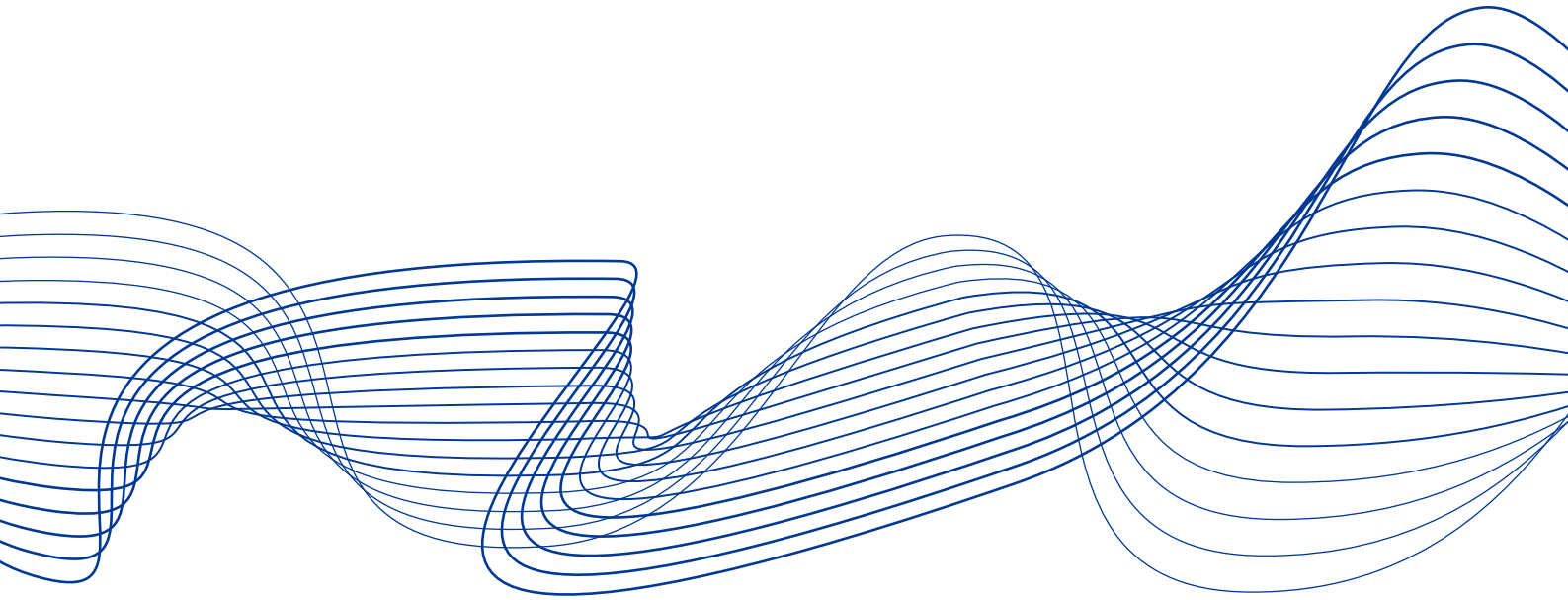
Advancing macroprudential tools for cyber resilience

February 2023



ESRB
European Systemic Risk Board
European System of Financial Supervision

Contents

Executive summary

The ESRB worked in 2022 within the context of a substantially heightened cyber threat environment across Europe. The cyber activity resulting from Russia's invasion of Ukraine have affected both Ukraine and EU Member States directly and indirectly. Furthermore, an increase in cyber attacks and the active sabotage of power and telecommunications infrastructure in EU Member States – which the financial sector relies on – present significant threats to financial stability.

The ESRB responded to this heightened cyber threat environment by:

- **Enhancing the exchange of information across jurisdictions and authorities.**[1]
- **Focusing on the tools and elements needed to advance cyber resilience and strengthen preparedness for potential cyber incidents.**
    - **Advancing a cyber resilience scenario testing (CyRST) approach:** the ESRB completed further work on this approach, which could support authorities in (i) testing the response and recovery capacity of the financial system against severe but plausible scenarios involving a cyber incident, (ii) evaluating their impact on financial and operational stability, and (iii) identifying areas where further work is required to mitigate cyber risks.
    - **Developing the concept for a systemic impact tolerance objective (SITO):** the ESRB worked on developing SITOs, which can assist in identifying and measuring the impacts of cyber incidents on the financial system, and evaluating when they are likely to breach tolerance levels and cause significant disruption.
    - **Reviewing current financial crisis management tools:** the ESRB evaluated whether these tools are sufficient for adequately responding to system-wide cyber incidents.

The heightened cyber threat environment across Europe calls for a step change in enhancing system-wide cyber resilience. The resistance and detection capabilities of individual entities constitute a first layer of defence against cyber incidents. The Digital Operational Resilience Act (DORA)[2] is part of an ongoing effort at the EU level to improve the cyber resilience of individual entities. Threat-led penetration tests outlined by DORA, such as the European Framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU), provide a way of testing this first layer of defence. However, further layers of defence are needed to increase the resilience of the financial system as a whole against cyber incidents.

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

1 "Authorities" refers to national and EU public authorities engaged in operational or financial supervisory and oversight activities, as well as central banks.

