations. Many had to manually process trades and were forced to submit trading reports based on estimates which were revised later.
- **Amplification:** Not providing much information at the onset, ION Group frustrated both regulators and clients and ignited fears of systemic risk. After the financial press publicly reported on the incident, the US Department of the Treasury's office of cybersecurity and critical infrastructure protection took steps to assure market participants that the situation was under control. Some exchanges and clearing houses offered extensions to clearing and reporting deadlines to alleviate the burden on market participants and ION Group itself.
- **Systemic event:** Contingency measures ensured that the incident was not amplified by a lack of trust in a key node. Therefore, it did not trigger a loss of confidence in the market and did not become systemic. ION Group did not disclose details on the root cause of the incident.

**The disruption is a striking example of how an incident at a relatively little-known third-party provider (albeit one of great significance) can cause major disruption, if that institution provides vital central services through the financial industry's supply chain.** The case of ION Group underscores the critical need for third-party providers to have robust and comprehensive cybersecurity measures in place that are regularly audited, tested and in line with international standards. As dependencies on digital systems grow, financial institutions must continuously improve their own protection and evaluate their exposure to third-party providers.

**2 The ICBC FS ransomware attack**

In November 2023 a ransomware attack attributed to the LockBit ransomware gang on the Industrial & Commercial Bank of China Financial Services (ICBC FS), a financial services arm of China's largest credit institution and the world's largest bank by assets, disrupted the USD 26 trillion US Treasury and repo financing market. ICBC FS is an intermediary for proprietary traders, hedge funds and governments that want to buy and sell US debt. The incident had a lasting and wide-reaching impact on the markets and prevented the financial institution from settling US Treasuries on behalf of its clients.

[15] LockBit is a cyber criminal group that holds victim's data or devices hostage and threatens to keep it locked – or worse – unless the victim pays a ransom.

- **Context:** The cybercriminals introduced ransomware to the financial institution's systems. This temporarily prevented ICBC FS employees from accessing emails and connecting to the Depository Trust and Clearing Corporation (DTCC) to handle US Treasury trades. The attack was linked to a pre-existing vulnerability in Citrix platforms that are widely used for application delivery and VPN connectivity by many companies in most sectors. While Citrix made patches publicly available and urged customers to patch their systems over a month, ICBC FS failed to take necessary measures and had unpatched systems which were hit by the ransomware.
- **Shock:** The shock was felt at an international scale due to the core role of US Treasury markets in the global financial system. Ripple effects cascaded once ICBC FS proved unable to settle trades for other market participants. The trade backlog of US Treasuries was further compounded by the impossibility to initiate systemically vital repo agreement transactions. The attack also coincided with auctions for 30-year Treasuries in those days by the US Government.
- **Amplification:** While the shock caused loss of trust in a major lender, Bank of New York Mellon, which is the sole clearing bank in the US for Treasury repo settlement, was able to take over the clearing obligations on behalf of ICBC FS. This stopped any further amplification.
- **Systemic event:** The financial losses, the operational impact and loss of confidence were serious for ICBC FS as market participants were reluctant to reconnect to them after the incident had been resolved. As explained above, further dislocations in the repo and US Treasuries markets were, however, averted. Thus, the event did not trigger a serious threat to financial stability.

**The ransomware attack on ICBC FS forced the bank to reroute trades which, even though it did not bring the market to a standstill, revealed the overall vulnerability of financial markets and financial stability to cyberattacks.** ICBC FS required a USD 9 billion injection by its parent company to compensate BNY Mellon for taking over its obligations.

**The ESRB's macroprudential strategy to ensure financial stability in the event of a systemic cyber crisis should acknowledge the characteristics and nature of cyber risk.** The characteristics of cyber risk pose several challenges. First, there is a high level of uncertainty. While it is not possible to predict precisely when an incident will occur or how it will materialise, it is certain that incidents *will* occur. This is because errors are almost unavoidable given the complexity of technical systems and the dedicated efforts made by attackers to find and exploit such errors. Second, both the speed and scale at which cyber incidents occur shorten adequate response times. Third, the often short-lived nature of knowledge (i.e. due to the rapidly changing IT landscape) makes it more difficult to respond to an incident or avoid it in advance. Lastly, the causes of an incident are sometimes not tangible. Not only are attackers themselves rarely traceable but, in the event of an incident, the technological network extends far beyond the boundaries of the sectorally regulated system, making it considerably more difficult to identify and address the root cause.

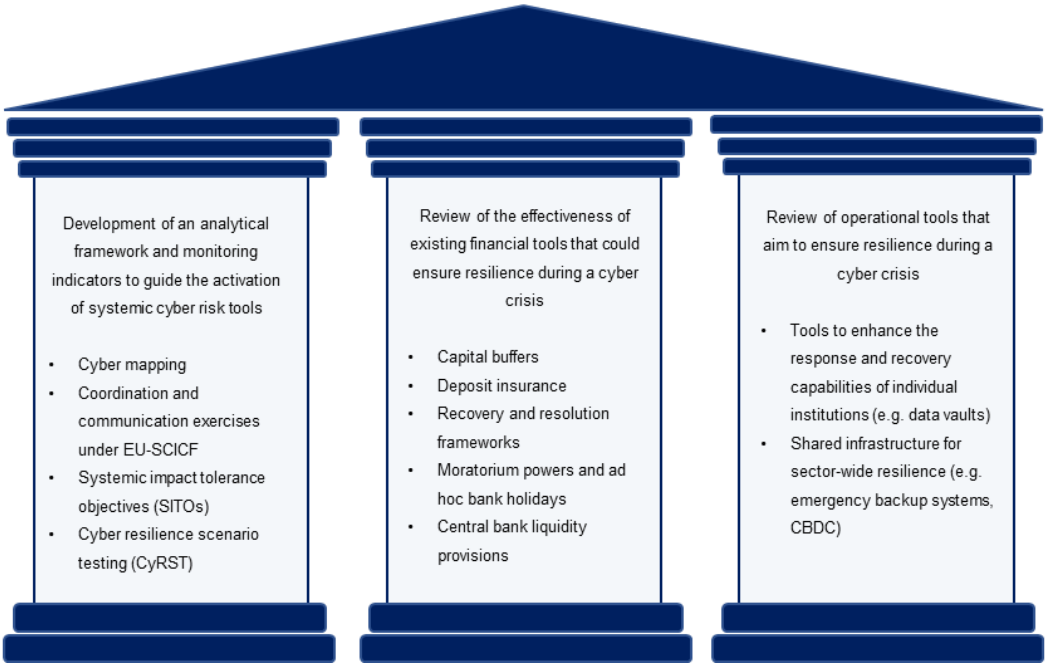
**The ESRB's macroprudential strategy to ensure financial stability in the event of a systemic cyber crisis aims to foster (operational) resilience.** The concept of resilience incorporates two key ideas: first, the ability of an entity or system to withstand an immediate shock and, second, its ability to adapt effectively to new conditions.[16] Moving beyond preventive risk avoidance or preventive risk management strategies, the concept of resilience addresses uncertainty via an "assume-breach mentality".[17] Under this assume-breach mentality entities, supervisors, policymakers and market participants assume that breaches and technical failures are inevitable and dedicate resources to coping with the consequences of an incident. To ensure a rapid response, institutions and authorities should always be prepared and aware in equal measure. As the root cause of cyber incidents is often uncertain or cannot be mitigated, cause-agnostic macroprudential tools can provide for an effective response. All of these points are reflected in the ESRB's macroprudential strategy to ensure financial stability in the event of a systemic cyber crisis (ESRB, 2022a; ESRB, 2023). The strategy is summarised in **Figure 1Error! Reference source not found.** below and comprise a three-pillar approach: (1) it consists of the development of an analytical framework and monitoring indicators to guide the activation and evaluation of systemic cyber risk tools, (2) it reviews the respective financial tools established by the ESRB (ESRB, 2023), and (3) it summarises the operational tools described in this report.

16 ECB (2022), **Macroprudential policy in Europe: building resilience in a challenging environment**, *welcome remarks by Christine Lagarde, President of the ECB and Chair of the European Systemic Risk Board, at the sixth annual conference of the ESRB*, December.

17 This is not necessarily specific to cyber risk but it is to crisis management more generally and is the foundation of bank resolution in the Bank Recovery and Resolution Directive.

Figure 1

**Macroprudential strategy to ensure financial stability in the event of a systemic cyber crisis**




*Source: ESRB.*

**The impairing effect of cyber incidents on the financial system's operability adds a new dimension to macroprudential policy and should be reflected in the macroprudential toolkit.** The ESRB has reviewed the effectiveness of the macroprudential toolkit in addressing risks to financial stability from cyber incidents (ESRB, 2022a; ESRB, 2023). This was carried out using a conceptual model of how a cyber incident can evolve from an operational disruption to a systemic crisis (ESRB, 2020a). The review identified a gap in the macroprudential toolkit that could help authorities mitigate the effects of the cyber incident spilling over from an operational to a financial level, thereby affecting confidence in the financial system. While the later stages of a systemic cyber crisis can resemble a more traditional financial crisis and can therefore be mitigated using traditional financial tools (like capital buffers, moratorium powers and ad hoc bank holidays or central bank liquidity provisions), any impairment of the financial system's operability remains unaddressed. Furthermore, the effectiveness of traditional crisis management tools could depend on the extent to which financial institutions, financial market infrastructures, authorities and central banks are still in operation (ESRB, 2023). Lastly, underinvestment in cybersecurity and threat intelligence as well as a significant capability gap and skill shortage add an additional layer of complexity to an effective response to a cyber crisis.