2 See **Digital Operational Resilience Act** (DORA).

- **The ESRB encourages authorities to use the CyRST approach to pilot system-wide cyber resilience scenario testing as soon as possible.** Such pilots can complement other analytical tools that the authorities might be using and deepen their understanding of CyRST and of the risks to system-wide cyber resilience. This is important and urgent, given the increased likelihood that a cyber attack will strike the European financial sector and because it will take time to pilot CyRST, identify the risks and implement appropriate mitigating measures. The ESRB will continue to work in this area as a hub for sharing progress and good practice, and will update the conceptual approach based on what the authorities learn from their more detailed work in the pilots.

- **The ESRB advocates the use of SITOs and will continue to transition from a conceptual approach to a practical basis for implementing them.** Specifically, the ESRB will identify a key economic function[3] where disruptions have cross-border implications and define appropriate SITOs at EU level so as to ensure consistency across the region/sector and authorities. The ESRB will work with authorities across the EU to identify where a consistent approach is required and to decide on the approach for setting SITOs where there are cross-border implications. The ESRB recognises that where disruptions have no or few cross-border implications, SITOs may differ across jurisdictions to reflect national specificities.

- **The ESRB will consider which operational policy tools are most effective in responding to a system-wide cyber incident and identify gaps across operational and financial policy tools.** This work will build on the analysis of financial crisis management tools described in this report.

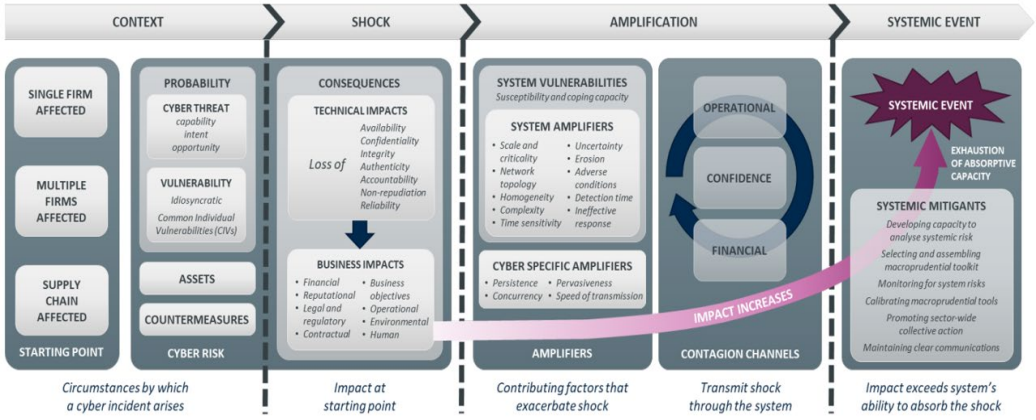
[3] A list of key economic functions is provided in the ESRB (2020) **report on systemic cyber risk.**

1 Introduction

The ESRB has identified cyber incidents as a risk to financial stability. The current geopolitical situation has increased this risk, calling for a step change in enhancing cyber resilience. The war in Ukraine, the broader geopolitical landscape and the increasing use of cyber attacks have significantly heightened the cyber threat environment. As well as incidents without a malicious motive, there is an increased risk of cyber attacks on the EU financial system by states or state-sponsored actors. The ESRB's initial response has been to enhance cyber threat intelligence sharing across all ESRB member institutions and the Bank of England. However, the current cyber threat environment calls for a step change in the EU's efforts to enhance cybersecurity at the system-wide level – efforts that need to go beyond improving cyber resilience at the level of individual entities. This includes operationalising the approaches to cyber resilience considered in this report.

Action is needed to mitigate the risk of a cyber incident impairing the delivery of key economic functions and evolving into a systemic event. A cyber incident refers to any technology disruption, including from a cyber attack. A cyber incident can 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 impair the delivery of a key economic function.[4] If the initial shock is amplified and transmitted via operational, confidence and financial contagion channels throughout the financial system, feedback loops can increase its impact, ultimately resulting in a systemic event. The ESRB illustrated this in its 2020 systemic cyber risk model as summarised in Figure 1.

Figure 1
Systemic cyber risk model

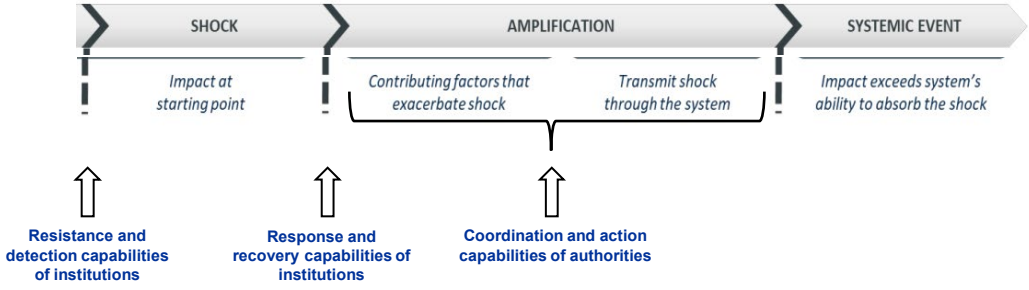


Source: ESRB (2020).