**Complementing the analysis of financial macroprudential tools, this report reviews the existing operational tools that are designed to prevent and mitigate systemic cyber crises.** As the overall macroprudential strategy to foster cyber resilience is constantly evolving and its implementation is gradual, the aim of this report is to focus on the currently implemented operational tools in the ESRB's member countries. Since the use of operational tools is heavily

dependent on available information and requires a high degree of communication and coordination with other authorities or institutions, the report reviews not only the operational tools but also the information and coordination arrangements currently in place. The report is divided into three main areas. Section 2 covers the tools used to manage and share information in various jurisdictions, while Section 3 sheds light on crisis management and coordination mechanisms across the EU, at both the national and the EU level. Section 4 considers how emergency and backup systems have been implemented in various jurisdictions. The last section presents conclusions.

# 2 Information management tools

**The digital network underlying the financial system and the cyber threat landscape are both evolving constantly and are highly dynamic. This calls for policy measures that are flexible and adaptable and requires individual institutions to be vigilant at all times.** The legal framework instructs financial institutions to cultivate situational awareness as well as to learn and evolve.[18] In this way, structural adaptation is stimulated through constant self-observation and improvement.

**To manage future cyber crises, policymakers and financial authorities should focus on the management (gathering, processing and redistribution) of information.** Any tools dedicated to these tasks are placed in the category of information management tools in this report. Information management tools primarily lay the foundations of an analytical framework with monitoring indicators. These in turn guide the activation and evaluation of further financial and operational tools. The concrete design and the purpose of various individual tools often interlink and inform each other. For example, cyber resilience scenario testing, CyRST (ESRB, 2023), is a specific tool that tests the capacity of the financial system to support the continuity of key economic functions in the event of severe cyber incident scenarios. By contrast, cyber maps have a broader scope and can be used to inform more specific tools like CyRST.

**Cyber maps can help authorities identify the main nodes of systemic importance and develop a perspective on concentration and contagion risk.** Cyber mapping defines the main links between financial sector entities, technology providers and technology solutions as well as the tolerances for disruption. The development of cyber maps is at the core of the Basel Committee`s principles for operational resilience.[19] Cybercartography consists of two networks, the financial network and the network of ICT dependencies and providers, which are intertwined in a single map. Several national central banks have already started developing cyber mapping tools (ESRB, 2022a), but there are still numerous challenges to their wider introduction. Apart from the lack of comprehensive and timely data on operational linkages and common exposures, the main challenge for these tools is to strike a balance between granularity and usability as well as to define tolerances across the entire financial system.[20]

**The digital network underlying the financial system results in interdependencies that extend far beyond its sectoral and geographical boundaries. As a consequence the relevant information is distributed across the digital network.** The integration of information resources at the European and the national level and across sectors provides valuable insights into patterns of current threats and vulnerabilities. At a national level numerous public and private initiatives focusing on risk identification, cyber incident reporting and threat intelligence sharing are already

[18] See, for example, Article 13 of the **Digital Operational Resilience Act**.

[19] See BCBS (2023), **Supervisory newsletter on the adoption of POR and PSMOR**.

[20] The ESRB has already started working on defining systemic impact tolerance objectives (SITOs). See ESRB (2023), **Advancing macroprudential tools for cyber resilience**, February, where the elements are set out that authorities should consider when defining SITOs.

established. This section reviews these information-sharing fora, identifying the benefits and challenges.

## 2.1 Information sharing at (supra-) national level

**Almost all Member States have fora in place where they can share information on cyber incidents, threat intelligence and cybersecurity in. Such fora are usually established as public private partnerships (PPPs).** While effective information management is a major focus of policymakers and financial authorities, this does not mean that the orchestration of information within the system is only the responsibility of authorities. In most jurisdictions there are several, sometimes overlapping, fora dedicated to this task. Most of these are based on the active participation of the private sector, given that they are established as PPPs.[21] Those fora exist in parallel with regulatory incident reporting by supervised financial institutions and are not a substitute for bilateral communication between individual institutions and authorities. Also in place, but significantly less common, are networks comprising only public institutions.[22] Bilateral, situational communication between authorities and other public institutions (e.g. between national cyber authorities and finance ministries) is more common.

**Fora are in place at a sectoral and a cross-sectoral level. Most frameworks have a national scope while some span across borders.** Most tools are specific to cyber risk but there are some that refer more generally to operational risk and include cyber risk.

**Some examples are as follows.**

- **The European Financial Institutes – Information Sharing and Analysis Centre (FI-ISAC).**[23] Information sharing and analysis centres (ISACs) are non-profit organisations that provide a central resource for gathering information on cyber threats (in many cases to critical infrastructure), allowing the two-way sharing of information between the private and the public sector with regard to root causes, incidents and threats, as well as experience, knowledge and analysis.[24] ISACs are a specific form of PPP. Each industry sector is free to set up its own ISAC. The FI-ISAC comprises country representatives from the financial sector, national computer emergency response teams (CERTs, i.e. GovCerts) and law enforcement agencies. Other organisations represented are the European Union Agency for Cybersecurity (ENISA), Europol, the ECB, the European Payments Council and the European Commission.

---

21 A PPP is a long-term agreement/cooperation/collaboration between two or more public and private sectors. See ENISA (2018b), **Public Private Partnerships (PPP) – Cooperative models**, February.

22 An example of this is the German **Cyber-AZ**. The Cyber-AZ is a cross-sectoral cooperation, communication and coordination platform of German (security) authorities and other institutions that deals in particular with cyber issues of national relevance. At present, the organisations involved in the Cyber-AZ include the Federal Office of Civil Protection and Disaster Assistance (BBK), the Military Counterintelligence Service (BAMAD), the Federal Office for Information Security (BSI), the Federal Office for the Protection of the Constitution (BfV), the Federal Criminal Police Office (BKA), the Federal Intelligence Service (BND), the Federal Police Headquarters (BPOLP), and the Cyber and Information Domain Service (KdoCIR) of the German armed forces as core authorities, along with the Customs Investigation Bureau (ZKA) and the Federal Financial Supervisory Authority (BaFin) as associated offices. The involvement of other relevant institutions, which include representatives of law enforcement agencies as well as relevant authorities at federal-state level, is currently being tested.

23 Further information can be accessed on the **ENISA website**.

24 See ENISA (2018a), **Information Sharing and Analysis Center (ISACs) – Cooperative models**, February.

- **The Nordic Financial CERT (NF CERT).**[25] The Nordic Financial CERT (NF CERT) is a non-profit organisation, governed and funded by its members in the Nordic financial industry. Most of the critical financial infrastructure in Norway, Denmark and Iceland and nearly all of the critical financial infrastructure in Finland is part of the NF CERT network. In Sweden the main financial institutions are in the process of becoming part of the community. The financial authorities, such as the Danish and Norwegian Finanstilsynet, are not formal members although they are part of the trusted community. NF CERT aims to connect its members with a broad external network comprised of Nordic stakeholders and international organisations in the areas of threat intelligence, incident response, anti-fraud, law enforcement and governmental bodies. The purpose of the NF CERT is to strengthen the Nordic financial industry's resilience to cyberattacks by enabling Nordic financial institutions to respond rapidly and efficiently to cybersecurity threats and online crime.

- **Cyber Information and Intelligence Sharing Initiative (CIISI-EU).**[26] CIISI-EU is a market-driven initiative focused on financial infrastructures. It comprises pan-European financial infrastructures, central banks (in their operational capacity), critical service providers, ENISA and Europol, as represented on the Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB). Authorities, in their capacity as regulators, overseers and/or supervisors, are not part of the CIISI-EU community and regulatory reporting on cyber incidents and data breaches are outside the scope of information and intelligence sharing within the CIISI-EU community. The core objectives of CIISI-EU are (i) to protect the financial system by preventing, detecting and responding to cyberattacks, (ii) to facilitate the sharing of information, intelligence and best practices between financial infrastructures, and (iii) to raise awareness of cybersecurity threats. The CIISI-EU model has also been adopted at the national level in a number of Member States, for example Ireland through CIISI-IE, a national version of CIISI-EU.[27]

- **PPPs at a national level** are for example:

    - **CERTFin**[28] is the most important sectoral cybersecurity cooperative body in Italy and is promoted by the Bank of Italy and the Italian Banking Association. Members contribute to the activities of CERTFin (CERT Finanziario Italiano) on a voluntary basis, on payment of an annual fee and according to their technical, organisational and security capabilities. The largest operators join the virtual team, which can be activated by any member and offers services to members. CERTFin provides financial operators with services related to intelligence, information sharing, awareness or support in the event of an emergency. Members participate in test, exercise and simulation sessions organised by CERTFin and guarantee the active participation of representatives from their organisation.

---

25 See the **NF CERT website**.

26 See the Euro Cyber Resilience Board Secretariat (2020), **Cyber Information and Intelligence Sharing Initiative (CIISI-EU)**.

27 For further information on CIISI-IE see the **Central Bank of Ireland website**.

28 For further information see the **CERTFin website**.

- **The Paris Resilience Group**[29] in France includes all major French banks and market infrastructures as well as the French financial authorities and some state services. The Group is chaired by the Banque de France and serves a dual purpose. In normal circumstances it aims to strengthen the operational resilience of the French financial sector by improving its ability to withstand an exogenous shock that could affect its critical functions (financing the economy, liquidity management, market operations, payments, etc.). In times of crisis, however, the group facilitates information sharing and coordination for members so they are able to continue to perform their critical functions and bounce back. For insurance and smaller banking entities the French Prudential Supervision and Resolution Authority (ACPR) has just implemented a new framework (**Protocole de gestion de crise cyber**).

- **The Financial Sector Cyber Collaboration Centre**[30] (FSCCC) in the United Kingdom was founded in 2019. It currently includes around 40 firms but will eventually extend across the financial sector. Although it is a private initiative its establishment was supported by the financial authorities. Furthermore, the FSCCC works alongside the UK Government and the National Cyber Security Centre (NCSC). The FSCCC supports intelligence sharing and incident response across the UK finance sector and aims to improve overall sectoral resilience.