[4] A list of key economic functions is provided in the ESRB (2020) **report on systemic cyber risk.**

There are three successive key layers of defence to prevent a cyber attack from evolving into a systemic event. The first layer is made up of the resistance and detection capabilities of financial institutions. If financial institutions can detect cyber threats and stop them entering their individual systems, a cyber incident can be prevented. The second layer is made up of the response and recovery capabilities of institutions. If a financial institution's first layer of defence has been breached, but it has the capacity to respond to and recover from the cyber incident and continue to provide its services in a timely manner, the cyber incident can be contained before it becomes amplified. The third layer of defence is made up of the coordination and action capabilities of authorities. If authorities can intervene using analytical and policy tools, they may be able to contain a cyber incident that has started to affect the wider financial system before it turns into a systemic event. Or, if it has turned into a systemic event, authorities may be able to mitigate the consequences. The second and third layers are likely to operate at the same time, as firms need to restore the operating capacity of the financial system. Figure 2 provides a stylised representation of the three layers of defence.

Figure 2
Stylised representation of the layers of defence



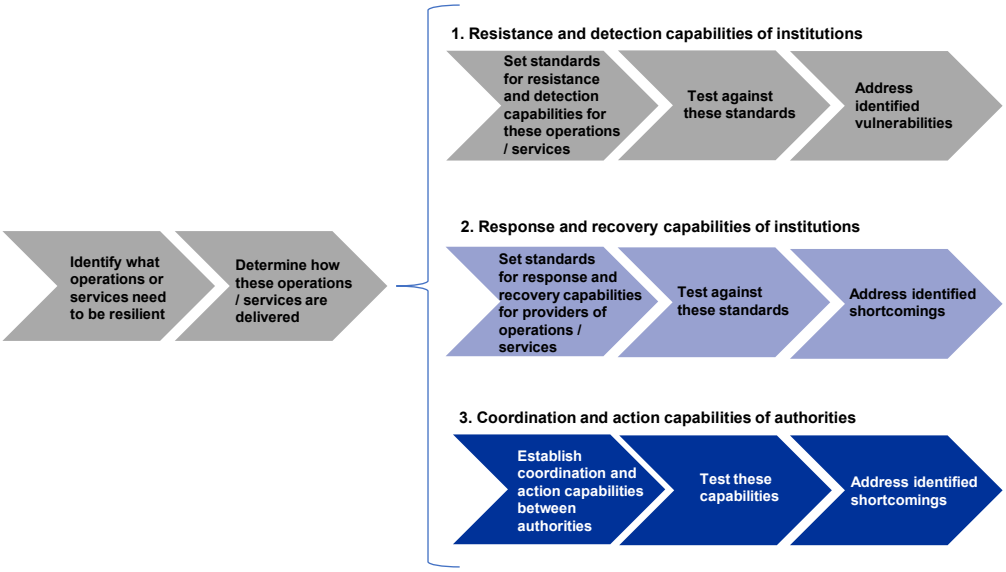
Source: ESRB.
Notes: Figure 2 is stylised as there is an overlap between firms' response and recovery measures and authorities' coordination and actions. For example, supervisory authorities will start to interact with firms as soon as a financial institution's first layer of defence has been breached and the incident is reported to them. Likewise, even if affected firms are unable to recover from a cyber incident in a timely manner, they will continue to try to respond and recover during the amplification phase and beyond. Reflecting this, coordination between authorities during the amplification phase would involve close collaboration between firms and authorities.

The ESRB and other authorities have been designing a framework for assessing and enhancing the resilience of these three layers of defence. For example, Prenio and Restoy (2022) set out a five-step approach for assessing and strengthening the operational resilience of providers of certain operations and/or services. This includes identifying those operations or services that are crucial for the delivery of key economic functions such as payments. As a next step, the authorities need to determine how these operations or services are delivered. Standards must then be set for how resilient they need to be. Finally, testing against these standards must be carried out and any vulnerabilities that such tests reveal need to be addressed. This framework, which focuses on the resistance and detection capabilities of institutions (the first layer of defence), can be generalised and extended to the system-wide level. It can then be applied to the response and recovery capabilities of institutions (the second layer of defence) and the collective

coordination and action capabilities of authorities (the third layer of defence). In each layer, standards need to be identified and tested against and any vulnerabilities or shortcomings identified by such testing need to be addressed. This is illustrated in Figure 3.

Figure 3

Designing, assessing and strengthening defences against systemic cyber risk



Source: The grey elements of the chart are adapted from Prenio and Restoy (2022), while the blue elements have been added to illustrate the second and third layers of defence.

Key elements of the first layer of defence are already being strengthened in line with the Digital Operational Resilience Act (DORA). The resistance and detection capabilities of the first layer of defence, along with initial response capabilities, are already tested using the threat-led penetration tests outlined in DORA. In the EU, this is done via the TIBER-EU approach and in the United Kingdom via the CBEST framework. While these tests help to identify potential weaknesses that need to be addressed, they do not typically test recovery capabilities. Therefore, it is paramount that the second and third layers of defence are tested and the identified risks mitigated in order to ensure that all three layers of defence are resilient and improve cyber resilience.

This report focuses on three elements related to the second and the third layers of defence that support the assessment and action capabilities of EU authorities. Sections 2 and 3 look at different analytical tools. Section 2 examines (i) how severe but plausible cyber scenarios can be safely tested; (ii) how to evaluate the scenarios' potential impact on financial stability; and (iii) based on the findings of the tests, how to identify actions required to mitigate the risks identified. Section 2 also sets out high-level principles for an approach to cyber resilience scenario testing (CyRST). Potential scenarios that EU authorities could use to pilot CyRST and learn from it, as well as mitigate relevant risks, are also presented. Section 3 considers how identifying and measuring the impacts of cyber incidents can assist authorities in evaluating when they are likely to breach systemic tolerance levels and cause significant disruption. Furthermore, Section 3 outlines the systemic impact tolerance objective (SITO). Section 4 evaluates the effectiveness of financial policy

tools in responding to the impacts of cyber threats. The final section concludes that the heightened cyber threat environment across Europe calls for a step change in enhancing cyber resilience. It proposes areas in which the ESRB and authorities in Member States need to make further progress.