**Some authorities and private institutions also engage in information-sharing initiatives of global scope**. These include the **Global Cyber Resilience Group** (GCRG)[31], which is a forum in which the chief information security officers of central banks discuss both strategic and tactical resilience objectives. 57 central banks participate, as of 2022. **FS-ISAC** (Financial Services Information Sharing and Analysis Center)[32] is a global, member-driven non-profit organisation. It is a real-time information-sharing network and aims to enhance the intelligence, knowledge and practices of its members. At the time of writing about 5,000 firms participate from 75 countries.

## 2.2 Structures for information management

**To collect and distribute cyber information within the system, information-sharing fora build on active contributions from members to create collective intelligence.** Although individual initiatives may differ, they all serve the overarching goal of creating a holistic picture. The aim of information-sharing networks is to bring as much decentralised information together as possible and to process it in a way that allows tailored information to emerge. This prevents bottlenecks from arising from an overflow of information for single participants and ensures knowledge is allocated effectively.

**Information can be managed within the network in different ways. The management of information can be intermediated by a dedicated body or, alternatively, information can be exchanged directly between members within the network.** The latter may be in the form of a

29 For further information see the **Banque de France website**.

30 For further information see the **FSCCC website**.

31 See BIS (2023), **Annual Report 2022/23**, May.

32 For further information see the **FS-ISAC website**.

bilateral exchange or a simultaneous direct exchange between several members. In many information-sharing fora both mechanisms are deployed.

**Figure 2 below shows one example for the intermediated management of information in the case of CIISI-EU network operations.**[33]

1. On a contractual basis, members actively provide input (e.g. in the form of first-hand data such as incident reports or data from other useful sources such as third-party threat intelligence).

2. The information is pooled in the network, in this case via the Malware Information Sharing Platform (MISP), which is an open-source threat intelligence platform for sharing cyber security information. The platform is funded by the Computer Incident Response Centre Luxembourg and the EU.[34]

3. The information is then filtered, combined with external sources and processed to deliver several specific outputs. This task is fulfilled by a third-party cyber threat intelligence provider.

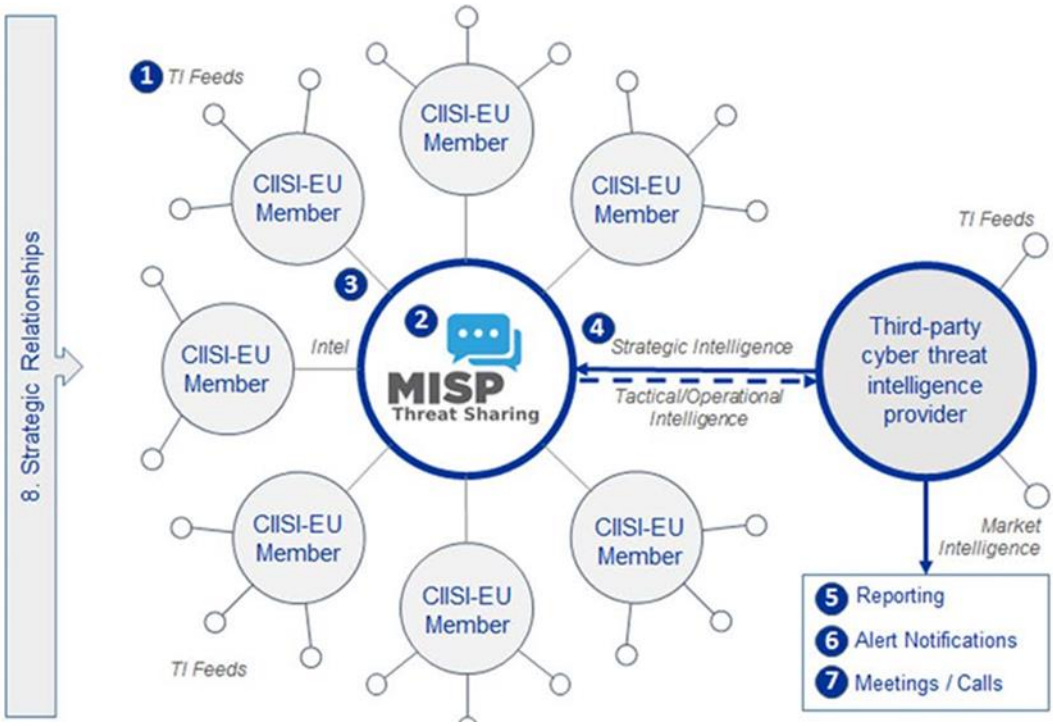
4. The output of the network consists of the transmission of situation-specific information to the individual members. This includes strategic intelligence, monthly dashboards and biannual reports at board level, as well as alert notifications.

[33] See **Euro Cyber Resilience Board Secretariat** (2020).

[34] For further information see the **MISP website**.

Figure 2

**CIISI-EU network operations**




*Source: Euro Cyber Resilience Board Secretariat (numbers refer to descriptions in the CIISI-EU report).*

Another example for the intermediated management of information is provided by **CERTFin.** CERTFin has an operational directorate which gathers all sources of information both from members and from external sources. Members share information on cybersecurity events, threats, vulnerabilities, incidents and near misses detected by their security structures and deemed relevant for CERTFin. The MISP platform is also leveraged and has been fully automated since 2020. CERTFin uses a "campus" operational model in which the operational directorate coordinates a virtual team (about 11 members) which has wide experience and can offer in-depth analysis to the whole network in case of need. For example, in the case of an incident the affected member can call upon the operational directorate to activate the virtual team to provide further support. Bilateral collaboration can be drawn upon at any time.

**Collaborative structures are characteristic for many information-sharing fora. They create an environment that enables participants to interact directly with each other.** Collaboration can, for example, be initiated in specific meetings or in working groups. Through constant interaction, mutual trust increases over time, methods of communication are optimised and cooperation develops gradually and instinctively within the network. Once acquired, the internally generated knowledge is stored within the network, for example in the form of common vocabularies or cybersecurity best practices.

**Furthermore, information-sharing networks can also be linked to other initiatives.** This could be in the form of joint initiatives in specific situations, the regular exchange of expertise or strategic relationships.

Collaborative structures and interactions with other initiatives are common features of most PPPs – the following examples are non-exhaustive.

- **NF CERT** provides members with Nordic threat intelligence (e.g. in the form of quarterly situational reports, relevant warnings and notifications of incidents tailored to individual members). However, it also provides for direct information sharing among members (e.g. in regular calls and face-to-face fora). Collective learning is promoted to enable the NF CERT community to efficiently communicate and assess cyber threats and incidents (i.e. by agreeing on a common terminology, methodology and toolkit). NF CERT provides members with access to an external network comprising Nordic stakeholders and international organisations in the areas of threat intelligence (i.e. security communities such as FS-ISAC/FI-ISAC) and incident response (i.e. national CERTs, anti-fraud, law enforcement and governmental bodies). In this way, expertise is shared and members can pool the resources necessary to achieve more efficient incident and fraud detection and an improved response.[35]
- The **CIISI-EU network** is also not limited to intermediated communication. It is a trusted community where members can meet to discuss cybersecurity threats and share related information, intelligence and best practices. While it is a "closed" community, the platform is open for strategic relationships with other information-sharing communities.

## 2.3 Governance and participation rules

**National competent authorities or national cyber security bodies coordinate information-sharing fora.** In certain cases the relevant forum might be a private organisation such as NF CERT, which is a private non-profit association. These frameworks share similar participation rules, formats and primary sources/types of information that is shared and discussed among their members[36]. Approximately half of all tools are anchored in national law – others are based on contracts and a few are on a voluntary basis.

[35] See the **NF CERT website**.

[36] The term "Information" here is used very broadly and can mean that information has originated from past events (e.g. incidents such as threats, attacks and vulnerabilities, or any type of alert). In certain cases, market intelligence and media coverage can also be a source of information.

## 2.4 Identified benefits and challenges

### 2.4.1 Benefits

- **Higher overall resilience.** Information-sharing fora and incident reporting have contributed to early threat detection, enhanced situational awareness and enhanced safety among members.
- **As information sharing creates openness and trust between participating members, collective and collaborative defences in the face of cyber threats or incidents can be improved.** Over time, constant interaction increases mutual trust and improves ways of communication through which cooperation is developed gradually and instinctively from within the network. In times of crisis, miscommunication – or the failure to use common language – may lead to potential tensions between members. Close collaboration can therefore reduce tensions and conflicts of interest, and foster integration.
- **Data-driven analyses and standardisation.** Based on established severity criteria, information-sharing fora have supported authorities by gathering information and generating data. This allows authorities to assess cyber events through ex post data analyses and draw conclusions that build resilience.

### 2.4.2 Challenges

- **The effectiveness of information-sharing fora may be jeopardised if operational aspects are not standardised and streamlined.** Standardising and streamlining existing tools can be beneficial, considering how fast and severe a cyber incident can be. Unless the format, channels and language of transmitted information are standardised the information itself may contribute to confusion and pressure across all actors. However, a balance needs to be struck between standardisation and flexibility to avoid creating information-sharing bottlenecks resulting from over-standardisation and over-rigid frameworks.
- **Some tools are not sector specific.** This implies that many parties are often involved, with vastly differing objectives, frameworks, responsibilities and data protection schemes. Information needs may vary across sectors and responses may depend on how specific they need to be. If tools are not cross-sectoral by design they may fail to increase awareness of the whole value chain. The relevant authorities could play a facilitating role across sectors.
- **In certain jurisdictions there are multiple fora with a similar scope.** It could be beneficial to link the existing frameworks and formulate a shared understanding of the role of each framework. This should be done both at the national and the EU level to ensure better collaboration between members, reduce barriers and avoid costs and overlaps. Costs associated with closing existing fora should be considered and should be weighed against taking a more integrated approach.