2 Cyber resilience scenario testing (CyRST)

This section addresses cyber resilience scenario testing (CyRST) and sets out principles to help authorities develop and pilot it. CyRST[5] is an analytical tool that tests the capacity of the financial system to support the continuity of key economic functions. CyRST assesses whether the financial system can swiftly and efficiently respond to and recover from a severe but plausible cyber scenario that causes significant disruption and could affect financial and operational stability (see Box 1). Such a tool is needed to complement the analytical framework already in place, which is designed to facilitate an understanding of existing and emerging system-wide cyber vulnerabilities that may pose risks to financial stability.[6] CyRST will help authorities identify, develop and calibrate adequate risk mitigants, and guide and evaluate policy interventions.

2.1 Closing a gap in the analytical toolkit

Various analytical tools already exist to support the assessment of certain elements of systemic cyber risk. The systemic dimension of cyber risk is referenced in the Digital Operational Resilience Act (DORA). It indicates that EU authorities can develop mechanisms for identifying common cyber vulnerabilities and risks across sectors. In addition, the DORA states that EU authorities can develop crisis management and contingency exercises for a cyber incident that has a systemic impact on the EU's financial sector as a whole.[7] In addition to EU[8] regulatory requirements for firms[9], a number of cyber resilience tools have recently been developed to support authorities in their analysis of cyber risk at both the firm and system levels. For example, cyber information and intelligence sharing initiatives between the public and private sectors, including the EU's Cyber Information and Intelligence Sharing Initiative (CIISI-EU), help to build system-level understanding of potential cyber threats and vulnerabilities. Threat-led penetration testing frameworks such as TIBER-EU help authorities to enhance cyber resilience in the financial sector by testing firms' cyber threat detection and cyber incident resistance capabilities. System-wide crisis simulation exercises help firms and authorities to assess their preparedness to coordinate, communicate and act in the event of a cyber incident. In addition, in January 2022 the ESRB recommended the establishment of a pan-European systemic cyber incident coordination framework (EU-SCICF). Its purpose is to strengthen coordination between the relevant authorities themselves and with other authorities in the Union and other key actors at international level in the event of a major cyber incident, in line with Article 49 of DORA.

The lack of a tool that focuses on the financial system's capacity to respond to and recover from a severe but plausible cyber scenario leaves a gap in the analytical toolkit. To date, no

5 The **ESRB Report on Mitigating Systemic Cyber Risk** referred to systemic cyber resilience scenario stress testing. This report uses the term cyber resilience scenario testing (CyRST) to better distinguish this analytical tool from stress-testing frameworks that have been developed to test financial resources (e.g. capital and liquidity), rather than the operational capacity of firms to absorb a shock.

6 See the ESRB (2022) **report on Mitigating Systemic Cyber Risk**.

7 See Article 49 of DORA.

8 Such as the Eurosystem's cyber resilience oversight expectations for financial market infrastructures and DORA for financial institutions.

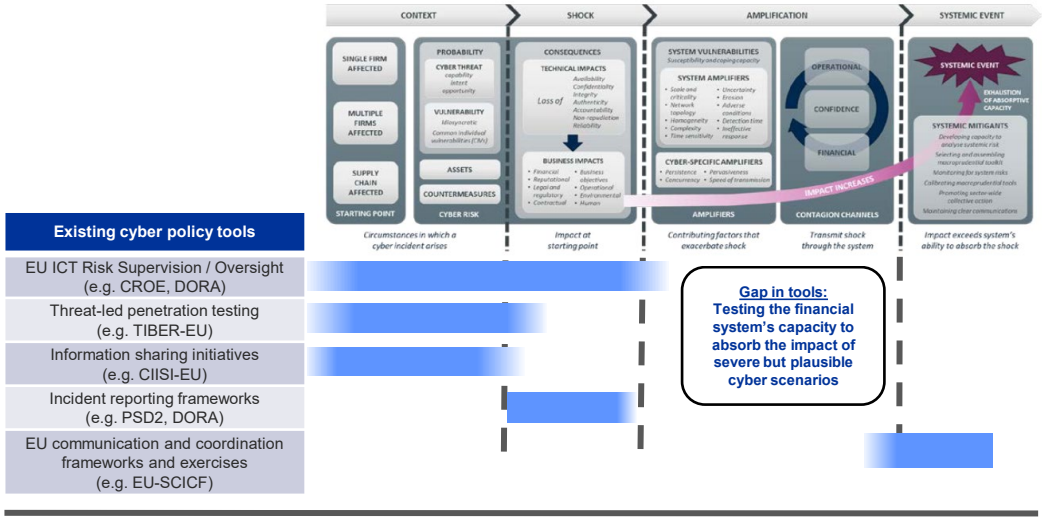
9 The term "firm" includes both financial institutions and financial market infrastructures.

tool has been developed at European level that can test the capacity of the financial system to respond to and recover from a severe but plausible cyber scenario. This gap in authorities' analytical frameworks for cyber risk is illustrated in Figure 4, which outlines where existing analytical tools can help assess cyber resilience as a cyber incident unfolds through the systemic cyber risk model.

CyRST could be a valuable analytical tool for helping to close this gap, as it could enable an assessment of how the financial system would respond to and recover from a severe but plausible cyber scenario. CyRST could complement other analytical tools and would be useful in evaluating the impact on financial and operational stability and identifying areas where further work is required to mitigate risks. This is turn would reduce the likelihood of contagion through confidence, financial and operational channels. Building on the ESRB's 2022 report, this section explores whether and how CyRST can increase financial system resilience so that key economic functions can continue and financial and operational stability can be maintained in a severe but plausible cyber scenario. It also develops a conceptual approach on CyRST for authorities.

Figure 4

Illustrative schematic overview of analytical and policy tools that can be used to assess resilience as a cyber incident unfolds through the systemic cyber risk model



(color blends mean partial coverage)

Source: ESRB.

Note: This schematic overview illustrates how existing cyber tools can support authorities in assessing the resilience of firms and the financial system as a cyber incident unfolds through the stages of the systemic cyber risk model. It also highlights that there is a gap in the system-wide response and recovery aspects of cyber resilience.

Box 1

Cyber resilience scenario testing (CyRST)

CyRST is an analytical tool for testing the capacity of the financial system to swiftly respond to and recover from a severe but plausible cyber scenario that causes a significant disruption and could affect financial and operational stability. The ability of the financial system to respond to and recover from such an event determines the extent to which it can support the continuity of key economic functions in a severe cyber scenario.

This is assessed by designing a hypothetical cyber scenario and asking participating firms to document the scenario's impact, how they would respond to and recover from it, and the extent to which key economic functions could continue to operate under the scenario. The test is used to evaluate the overall impact of the scenario on financial and operational stability and to identify areas where further work is required to mitigate risks.

CyRST can involve financial institutions, financial market infrastructures and other firms that support the operation of the financial system, including information and communications technology (ICT) third party service providers.

Relationship with other analytical tools

CyRST can complement other analytical tools in the analytical framework set out in Figure 4. It should be viewed as one component of the overall framework for assessing system-wide cyber resilience. For example, any vulnerabilities identified by CyRST could be explored further in a market-wide crisis simulation exercise involving relevant firms. CyRST can also be informed by, and support, other cyber resilience initiatives that are undertaken by certain authorities. The outcome of CyRST may also be able to inform more traditional financial resilience tools, such as financial stress tests that test the impact of a cyber scenario on a firm's balance sheet, by helping to calibrate the cyber incident-induced losses. See Section 3 for further information on how CyRST and SITOs can work together.

2.2 Key findings

Given that CyRST is a new tool, the ESRB sought to:

- develop a shared understanding of what CyRST is and how it could interact with and complement other analytical tools;
- identify the benefits that CyRST could provide to firms and authorities (see Section 2.2.1);
- provide a conceptual approach to CyRST that could be further developed and explored by authorities undertaking CyRST exploratory work and/or pilots (see Section 2.3);
- consider how the ESRB could support authorities as they undertake exploratory work on CyRST (see Section 2.4).

2.2.1 Benefits of CyRST

CyRST can assist authorities in testing the potential impact of a severe but plausible cyber scenario on the provision of one or more key economic functions. As part of this, it can help identify any cyber vulnerabilities that could create risks to financial and operational stability and gauge the need for action at a firm- and system-wide level. CyRST could also provide insights to authorities on the individual and collective ability of firms to absorb the shock from a severe but plausible cyber scenario and analyse its potential amplification into a systemic event. This in turn could provide insight into the potential operational, financial, reputational and legal effects of the cyber scenario. CyRST could also help authorities discover new vulnerabilities or assess the scale of system-wide vulnerabilities (e.g. potential vulnerabilities arising from system-wide operational dependence on ICT third-party service providers, reliance on common contingency plans or lack of substitutability). Furthermore, CyRST could help authorities obtain information on interdependencies in the financial system and how contagion channels could be triggered in a specific scenario (e.g. how the response of one firm could impact other firms and the broader financial system). Given the interconnectedness and complexity of the financial system at an operational level, another potential benefit of CyRST is that firms learn about the operation of the wider system, including any own dependencies and reciprocal dependencies. Most importantly, the outcome of CyRST could help identify any actions that authorities and firms, individually and collectively, should take to build cyber resilience at firm and system level, either ex ante to reduce the impact of a severe cyber incident, or ex post to intervene in a timely and focused manner.

CyRST can support authorities in implementing supervisory and/or oversight requirements such as DORA. In particular, CyRST can help identify common cyber vulnerabilities and risks and help assess the implementation by key firms of response and recovery requirements. DORA indicates that EU authorities may develop mechanisms to identify common cyber vulnerabilities and risks across sectors. In addition, DORA requires firms to assess the potential impact of severe business disruptions by means of quantitative and qualitative criteria, using internal and external data and scenario analysis, as appropriate.[10] The aim behind this impact assessment is to evaluate the criticality of identified and mapped business functions, supporting processes, third-party dependencies and information assets, and their interdependencies. CyRST is a tool that could assist financial supervisory and oversight authorities, including DORA competent authorities, in assessing how firms are meeting their response and recovery requirements.