Box 2

## The Danish approach to cyber resilience

The Danish macroprudential authority started focusing on operational and cyber risks in 2015. Danmarks Nationalbank (the Danish central bank) and the Danish financial sector established the PPP Financial Sector forum for Operational Resilience (FSOR)[37] comprising systemically important institutions in the financial sector. This includes the eight largest systemically important financial institutions, two representatives from the insurance and pension industries, four data centres that operate critical systems, three business and industry organisations (including NF CERT), six owners of critical financial infrastructures, four central authorities including Finanstilsynet (the Danish Financial Supervisory Authority) and the Centre for Cybersecurity. It is chaired by Danmarks Nationalbank, which also provides the secretariat.

Its three main areas of action are:

- strengthened sectoral collaboration and improved scope for action for individual players;
- stronger national and international collaboration with relevant stakeholders;
- increased awareness and knowledge of cybersecurity.

The forum must ensure it offers a common overview of the operational risks that may have a cross-sector impact and that could threaten financial stability. Moreover, it must decide on joint measures and ensure they are implemented.

Danmarks Nationalbank and the Danish financial sector have developed a methodology through which the sector ensures there is a common overview of sector-relevant operational risks. A risk-based approach is necessary to ensure that the most critical risks are addressed quickly and thoroughly as resources are scarce and initiatives can be very costly. The methodology is updated semi-annually and comprises four main steps.

1. Define the scope and prepare a full list of the sector's business activities. Based on this, define and map the most critical business activities including systems, networks and suppliers (and their interconnectedness).
2. Define risks based on information on historical events, threat assessments, identified vulnerabilities, knowledge of future system changes, etc.
3. Assess and classify risks in terms of probability and consequence.
4. Identify mitigation measures for the most important risks identified in point 2 above.

The analysis provides a foundation which can be used to prioritise and implement joint measures. These include:

[37] For further information on the FSOR see the **Danmarks Nationalbank website**.

- a sector crisis management plan that aims to minimise the scope and consequences of an operational crisis that could potentially threaten financial stability;
- the TIBER-DK (threat intelligence-based) programme that aims to strengthen cyber resilience and financial stability;
- a task force whose aim is to prepare the financial sector for worst-case scenarios and ensure that most critical business activities are functioning.

The above-mentioned task force will carry out ex ante analyses of the current level of resilience in the Danish financial sector and is mandated to provide concrete recommendations. These system-level tools should supplement bank and FMI business continuity in extreme conditions.

The Danish authorities are continuously working on how to recover data and systems in the case of an extreme-but-plausible scenario. One possible approach would be to map critical data at the individual and the sector levels and to develop appropriate recovery solutions. Although this is a complex and costly task the Danish financial sector agrees that work in this area should continue.

# 3 Crisis management and coordination

**The financial authorities need to build on their capabilities with regard to cooperating with other financial and cyber authorities in coordination networks.** A rapid response is required from financial institutions and authorities to mitigate the potentially negative effects of cyber incidents on financial stability. Therefore, institutions need to remember that severe incidents can and do happen and they need to be prepared to initiate crisis management plans. A cyber incident can lead to financial and liquidity crises but could evolve differently from a traditional crisis. Severe incidents can exceed the capabilities of individual institutions and can require collective solutions. Since no single authority has an overarching mandate, a collective response depends on cooperation between local authorities in regional and global networks, as well as cooperation with parties beyond those with which financial authorities interact in a purely financially driven crisis.

**Adopting a pre-crisis perspective is essential to ensuring readiness and preparedness in the event of an extreme-but-plausible cyber incident.** Coordination in the event of a cyber crisis is preceded by the use of tools that are designed to establish or improve the shared knowledge or communication base, simulate expected cooperation and, ultimately, enhance the readiness of all relevant actors. Since there is no historical precedent for a systemic cyber crisis in the financial system, decentralised efforts contribute significantly to exploring potential scenarios and testing the effectiveness of various strategies. While most coordination networks still focus on the orchestration of information, there is an increase in the number of preparedness activities relating to technical support and operational cooperation. The next section reviews operational crisis management coordination mechanisms and identifies the benefits and challenges which provide a platform to build on.

## 3.1 Operational crisis management coordination mechanisms

**A variety of coordination networks have already emerged at the international, EU and national levels and are both cross-sectoral and sectoral in scope. At the EU level, high-level coordination frameworks have been established to enable a joint response.** As cyber risk is not limited to the financial system, numerous agencies have been established and initiatives developed in parallel for action in the event of cyber incidents. Financial institutions and authorities are engaging with the relevant actors in formal or informal networks. At the EU level, EU-CyCLONe[38] provides a cross-sectoral coordination network while the EU-SCICF (see **Box 3** below) sectoral initiative aims to bridge any coordination and communication gaps between financial authorities, authorities from other sectors and other key actors at the international level. Furthermore, at the global level the G7 have established a cyber incident response protocol (CIRP).

**Most Member States have an operational crisis management and coordination mechanism in place that could be used during a severe-but-plausible cyber incident.** Some of these

[38] The European cyber crisis liaison organisation network (EU-CyCLONe) is a cooperation network for Member States' national authorities in charge of cyber crisis management. For further information see the **ENISA website**.

mechanisms are sector specific while others are cross-sectoral. Most mechanisms have a national scope while a few (NF CERT, ECB/SSM (Single Supervisory Mechanism), ECB/MIP (Market Infrastructure & Payments)) have a cross-border or EU-wide dimension. More than half of the tools are specific to cyber risk while a few refer to operational risk more generally and include cyber risk. In most Member States the authorities have “at-crisis” instruments at their disposal and most authorities also employ pre-crisis instruments.

In this report the individual tools and mechanisms are viewed through the lens of an overall strategy which can be broken down into several protocols and the interactions between various private and public stakeholders. This overall strategy is analysed from two perspectives and depicted below.

Table 1
**Overall crisis management and cooperation strategy**

| **Time**<br>**This perspective differentiates between tasks deployed before and after an incident occurs.** | **Actor (collaboration)**<br>**This perspective focuses on the collaboration of private and public actors.** |
|---|---|
| Pre-crisis tools are designed to establish and improve a base of shared knowledge and communication, simulate anticipated cooperation and, ultimately, improve the readiness of all relevant actors before an incident has occurred (e.g. by conducting testing and exercises). | PPPs foster information sharing and often feature elements of cooperation and coordination. PPPs actively perform tasks that contribute to both pre-crisis and at-crisis tools and are embedded in the overall crisis management strategies. |
| At-crisis tools enable a fast and joint response after an incident has occurred. This is to activate system-wide crisis management plans, coordination frameworks and communication channels that also take a cross-sectoral perspective. | Public institutions such as national central banks, financial authorities and ministries of finance are most often in charge of the sectoral crisis management strategy and initiate crisis plans and protocols. |

*Source: ESRB.*

### 3.1.1 Pre-crisis and at-crisis tools

**Operational tools can be divided into two categories, according to their objective. They are either pre-crisis tools that are activated in advance of a hypothetical incident (and therefore continuously and recurrently) and at-crisis tools that take effect after an incident has occurred above a certain threshold (and are therefore activated situationally), as depicted below.**

Figure 3
**Distinction between pre- and at-crisis tools**


*Source: ESRB.*

**Pre-crisis tools are the basis for at-crisis tools to be effective and foster readiness and preparedness.** Coordination in the event of a cyber crisis is preceded by pre-crisis tools that have been designed to establish or improve the shared knowledge/communication base, simulate anticipated cooperation and, ultimately, improve the readiness and preparedness of all relevant actors. Moreover, some authorities employ information-sharing tools to increase awareness and reduce the exposure to or impact of a crisis. Their primary focus is to exchange information on cyber incidents among their members, collect data, run exercises and, overall, work pro-actively in case of a cyber threat.

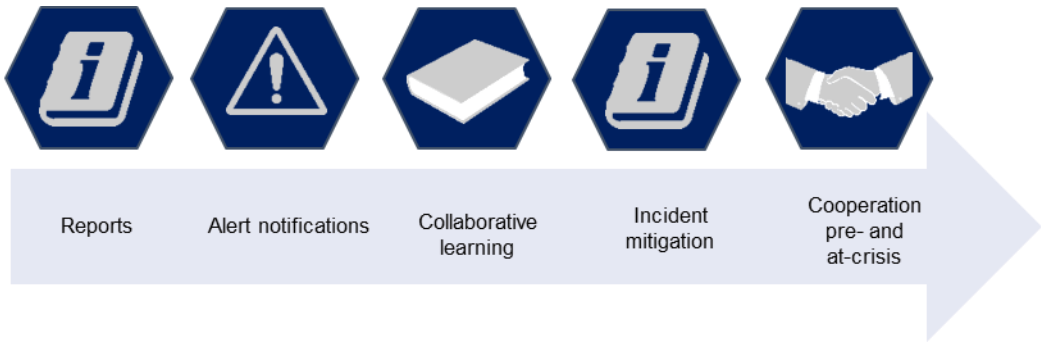
**At-crisis tools are key to a collective and efficient response.** At-crisis tools are not exclusively those tools concerned with the response capacities of institutions. They also include, from a macroprudential perspective, system-wide crisis management plans, coordination frameworks and communication channels that take a cross-sectoral perspective. Some at-crisis tools are based on internal procedures for decision-making and escalation while others have a dedicated unit that leads crisis management and coordination.

### 3.1.2 Public private collaboration

**Public private partnerships (PPPs) play an important role both before and after an incident.** PPPs often have elements of both cooperation and coordination (see **Figure 4** below). They expand their services actively to create a more holistic model and engage not only in information sharing but also actively in handling cybercrime and responding to threats in a coordinated manner. PPPs sometimes even offer tailored assistance to individual members in the case of a cyber threat.