2.3 A conceptual approach to CyRST

As CyRST is in the early stages of development at certain authorities, there is no defined approach or methodology on how to design and operate it. The Bank of England and the Danish Financial Supervisory Authority (FSA) are conducting exploratory work in this area with considerable commonality in their approaches (see Box 2). Their approaches consist of involving systemically important firms, preparing a common scenario and running the test over a period which allows firms to develop their responses[11] before collating results. Their approaches also

[10] See Article 10 of DORA.

[11] Firms may be asked to complete a questionnaire or prepare a report on their response to the cyber scenario under structured headings.

focus on the capacity of both individual firms and the financial system to absorb a severe but plausible cyber scenario and continue providing key economic functions.

The exploratory work of the Danish FSA along with insights obtained from other EU authorities as well as the Bank of England, supported the development of the ESRB's conceptual approach to CyRST. This conceptual approach outlines the key components of CyRST and some high-level principles that may aid authorities seeking to conduct a pilot or exploratory cyber resilience scenario test. The conceptual approach is intended to help build an understanding of what CyRST entails and includes some considerations and potential options for authorities involved in CyRST, recognising that the structure and format of any test will depend on the outcomes that authorities are trying to achieve. In addition, the approach is likely to evolve over time as CyRST becomes more established among authorities and they incorporate knowledge gained from pilots and tests.

Box 2

The Bank of England and the Danish FSA experience

Bank of England

In 2017 the Bank of England's Financial Policy Committee (FPC) set out its framework for building and maintaining cyber resilience. Two of the elements of this framework involve setting clear baseline expectations for firms' resilience that reflect their importance for the financial system, and regular resilience testing by firms and supervisors. Since then, the Bank of England has been working on the development of a new tool known as "cyber stress testing" which combines these two elements of the FPC's framework and focuses on the key cyber risks to the stability of the financial system. The Bank of England is using its test to explore firms' capabilities and the potential impact on financial stability in a hypothetical scenario.

Following a successful pilot in 2019, the Bank of England carried out an exploratory cyber stress test in 2022[12] with several firms on a voluntary basis. The test had a data integrity incident as the disruption scenario and was intended to test firms' ability to meet the impact tolerance for payments[13] in a severe but plausible scenario involving the retail payments system.

Danish FSA

In June 2022 the Danish FSA announced the launch of its programme for strengthened operational resilience in the financial sector. The programme uses cyber stress testing to analyse the consequences of an extensive ICT disruption.[14] The programme builds, among other things, on the work of the Danish Financial Sector forum for Operational Resilience (FSOR), which is chaired by Danmarks Nationalbank.[15] The cyber stress test, in which systemic firms will be required to participate, is being led by a team of information and cybersecurity supervisors assisted by core

12 See the **Bank of England's PRA statement on the 2022 cyber stress test**.

13 Impact tolerance for payments: see the **Financial Policy Summary and Record** of the March 2021 Financial Policy Committee meeting.

14 See **Danish FSA statement on its cyber stress testing programme**.

15 See the **Danish FSOR webpage**.

banking and resolution supervisors at the Danish FSA. Danmarks Nationalbank is included in the programme as an advisory partner.

The objective of the programme is to analyse what would happen at the firm and sector levels in the event of an extensive ICT disruption. Based on the information gained from the test, the Danish FSA intends to further the implementation of appropriate initiatives with the individual firms in order to prevent and minimise the consequences of a disruption. Follow-up initiatives at sector level will be coordinated with Danmarks Nationalbank and within the FSOR.

The initial project under the programme involves a scenario that is based on an extensive ICT disruption at a systemically important ICT service provider and/or financial institution. The firms that participate in the test will:

1. describe the actions taken, step by step, to recover normal ICT operations and assess the time taken to recover;
2. describe how, to what extent and for how long critical business processes/key economic functions were kept going during the disruption of normal ICT operations as well as the resources required to maintain the functions;
3. map the financial, reputational and legal consequences of the disruption at various stages up until normal operations can be restored, and provide supporting evidence.

Depending on the results of the test, there will be an assessment to identify whether there is a need for additional measures/investments in the individual firms and/or at sector level.

2.3.1 Fundamental components of CyRST

- **Defining the objectives and scope of the test:** at the outset, authorities should clearly identify the objectives and outcomes they are seeking to achieve, and pinpoint the particular cyber risk or vulnerability being tested. This will help define the scope of the test, including firms that should be involved, the key economic functions that are affected, the required severity of the scenario and the assessment approach that should be taken. For example, if the objective is to test the capacity of the financial system to absorb a cyber shock that causes a significant disruption to the operation of retail payments, this objective will help determine the cohort of firms that should participate in the test. By helping define the scope of the test, this will in turn help ensure adequate coverage and support a robust and representative assessment of system-wide cyber resilience.
- **Designing the CyRST approach:** consideration should be first given to how the test should be structured so that the required information is gained. Authorities should identify the information required from firms, both qualitative and quantitative (where possible), that will enable them to understand how the firms would respond to and recover from the cyber incident in the scenario. For example, firms might be asked to provide an account of their actions (including triage and decision-making in the early stages of the incident) and a related

timeline to recovery[16], as well as a comprehensive assessment of the business, operational, financial and other impacts. Firms may also be asked to identify any wider impacts that might arise from the scenario, including interdependencies between firms or any second-round effects from the response actions they take. Asking firms to provide information on both the gross impact and net impact (i.e. before and after contingency measures have been taken) can also test the effectiveness of their contingency measures. At the end of the test, firms should be asked to consider what they have learned from completing the test and outline any areas they are planning to work on to enhance their response and recovery capacity. Authorities could obtain this information from firms by asking them to provide a response to a questionnaire or prepare a structured report.