Figure 4

**Typical outputs and services provided by PPPs**




*Source: ESRB.*

**Some examples of PPPs are as follows.**

- The **NF CERT** is not limited to the exchange of information. As a collaborative initiative, it allows members to work together when handling cybercrime and responding to threats in a coordinated manner. This also includes coordinating responses in the case of an incident as well as assisting in cyber threat and online crime mitigation activities (using resources in the network).
- **CERTFin** has expanded from offering a basic set of services to offering a wider set that could also be enriched in the future. Besides sharing relevant information CERTFin also provides support in emergencies or during regular exercises and testing. CERTFin is the coordination hub for its members and is at the forefront of any relations with other bodies/authorities on behalf of its members (e.g. with the National Cybersecurity Agency, the Postal Police, the authorities at cross-sector level etc.).
- The **Paris Resilience Group's** operational services range from activities aimed at raising operational risk awareness to concrete initiatives enhancing members' individual and collective preparation for crisis response (notably via the organisation of large-scale crisis simulation exercises).

**PPPs play a particularly important role in the areas of pre-crisis tools and lower intensity incidents.** Incidents that only affect individual participants can potentially be resolved through collaboration within the PPP, without the need for the authorities to take extensive action.

**Public-private information-sharing frameworks collaborate with policymakers and authorities and participate in the development and calibration of pre-crisis tools, especially those used in cyber exercises and testing.** The knowledge generated within PPPs can provide important input for cyber exercises and testing. The intelligence from threat landscape reports provides a valuable basis for designing threat-led scenarios in TIBER tests (threat intelligence-based tests). These will be mandatory for certain institutes under DORA – more active participation

models are also conceivable. CERTFin, for example, led the REDFin[39] project and has developed guidelines on scenario drafting for threat-led penetration testing (TLPT). Moreover, PPPs also support or initiate tests and exercises among their membership.

**Collaboration between public and private actors has further potential. European initiatives, such as ENISA's biannual European cyber exercise, should be tailored to the financial sector and regularly conducted between all relevant financial institutions and supervisors.** Exercises at the EU level and with third-party countries are also intended to form a core element of the EU-SCICF when it is in place. The overall learning through these tabletop exercises should be enormous since they prepare the entire system on a systemic scale (instead of just at an individual institutional level) for severe-but-plausible cyber incidents. These exercises simulate real challenges that involve decision-makers and help them to identify missing links in their response and recovery plans.[40] These exercises could prove to be very useful if they are coordinated across all European authorities. It would facilitate the development of orderly communication channels and would foster collaboration and resilience.

**How exactly collaboration between private and public actors is organised after an incident has occurred depends on protocols and coordination agreements. Such at-crisis tools are widely used across the EU.** At an EU-wide level, communication and crisis coordination tools are deployed through the Cyber Incident Emergency Process (CIEP) of the SSM, the Oversight Crisis Coordination Framework (OCCF) of the ECB, and the EU-SCICF planned as part of DORA implementation. National competent authorities and financial institutions are also included.

**At a national or a supra-national level, sophisticated PPPs play a key role in activating specific crisis frameworks and mechanisms. Ultimately, national central banks or finance ministries take the lead on mechanisms at the sectoral level**. The networks will continue to contribute extensively in a supporting role – PPPs often offer valuable advice to the relevant authorities in this case and assist in coordination actions.

**The following non-exhaustive examples provide an illustration.**

- **CERTFin** is the coordination hub for its members in Italy. In case of a crisis, **Codise** oversees crisis management and coordination. It is chaired by the Banca d'Italia and includes representatives of CONSOB (the Italian national commission for listed companies) and the systemically important financial institutions (i.e. banks, financial market infrastructures, central securities depositories, central counterparties, trading venues and critical service providers). Codise's role is to coordinate crisis management in the Italian marketplace for all types of operational incident, including cyber incidents. It serves (i) to facilitate the exchange of information, (ii) to facilitate the adoption of measures needed to deal with events that may be putting the system's business continuity at risk, (iii) to maintain the smooth functioning of financial infrastructures and, (iv) to maintain public confidence in money. Interventions depend

[39] The Readiness Enhancement to Defend Financial sector – REDFin project is geared towards enhancing the defences of the European banking and financial sector by establishing innovative methods for analysing and preventing cyber risk. Further information is available on the **website** of ABI Lab, the coordinator of the project.

[40] See Krüger, P. and Brauchle, J.-P. (2021), **The European Union, Cybersecurity, and the Financial Sector**.

on the type of event, its extent and its potential impact on the financial system. CERTFin offers technical support to Codise.

- **FSOR Crisis Management** in Denmark is another example. Financial organisations report incidents to NF CERT and CIISI-EU (provided they are members) and to the Centre for Cybersecurity. If incidents are assessed as relevant at a sectoral level the sector's crisis management initiative (the Financial Sector Forum for Operational Resilience, FSOR) is contacted, as prescribed by the crisis management plan. This is a sector collaboration hosted by Danmarks Nationalbank, the aim being to enhance operational resilience in the Danish financial sector.

- **The Paris Resilience Group** remains in control in France. In the case of an incident, members meet within a dedicated structure, the coordination unit, to assess the situation, share information and take collective decisions where relevant. The group is chaired by the Banque de France and is supported by three crisis units: liquidity, cash and communication. These crisis units comprise professionals from both the private sector and Banque de France. The French financial authorities and state services are also members of the Paris Resilience Group – as such they participate in crisis calls and contribute to information sharing.

**In the United Kingdom, by contrast, the private sector plays a leading role during a crisis.** The **Sector Response Framework (SRF)** provides the mechanism for UK response groups to coordinate during an incident. It is a voluntary framework agreed as part of the UK collective action approach (the Cross Market Operational Resilience Group or CMORG), rather than on a contractual basis. The SRF is composed of several response groups, owned and operated by industry. For the private sector, the most strategic SRF group is the Cross Market Business Continuity Group (CMBCG), chaired by the Bank of England. The primary cyber response group is the FSCCC, which shares information during incidents. Response groups within the SRF are responsible for maintaining their own capabilities and coordination links with the wider framework. The SRF is designed to be modular so that its cyber-focused groups can be activated as required during a cyber incident, while non-cyber groups need not be called on. The authorities also have a response framework (the Authorities Response Framework) which is used to coordinate actions between the finance ministry, the central bank and the regulators. It is joined by the NCSC and other government entities including law enforcement for cyber incidents and the Information Commissioners Office (ICO) for data breaches.

**The success of collaboration between private and public parties when an incident has occurred depends heavily on effective communication. At-crisis communication can be depicted by and described in three layers.** This structure, which is described below and depicted in **Figure 5**, may differ slightly from organisation to organisation.[41]

1. **The first level is tactical** and is where initial action is taken (e.g. IT teams restore systems, markets teams analyse how much liquidity may be needed and briefings are provided to other parts of the organisation). These teams establish communication lines to third parties and employees at other authorities with relevant technical capabilities, as well as internal

[41] See ENISA (2016), **Strategies for incident response and cyber crisis cooperation**, August. For the application of the structure to communication between the Member States and EU institutions, bodies and agencies see ENISA (2024), **Best Practices for Cyber Crisis Management**, February.

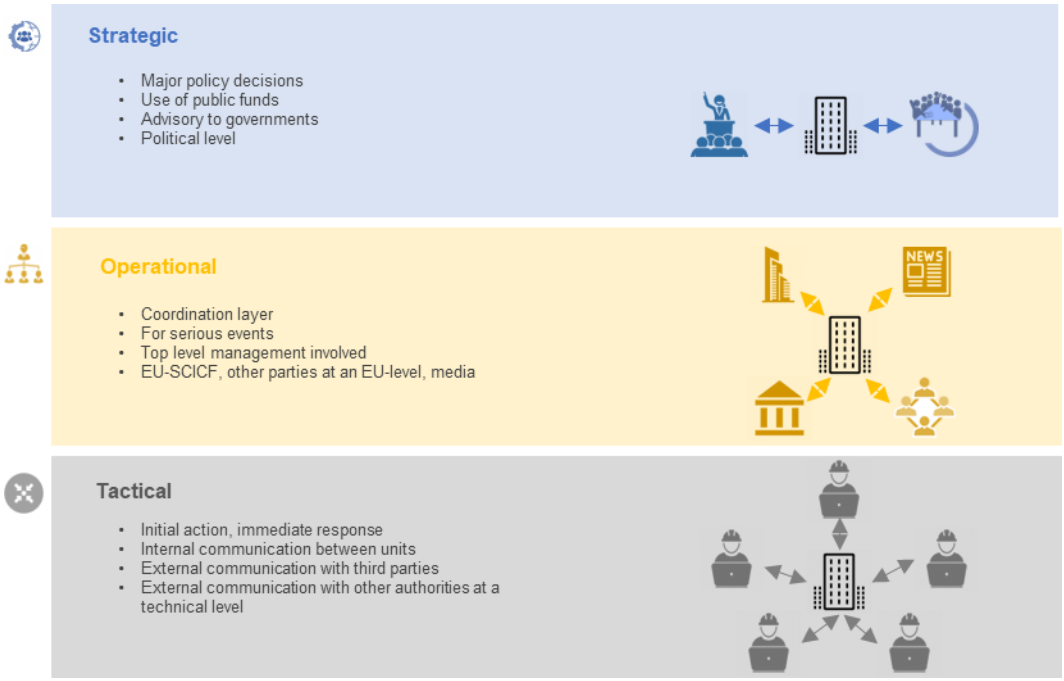
communication between relevant units. The main actors at the tactical level are computer security incident response teams (CSIRTs).

2. **The second level is operational** and is where (macroprudential) coordination is initiated and management informed. This level has the main responsibility for coordination in a crisis. It is activated quickly for serious events and entails crisis preparedness and contact with higher-level officials at other authorities (including other central banks), with other coordinating bodies and with the media. At this level, EU-wide frameworks such as the EU-SCICF may be activated (see also **Box 3** below on EU-SCICF and its interplay with DORA and NIS2[42]).