Authorities should consider what evidence to request from firms as a response or as supporting evidence for their response. Firms should also be requested to provide information on any assumptions they have made (e.g. on dependencies) to help authorities understand whether they are comparing like with like. Authorities will also need to consider the appropriate timeframe for the test, including the period of time firms are given to prepare and provide their responses.

The selection and development of an appropriate scenario for the test is also fundamental to designing the CyRST approach (see Section 2.3.2).

- **Engaging with firms:** early engagement on CyRST plans can help ensure buy-in and support from firms and facilitate their planning for the test. Authorities will also need to consider the guidance required to support firms in carrying out the test. Given that CyRST is a new tool, incorporating check-in mechanisms over the course of the test can help address any potential misinterpretations and ensure that responses are provided on a consistent and comparable basis across firms. For example, a central query and response hub could be made available where responses to queries are provided to all participants.

  In order to ensure that comprehensive responses are received during the test, firms should be asked to bring in a breadth of expertise from across their organisation (e.g. business, technical and operational) to participate in the test, including expertise on the financial stability impacts. For quality assurance purposes, firms should be asked to ensure that second line management and senior management provide internal challenges to the firm's response and that the board sign off on the final response to guarantee that it is robust and holistic.

- **Collating and analysing results at firm and system level:** the responses received from firms will support the authorities in assessing the operational capacity of firms, individually and collectively, to absorb the shock arising from the cyber scenario and actions taken in response.

  Information provided by firms on potential wider impacts will support the system-wide assessment. Such a system-wide assessment includes identifying the systemic relevance of firms from an operational perspective, concentration risks, potential transmission channels (direct and indirect) and amplification mechanisms. The assumptions that firms have made and provided in their responses, including any dependencies identified, can also inform the

[16] Details on response actions are requested to the extent that they inform the response timeline to recovery.

system-wide assessment (for example, if firms have a common dependence on a contingency plan or solution that is not adequate to support a cyber shock at a system level). System-wide implications can also be drawn from individual responses by looking at firms' individual responses in aggregate to examine the situation at a system level (e.g. ability to meet SITOs and potential barriers) and by comparing firms' qualitative responses to identify commonalities (or differences) that may cause issues at a system level.

Authorities should also include any information they have from other cyber analytical tools (e.g. system mapping and market-wide crisis simulation exercises) to inform their system-wide assessment.

- **Finalising the assessment, identifying learnings and potential actions required:** the final assessment will help authorities identify whether they have achieved the outcomes sought and what the test results indicate about the capacity of firms and the financial system to absorb the shock from a severe cyber scenario. CyRST does not involve a pass/fail result but is a more nuanced examination that looks at the implications of a cyber scenario and firms' response actions. Much of the information provided by firms is likely to be qualitative, with a few quantitative metrics (e.g. time to recovery, customers affected and the value and volume of transactions). As a result, a system-wide assessment of the overall response and recovery capacity is likely to be mainly qualitative in nature and involve an element of judgement.

  Firms' responses on what actions they plan to take following the test will help inform authorities on further actions that may be required by individual firms or firms and/or authorities on a collective basis. This could include measures to be taken by authorities or collective action initiatives at industry level. Identifying learnings from the test is another important step for firms and authorities. For authorities, this may include learnings regarding the test methodology which can help inform the evolution of CyRST as a tool, or learnings regarding specific cyber vulnerabilities that may need to be considered in more depth (e.g. through further CyRST or using other cyber analytical tools, such as a market-wide crisis simulation exercise).

2.3.2 Principles for developing a CyRST scenario

The CyRST scenario should support the objectives of the test and the outcomes sought by authorities, including the severity of the cyber incident to be absorbed. For example, in testing the capacity of the financial system to absorb a cyber incident, a scenario that affects the availability of one or more key economic functions could be appropriate or a more complex scenario involving data integrity issues may be required to achieve the desired level of severity. The most severe shocks are likely to involve the destruction, encryption or alteration of data related to value.[17] In addition, the cyber risk or vulnerability to be tested in the scenario may be likely to affect one key economic function (e.g. payments) or multiple key economic functions. Depending on the outcomes sought from the test, the scenario could also include several escalations, with additional information provided to firms over time.

[17] See ESRB (2020).

The CyRST scenario should focus on the impact of the system-wide cyber incident on firms and how they manage their response and recovery, rather than the detailed technical factors that caused the incident. As CyRST does not focus on testing the technical response of firms in detail, the scenario should be realistic but not overly technical so that it can apply to a range of firms. For example, the scenario could stipulate that the SEPA system has been compromised and that all retail payments are blocked, but it does not have to go into the technical details of what might have caused the disruption.

A uniform CyRST scenario that can apply to all firms involved in the test and support a system-wide assessment should be considered. In order to ensure comparability of results across firms and obtain a system-wide assessment, the same scenario should be provided to all participants in the test. One of the challenges authorities will have in developing a uniform scenario is ensuring that it is sufficiently high-level to apply to all firms involved, but also detailed enough so that firms provide consistent responses that are comparable and can be aggregated to provide a system-wide view.