3. **The third level is strategic** and deals with major policy questions such as changing liquidity policies and coordinating with the Government and advising it on major policy issues such as use of public funds. This level is particularly important for pan-European incidents where high-level EU crisis management mechanisms (such as the Integrated Political Crisis Response) may be triggered.

Figure 5

**Schematic overview of at-crisis communication**




*Source: ENISA and ESRB.*

[42] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80.)

**PPPs contribute to the overall strategy via the development of best practices as follows.**

(a) Conducting both information sharing and crisis coordination activities (NF CERT and the Norwegian Financial Infrastructure Crisis Preparedness Committee).

(b) Putting specific arrangements in their operating model into place (Italy's Codise and its integration with the Italian CERTFin). In situations of "at-crisis", CERTFin can propose the activation of Codise and can provide Codise with technical support on request. Codise is in charge of coordinating operational crises at the national level. Participants take part in regular information-sharing calls, awareness sessions and training, and participate in governance bodies on a rotation basis.[43]

(c) Coordinating with cross-sector bodies (Danish FSOR crisis management, see **Box 2**).

(d) Structuring the organisation in a modular way and acknowledging the industry's leading role (the UK SRF).

## 3.2 Legal basis for existing mechanisms

**Many coordination mechanisms are based on legislation and are mandatory.** Crisis and coordination mechanisms may have been developed specifically at the national level or may be based on international standards. Most crisis frameworks are based on legislation and are mandatory. For instance, participation in Italy's Codise is legally compulsory for all financial operators that have been identified as systemically important by the Banca d'Italia. During a crisis PPPs, which operate on a contractual basis and are governed by members, can, however, also play critical supporting roles. PPPs like the Paris Resilience Group, in which the authorities play more active roles, may even remain in control during a crisis. It is also common for coordination frameworks to be based neither on contractual agreements nor on legislation. The CIISI initiatives at the EU and the national levels are voluntary initiatives that do not have a legal basis.

**The use of coordination tools is mostly governed by internal procedures.** Authorities can develop their own protocols to govern specific aspects of managing cyber crises. This is the case for the Paris Resilience Group, for major banks and market infrastructure's cyber resilience and for ACPR's Protocole de gestion de crise cyber in the case of insurers and smaller banks. Two other mechanisms in this category are voluntary or display mixed characteristics, such as the Danish FSOR crisis management which has voluntary participation with binding membership and the UK's SRF, a voluntary and industry-driven framework which responds to systemic incidents in a coordinated manner.

## 3.3 Governance and participation rules

**Typically, authorities' roles in the financial system also govern their role in the mechanism.** When mechanisms are at the sectoral level (mainly at the financial sector level), the national central

[43] See the **CERTFin website**.

banks or the finance ministries are typically in charge. For instance, Italy's Codise is chaired by the Banca d'Italia and includes representatives of CONSOB and systemically important financial institutions, central depository systems, central counterparties, trading repositories and other institutions that are considered significant by Banca d'Italia. The tools with EU-wide scope are managed by the respective supra-national organisations (i.e. ECB/SSM, ECB/MIP and the Single Resolution Board). All competent authorities participate if they have a relevant mandate.

**Tools based on contracts and voluntary arrangements are owned and operated by their participating members.** For instance, the UK's SRF is maintained by a permanent sub-group that includes representatives from various response groups among its members. Response groups within the SRF are responsible for maintaining their capabilities and coordinating links with the broader framework.

## 3.4 Identified benefits and challenges

Most of the tools have the same benefits and issues. The benefits of crisis management coordination frameworks for cyber incidents include improved collaboration, coordinated responses, timely incident handling and effective information sharing. However, difficulties may arise from the complex and rapid nature of cyber incidents, the need for cross-sectoral coordination and challenges relating to resource availability and speed of response.

### 3.4.1 Benefits

- **Fast collaboration and information sharing for decision-making**. A well-defined crisis management framework enables the units responsible to exchange relevant information effectively and to collaborate efficiently during cyber crises.
- **Agreed procedures and actions for more organised responses**. The presence of agreed procedures, contacts and action plans is crucial when there is little time for decision-making. Having a pre-established framework in place allows for more organised and efficient responses.
- **Improved coordinated and effective responses for financial stability**. The existence of a dedicated forum for different stakeholders facilitates a coordinated approach to handling cyber incidents. It also allows for efficient responses to incidents that have the potential to impact financial stability by bringing together relevant teams from different sectors (e.g. financial risk, recovery and resolution, etc.).
- **Identification of unaddressed problems**. The crisis management coordination framework can help to identify issues that individual members may not have addressed in their crisis management plans.
- **Preparedness through exercises and stakeholder engagement**. Some frameworks include exercises and engagement with stakeholders, helping them to be better prepared to handle actual crises.

### 3.4.2 Challenges

- **Subjectivity in defining a cyber crisis**. One of the challenges during the implementation of crisis management frameworks is the subjective nature of defining a cyber crisis. Objectively quantifying and classifying cyber incidents as crises can be challenging. Expert judgment is crucial in determining when to activate the crisis management process, which may lead to delays or confusion in initiating the appropriate response.

- **24/7 availability and rapid responses to cyber incidents**. Unlike other types of crisis, cyber incidents can happen at any time and their severity can escalate rapidly. Having resources available 24/7 to identify incidents, assess their severity and inform stakeholders promptly poses a significant challenge and requires robust coordination and (possibly) automated mechanisms.

- **Complexity and insufficient resources when handling cyber incidents**. Shortages of skilled cybersecurity experts can pose challenges to responding adequately to large-scale cyber incidents. Cyber crises may pose additional layers of complexity as they can transform into full-scale financial crises and may further exacerbate risk.

- **Communication and integration challenges**. Despite the benefits of coordination, difficulties may arise in fully defining communication channels and ensuring there is effective integration between the various teams, sectors and regulatory frameworks.

- **Complexity of response processes**. Response processes can be complex, particularly in the case of incidents involving multiple groups which have overlapping areas of focus and which share information. This complexity may pose challenges to streamlining and managing responses efficiently.

- **High expectations for speed of response and adaptability**. Cyber incidents often develop and spread rapidly, demanding immediate action. Crisis management mechanisms designed primarily for financial and operational crises might need to be more agile to cope with the speed at which cyber incidents evolve.

Box 3

## ESRB Recommendation to establish a pan-European systemic cyber incident coordination framework (EU-SCICF)

In 2021 the ESRB, recognising a gap in crisis coordination frameworks, recommended European supervisory authorities (ESAs) to start preparing for the gradual development of an effective EU-level coordinated response in the event of a cross-border major cyber incident or a related threat that could have a systemic impact on the Union's financial sector. The ESRB recommended establishing the pan-European systemic cyber incident coordination framework (EU-SCICF).

The EU-SCICF should build on the Digital Operational Resilience Act (DORA) for the financial sector and should complement existing frameworks (e.g. financial and cyber incident) as well as the Network and Information Security (NIS2) Directive and the Resilience of Critical Entities Directive (CER).[44] It will also consider the interplay between operational disruption (including mitigants and financial stability) and relevant macroprudential tools.

The swift coordination and communication required, and bridging coordination and communication gaps between the relevant authorities at the Union level, will make it possible to:

- make an early assessment of a major cyber incident's impact on financial stability;
- coordinate properly and develop a clear action plan, if required, among the financial authorities involved in planning a coordinated response to a major cyber incident;
- maintain confidence in the financial system;
- limit contagion across the financial sector.

The EU-SCICF will contribute to preventing a major cyber incident from becoming a risk to financial stability. It also establishes a list of designated points of contact for the ESAs, the ECB and each Member State.

[44] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (OJ L 333, 27.12.2022, p. 164.)

# 4 Emergency and backup systems

**A new set of macroprudential tools, aimed at ensuring the provision of critical economic functions even in the worst cyber incident scenarios, could help to address systemic cyber risk.** A technological disruption due to a cyber incident may result in the loss of availability of a critical service and/or the loss of the confidentiality, integrity or reliability of data underlying a critical service. This in turn could affect the delivery of an important economic function. In the worst-case scenario the initial shock spills over from the operational channel to the financial and confidence transmission channels and is amplified through feedback loops. Although traditional macroprudential tools for financial resilience contribute to the financial system's loss-absorbing capacity, the corresponding tools are applied relatively late in the case of cyber crisis mitigation.[45] A new set of macroprudential operational tools could fill this gap by ensuring the provision of critical economic functions, even in severe cyber incident scenarios.[46] Such tools could build the foundations for an environment in which traditional financial tools can be implemented. For instance, if a major bank needs to be resolved, the necessary bail-in tool cannot be applied if the underlying data are corrupted. In this case, a backup solution would be needed in advance to retrieve uncorrupted data.

**Macroprudential tools, such as emergency and backup systems, enhance operational resilience. They take effect after an incident has occurred and are intended to limit the consequences at the systemic level.** When a severe incident occurs the response and recovery capabilities of individual institutions take effect. Measures covered by current legislation are in place at this level and typically aim to provide capacity or backup systems. [47] While such measures contribute to the ability of the institution to restore itself, it must nevertheless be assumed that certain critical services will be temporarily unavailable. Whether key economic functions are affected is likely to depend on how well other institutions are able to mitigate the disruption. Joint action will also likely benefit from the coordination frameworks in place. Large-scale outages, however, can exceed sector-wide compensation capabilities. In such cases additional backup capacities in the form of special emergency systems could ensure the provision of certain key economic functions.

**The authorities should focus on helping institutions to adapt their response and recovery mechanisms to match the speed of the threat landscape. At the sectoral level collective solutions should be analysed.** The promotion of research and development initiatives targeting further operational solutions, such as data vaults, could help to keep pace with the evolving threat landscape. At the sectoral level, the active development of infrastructures should be continued. This section is aimed at supporting the authorities in these tasks by providing a stocktake of current national initiatives.

---

45 ESRB (2022b), **Review of the EU Macroprudential Framework for the Banking Sector**, March.

46 ESRB (2023), **Advancing macroprudential tools for cyber resilience**, February.

47 Article 12 DORA contains provisions on "Backup policies and procedures, restoration and recovery procedures and methods", which are specified in Regulatory Technical Standards and will be applicable from 17 January 2025 onwards. This provides for the harmonisation of the currently fragmented regulatory landscape.

## 4.1 Systems supplementing business continuity

**Responding to a large-scale systemic cyber incident may require emergency systems that individual financial institutions alone cannot cater or prepare for.** Operational risk can materialise in many ways and financial institutions have a need to ensure business continuity. In addition to business-related preparedness needs, institutions in the financial sector face regulatory requirements set by national and EU bodies which oblige them to mitigate operational risks by taking adequate measures. For example, a bank must have its own backup arrangements in place for important operations. Market infrastructures such as clearing houses[48] or systemically important payment systems are required to implement measures such as an alternative data transmission channel or a secondary operations centre that can be activated if the primary centre is unavailable.[49] A major disruption can affect several actors directly or a serious incident affecting a single actor can impact other actors through contagion channels.[50]

**System-level tools that respond to the realisation of a risk have only been introduced in a few countries.** The systems that have been introduced vary substantially in terms of implementation, coverage and the scenario they can be used for. For example, in Norway the backup system for the national payment card scheme can be used for payments made for goods and services in situations where the payment infrastructure is not operating normally.[51] In Finland, a backup system ensures that citizens and companies retain access to funds on their accounts and that they can use the most important daily payment tools (see **Box 4**). Both solutions only function at the national level.

**Central bank digital currencies (CBDCs) could increase the resilience of payment systems.** Outages of traditional card payment schemes and cash withdrawals following cyberattacks could affect retail payments and could erode trust in the financial system.[52] To withstand extreme incidents, CBDCs should be widely available and should be transacted via secure and resilient channels. Moreover, the overall resilience of the payment system may be improved through reliance on its own underlying infrastructure.[53] However, it is difficult to estimate the feasibility and efficiency of a CBDC emergency system without knowing its technical design characteristics, the core members in the value chain and the quantity restrictions that may be set for financial stability reasons.

## 4.2 Data vaulting

**Only a few technical mitigants exist that reduce risks when data integrity or availability cannot be guaranteed.** Incidents affecting confidentiality can be addressed via prevention

---

48 See ESMA (2022a), **Report on 4th ESMA Stress Test Exercise for Central Counterparties**, July.

49 For a system-wide view see ESMA (2022b), **TRV Risk Analysis - A framework to assess operational resilience**, December.

50 For more details of amplification channels see Figure 2 in ESRB (2020), **Systemic cyber risk**, February, and Ros, G. (2020), "**The making of a cyber crash: a conceptual model for systemic risk in the financial sector**", *Occasional Papers Series*, No 16, ESRB, May.

51 See ESRB (2023), **Advancing macroprudential tools for cyber resilience**, February.

52 See ECB (2020), **Report on a digital euro**, October.

53 See ECB (2023), **A stocktake on the digital euro**, October.

measures such as authentication and zero-trust access procedures as well as cryptographic standards, while incidents affecting availability can be mitigated by functioning backup systems. The second-order effects of data integrity-related incidents are especially significant.[54] Data vaulting procedures can protect against ransomware attacks which cause a loss of confidence in the consistency, accuracy and trustworthiness of data.

**Data vaulting is an established solution that can act as a fail-safe way to restore critical data.** The ESRB has concluded that the loss of confidence in the integrity of data could in itself trigger a systemic event if the impact was large enough.[55] In a data vault companies create backups of critical data at regular intervals, in a standardised format. The data can be backed up by the companies themselves or by other firms, or they can be centralised by an entity. The vault must be encrypted and kept entirely separate from the business's infrastructure so it cannot be subsequently tampered with.

**The US not-for-profit initiative Sheltered Harbor set the standards for data vaulting, resiliency planning, testing and recovery.** After each participating institution had vaulted its data it received a certificate from the initiative. It is worth noting that the data are stored neither with Sheltered Harbor nor on the same platforms as the data used by institutions in their day-to-day business: they serve merely as a form of attestation. The initiative is primarily microprudential in nature, although the distinction between microprudential and macroprudential tools becomes increasingly blurred if enough entities participate in the initiative.

**For a tool to be far reaching and effective and for it to be seen as a macroprudential policy tool, smaller entities need to be integrated.** Larger entities have more incentives and ways to participate in a system such as that proposed by Sheltered Harbor. Given the amount of time, effort, expertise and funding required, it may be necessary to employ PPPs and provide financial and technical support in order to create incentives to integrate smaller entities. Rising risks of ransomware attacks create externalities – these could cascade into wider societal costs that could be internalised by PPPs. Furthermore, given the financial system's inherent complexity a centralised system may be more difficult to establish than distributed and certificate-led initiatives.

**In the banking industry, vaulting could also be based on deposit guarantee data and a specific, dedicated restoration platform.** Deposit guarantee data on their own are limited to restoring account balances only but data could be enriched by adding more information, depending on need. For example, financial positions against FMIs and counterparties might be needed to restore operations in the interbank market. An example of extended deposit guarantee data-based vaulting can be seen in the Finnish contingency system.

## 4.3 Governance and participation rules

**For emergency systems to be effective in ensuring there are no systemic effects following an incident, all (or at least most) of the significant parties must be involved.** An emergency

[54] See Maurer, T. and Nelson, A. (2020), **International Strategy to Better Protect the Financial System Against Cyber Threats**.

[55] ESRB (2020), **Systemic Cyber Risk**, February.

system requires an operator and participants that are committed to using the system. The operator develops the system and maintains its readiness for use while the participants make the adjustments to their business processes and systems that are required for them to use the backup system. Participation may be voluntary, with parties committing to using the system in participation agreements. However, private institutions may have insufficient incentives to participate and regulation may be required. This is likely to depend on the magnitude of the required adjustments, efforts and other cost factors arising from negative societal externalities if emergency systems are not implemented. On the other hand, legislative obligations could guarantee a level playing field and equal treatment between the regulated participants, and could remove any competitive effects between parties to the system. The Norwegian reserve system is voluntary for places of payment (points of sale) and banks. While all Norwegian banks participate actively in the country's national payment system (Bank Axcept), some merchants do not have the reserve solution in their payment terminals. The Finnish backup system has a regulatory basis in which credit institutions and significant branches are required to participate.

**The efficiency and effectiveness of emergency solutions also depend on customers' ability to use them.** The more similar emergency user procedures are to the procedures customers use in normal circumstances, the more effective emergency solutions will be. The user procedure for the reserve solution in Norway is largely the same as the normal payment procedure. The backup system in Finland does not require consumers to make any preparations in advance, whereas banks participating in the system would need to adjust their operations. In general, the changes required by backup systems can vary greatly at the service provider level.

## 4.4 Identified benefits and challenges

### 4.4.1 Benefits

- **Downtime can be minimised for the most critical functions to maintain trust in the financial system.** A backup system could replace financial institutions' or FMIs' systems and processes if it turns out that their business continuity measures are insufficient for the continuing provision of critical operations. Activating a backup system could, for example, mitigate the outage of core systems or a critical payment system if these were down for a prolonged period following an incident. Trust in institutions' ability to continue operations and act as reliable service providers or counterparties is crucial in the financial sector.
- **A backup system that covers the most critical functions of the industry makes it possible to recover from events that individual financial institutions cannot prepare for alone.** Such a system could cater for differences in, and be based on, individual financial institutions' technical expertise and financial means. Data vaulting, combined with a restoration platform, could also make it possible to recover from incidents that have been considered too improbable to justify continuity preparations.

- **Backup solutions supporting continuity of services could contribute to the functioning of society in a systemic cyber crisis.** Financial institutions' continued provision of everyday services to society is essential.

### 4.4.2 Challenges

- **In addition to the costs of designing, developing, testing and maintaining a contingency system, there are also costs that arise due to changes in participants' systems and business processes.** Costs are incurred from using a backup system followed by recovery and return-to-normal. In addition, financing the backup systems' liquidity requirement can lead to further financial costs stemming from contingency systems.

- **If the backup system requires different operating procedures from those used in normal circumstances, activation could increase risk level.** This can, however, be mitigated by testing and by conducting exercises. Some risk factors will require financial support and/or political will if effective mitigation is to be achieved. The Norwegian reserve system, for instance, can lead to banks taking on substantial credit risk towards counterparties and customers.

- **One of the key challenges is the need to ensure confidentiality for all the sensitive customer information that would be concentrated in one platform and protect it from cyberattacks.** The emergency or backup system could become a prime target for attacks and threat actors and could be viewed as a single point of failure.

- **Ensuring control of proper access to a backup platform could prove to be a challenge.** When a backup system is activated, end customers need to be able to authenticate themselves in an emergency. This entails defining and securely storing login credentials. In turn, the backup system's operator must have very strong controls in place to restrict and monitor administrator access. Access rights need to be clearly defined to manage who can read data when the system is not in operation.

- **Accountability of the individual firms may be a challenge. Incentives for individual financial institutions to invest in IT and their own cyber resilience measures may be in conflict with relying on a backup system offered as a public service.** Macroprudential tools such as emergency and backup systems should enhance operational resilience and should complement – but not replace – individual financial institutions' recovery capabilities. In the case of a data leakage of customers' financial information, it could initially be unclear whether the leakage occurred in the central backup system or in the financial firms' systems. This could erode accountability and could even incentivise firms to try to avoid taking responsibility during confidentiality-related incidents.

- **The issue of compatibility with data protection regulation in the EU will need to be examined further.**

Box 4

## Finland’s backup solution to secure retail payments[56]

Finland’s authorities employ a backup solution to secure the general public’s access to their bank account balances and their ability to pay by debit card or credit transfer and withdraw cash. This backup solution is, however, limited to national transactions. It is based on national legislation that obliges:

- the Finnish Financial Stability Authority to maintain a backup account system that secures banks customers’ access to their accounts as well as the functioning of customers’ existing debit cards and cash withdrawals;
- the Bank of Finland to maintain a contingency system for credit transfers between banks;
- credit institutions and significant branches to ensure they are continuously able to use the backup systems.

In addition to the parties above, certain critical retail organisations have also been onboarded.

If a bank is affected by a serious and long-term disruption, its customers’ accounts and card services can be handled by the backup account system. The customer relationship in the affected bank remains unchanged as the backup account system provides services on behalf of the bank suffering from the incident.

The Finnish Government ultimately decides on the system’s activation. When the incident is resolved, the accounts from the backup account system are returned to the original bank and the Government may decide to deactivate the system.

[56] Välimäki, T. (2023), **Finland's experiences with sector-wide backup solutions**, speech.

# 5 Conclusion

**In this report, the ESRB reviews the existing operational tools used to respond effectively to a systemic cyber incident.** In previous years, the ESRB identified the key components that need to be in place for a cyber incident to become systemic and identified the financial policy tools that could serve as a response. The ESRB concluded that financial policy tools alone may not be sufficient and proposed a review of the operational tools in use across Member States.

**The ESRB has identified the following three areas for action.**

- **The ESRB encourages financial institutions and authorities to improve their information management and information-sharing efforts.** The effectiveness of existing information-sharing tools and incident reporting centres in a major cyber incident depends largely on the format and the scope of the respective tool in place and whether it can be used across jurisdictions and sectors. In certain cases, market information and media coverage act as a source of information which can be misleading and inaccurate. This makes a clear case for employing structured and harmonised tools which can be used to gather, manage and share information. The use of information-sharing tools and incident reporting centres is critical to a functioning EU-wide information-sharing mechanism.

- **The ESRB advocates for national and EU-level crisis management and coordination practices in line with European and international standards**.[57] This helps to address the entire crisis management lifecycle of readiness, response and recovery. Although Member States have national crisis management coordination mechanisms in place, resource constraints mean that 24/7 availability is often difficult to achieve. Secure communication channels are needed for responses to be effective, while response speed could be improved through targeted training and by conducting exercises involving decision-makers. The complexity of the response process requires effective coordination among all stakeholders. This will be improved with the establishment and implementation of DORA as a first step at the national level and the EU-SCICF at the EU level.

- **The ESRB would consider the pros and cons of system-wide contingency options and backup arrangements.** This is because there may be systemic incidents that cannot be solved by the business continuity measures individual institutions have in place. It is primarily the responsibility of each individual institution to ensure its (time-) critical activities are functioning, although maintaining critical financial activities and functions in society is also a priority for the authorities. Moreover, the existence and use of a contingency option or backup system can also help maintain confidence in the affected financial institution. However, the costs and risks associated with developing, maintaining and using backup systems are likely to increase with the scope of an emergency system. Such systems are currently only in place at the national level. A European-level emergency system – or a framework for coordinating

[57] Common international standards for cybersecurity, which contain corresponding guidelines and are deployed in the financial sector, include the following: the **G7 Cyber Expert Group's family of "Fundamental Elements"**, the **CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures**, the **ISO/IEC 27000 family of standards on information security management systems** and the **NIST Cybersecurity Framework**.

national backup systems – would require extensive discussion with national institutions and a careful evaluation of its benefits and any potential implications at both the system-wide and the national level. It would also require effective coordination across all institutions.

**Through the work undertaken, the ESRB notes that to keep pace with the ever-evolving cyber landscape additional investment will be needed to build cyber expertise and capability.** In 2020 the ESRB identified a lack of investment in cyber threat intelligence as one of 13 key cybersecurity vulnerabilities. This increased need for cyber expertise and capabilities requires more funding and is a crucial challenge that needs to be overcome. However, higher expenditure on IT is associated with lower future cyber costs in the medium and the long run.[58] PPPs which include a pipeline for cybersecurity talent and grant funding could offer sustainable solutions to the challenge of attracting and retaining cybersecurity professionals. One such example is AustCyber, a PPP established by the Australian Government.

**Following on from the work done to date, the next step is for the ESRB to further identify the gaps between operational and financial policy tools.** Further work is needed on the interaction between financial and operational policy tools as well as their respective effectiveness. Ultimately, it may be necessary to explore tools beyond the existing financial and operational tools used as an effective response to a systemic cyber crisis.

[58] See Aldasoro, I. et al. (2022), "**The drivers of cyber risk**", *Journal of Financial Stability*, June.

# References


Aldasoro, I., Gambacorta, L., Giudici, P. and Leach, T. (2022), "**The drivers of cyber risk**", *Journal of Financial Stability*, Vol 60, June.

Bank for International Settlements (2023), **Annual Report 2022/23**, May.

Basel Committee on Banking Supervision (2023), "**Supervisory newsletter on the adoption of POR and PSMOR**", November.

Beck, T., Cecchetti, S., Grothe, M., Kemp, M., Pelizzon, L. and Sánchez Serrano, A. (2022), "**Will video kill the radio star? – Digitalisation and the future of banking**", *Reports of the Advisory Scientific Committee*, No 12, ESRB, January.

Crisanto, J., Pelegrini, J. and Prenio, J. (2023), "**Banks' cyber security - a second generation of regulatory approaches**", *FSI Insights on policy implementation*, No 50, June.

Euro Cyber Resilience Board Secretariat (2020), **Cyber Information and Intelligence Sharing Initiative (CIISI-EU)**, September.

European Banking Authority (2024), **Draft Regulatory Technical Standards**, EIOPA/ESMA, January.

European Central Bank (2020), **Report on a digital euro**, October.

European Central Bank (2022), "**Macroprudential policy in Europe: building resilience in a challenging environment**", *welcome remarks by Christine Lagarde, President of the ECB and Chair of the European Systemic Risk Board, at the sixth annual conference of the ESRB*, December.

European Central Bank (2023), **A stocktake on the digital euro**, October.

European Securities and Markets Authority (2022a), **Report on 4th ESMA Stress Test Exercise for Central Counterparties**, July.

European Securities and Markets Authority (2022b), **TRV Risk Analysis - A framework to assess operational resilience**, December.

European Systemic Risk Board (2020), **Systemic Cyber Risk**, February.

European Systemic Risk Board (2022a), **Mitigating systemic cyber risk**, January.

European Systemic Risk Board (2022b), **Review of the EU Macroprudential Framework for the Banking Sector**, March.

European Systemic Risk Board (2023), **Advancing macroprudential tools for cyber resilience**, February.

European Union Agency for Cybersecurity (2016), **Strategies for incident response and cyber crisis cooperation,** August.

European Union Agency for Cybersecurity (2018a), **Information Sharing and Analysis Center (ISACs) - Cooperative models**, February.

European Union Agency for Cybersecurity (2018b), **Public Private Partnerships (PPP) - Cooperative models**, February.

European Union Agency for Cybersecurity (2023a), **Undersea cables**, August.

European Union Agency for Cybersecurity (2023b), **ENISA Threat Landscape, 2023**, October.

European Union Agency for Cybersecurity (2024), **Best Practices for Cyber Crisis Management**, February.

Fell, J., de Vette, N., Gardó, S., Klaus, B. and Wendelborn, J. (2022), "**Towards a framework for assessing systemic cyber risk**", *Financial Stability Review*, ECB, November.

Krüger, P. and Brauchle, J.-P. (2021), "**The European Union, Cybersecurity, and the Financial Sector: A Primer**", *Carnegie Endowment for International Peace Paper*, March.

Maurer, T. and Nelson, A. (2020), "**International Strategy to Better Protect the Financial System Against Cyber Threats**", *Carnegie Endowment for International Peace Paper*.

Nordic Financial CERT (2019), **Nordic Financial CERT – presentation**, November.

Ros, G. (2020), "**The making of a cyber crash: a conceptual model for systemic risk in the financial sector**", *Occasional Paper Series*, No 16, ESRB, May.

Välimäki, T. (2023), "**Finland's experiences with sector-wide backup solutions**", *Speech at the 6th Annual Nordic Cyber in Finance Conference in Copenhagen, 26 September*.

# Imprint and acknowlegements

This report was approved by the ESRB General Board on XXX. It was prepared by the European Systemic Cyber Group, chaired by Francesco Mazzaferro of the European Systemic Risk Board and Andrew Nye of the Bank of England under the auspices of the ESRB Advisory Technical Committee. Substantial contributions were made by:

**Andrew Nye**
Bank of England and Co-chair of the ESCG

**Francesco Mazzaferro**
ESRB Secretariat and Co-chair of the ESCG

**Jussi Terho**
Bank of Finland and work stream lead

**Maximilian Liegler**
ESRB Secretariat and Secretary to the ESCG

**Jessica Ray**
ESRB Secretariat

**Sara Batres Fernández**
Former ESRB Secretariat

**Filippo Bucchi**
ESRB Secretariat

**Nuria Mata Garcia**
SRB

**Daniela Lo Monaco**
Banca d'Italia

**Eirini Liakopoulou**
EIOPA

**Thomas Nyegaard Hellen**
Danmarks Nationalbank

**Ylva Søvik**
Norges Bank

**Aziza Halilem**
Banque de France

**Pascal Jourdain**
Banque de France

**Vadim Kravchenko**
ECB

**Catherine Brodie**
ECB

Postal address 60640 Frankfurt am Main, Germany
Telephone +49 69 1344 0
Website **www.esrb.europa.eu**



For specific terminology please refer to the **ESRB glossary** (available in English only).

PDF ISBN 978-92-9472-384-0, doi:10.2849/05420, DT-09-24-197-EN-N