Authorities should consider engagement with firms and cyber authorities during the development of the scenario to help ensure that it is credible and fit for purpose. Given the challenges involved in developing a scenario, engagement with a small number of firms during the development process can help ensure that authorities design a scenario that is well understood by and applicable to all firms involved in the test and that takes account of industry knowledge and expertise. Consulting with other authorities during the development of the test, particularly national or European cyber authorities, could also help to ensure that the scenario is realistic and plausible.

2.3.3 Authorities involved in CyRST

The involvement of authorities in CyRST will depend on several factors, including the objectives of the test, the expertise required[18] and the institutional arrangements in Member States and at an EU level. Microprudential authorities, responsible for firm-level supervision and/or oversight, and macroprudential authorities, responsible for financial stability, can collaborate and conduct CyRST in line with their statutory mandates. In the United Kingdom, the Bank of England is the microprudential authority and the macroprudential authority, and experts from both authorities were involved in the UK's 2022 exploratory test. In Denmark, the test is being carried out by the microprudential authority, the Danish FSA. Danmarks Nationalbank is included in the programme as an advisory partner.

Consultation with national cyber authorities should also be considered. Both the UK and Danish authorities rely on independent judgements, including those of their respective national cybersecurity authorities.

Authorities at European level could have a role in CyRST, including in supporting both individual tests and the further development of CyRST. The European Supervisory Authorities may consider how CyRST could provide experience and lessons learned for the tasks to be carried out under DORA, such as by establishing mechanisms to identify common cyber vulnerabilities and

[18] Including any ICT-related skills and expertise required as referenced in Section 4.2.

risks across sectors.[19,20] ENISA could also be of assistance given its expertise and role in achieving a high common level of cybersecurity across Europe.[21]

National and European authorities should collaborate to ensure that tests are aligned and maximum benefits are obtained from CyRST. This is important as many financial institutions and financial market infrastructures operate in several Member States. In addition, cross-border interactions should not be considered as a limitation in conducting tests, as this could be addressed through a formal and comparable representation of the dependencies.

Authorities involved in tests should identify who should lead the test and the role of each authority. Institutional arrangements at a national and European level are likely to influence the choice of the lead financial authority and the allocation of responsibilities. At the same time, each financial or cyber authority involved in a test will contribute in line with its own mandate in order to achieve a successful outcome. Authorities are also likely to work with the financial industry, such as via collective action programmes, as these initiatives help address system-wide vulnerabilities and play a key role in improving industry readiness to deal with an actual crisis.

2.3.4 CyRST – approach to conducting a pilot

Pilots provide practical experience and learnings that cannot be obtained from theoretical consideration and are therefore needed to advance the development of CyRST. When authorities conduct a pilot cyber resilience scenario test, there are some additional considerations to bear in mind, including scope and complexity. A conceptual approach to CyRST has been provided. However, given the early stage of development of CyRST as an analytical tool, further exploratory work by authorities is required to provide practical experience and learnings and support its further development. Indeed, authorities interested in using CyRST to address the gap in their cyber toolkit are likely to consider conducting a CyRST pilot as a first step. Several additional considerations have been identified for authorities conducting a pilot.

- **Provide clarity on outcomes sought in the pilot:** set clear objectives and outcomes sought at the beginning of the pilot and use these to help manage any potential scope creep as the pilot approach and scenario are developed. This includes clarity on whether the focus of the pilot is to test resilience to a cyber risk or vulnerability or to test the CyRST methodology.
- **Consider limiting scope and complexity in a pilot:** for a pilot, it may be worth limiting the scope of the test in the first instance. For example, the test could include a small number or representative proportion of institutions. The pilot should also factor in the level of complexity required in the scenario. For instance, a data or system availability scenario that affects one key economic function might be used rather than a data integrity scenario that involves multiple key economic functions. See Box 3 for suggestions on scenario development in a pilot.

---

19 See Article 49 of DORA.

20 There might be synergies that need to be considered between CyRST and ongoing work at the European Supervisory Authorities, such as **EIOPA's work on methodological principles of insurance stress testing with focus on cyber risk**.

21 See the **ENISA webpage** for further information.

- **Identify any additional steps that may support a successful pilot outcome:** as CyRST will be new to both authorities and participating firms, there may be some additional steps that could help ensure a successful outcome, such as testing the scenario and information requests with experts or a firm before finalising them for the pilot.

- **Start soon and iterate:** a key benefit to CyRST is the learnings that authorities and firms take away from the tests. Getting the test up and running at an early stage, rather than spending a lot of time seeking to develop a detailed methodology, will help ensure key learnings are obtained at an early stage. CyRST is likely to evolve and adapt as pilots and tests are undertaken and an iterative approach is recommended for testing and methodological/conceptual development.

Box 3
Scenario development in a pilot

The following criteria were considered for a scenario that could be used in a CyRST pilot. The scenario should:

- have a severe impact on the continuity of the provision of a key economic function and pose a risk to financial and operational stability;
- provide an opportunity for other EU Member States and European-level entities to learn from the test;
- apply to all firms involved in providing the critical function (e.g. financial institutions and financial market infrastructures);
- be suitable for a pilot in terms of scale and scope.

Given the criticality of payments in all financial systems, a cyber scenario that involves a disruption to wholesale payments would have a severe impact on the financial system and would be relevant for all EU Member States and at a European level. This could include a malware attack that has infected a common component of a firm's payment infrastructure and paralysed the firm's ability to send or receive wholesale payments for a prolonged period. A more severe scenario could involve a distortion in the integrity of payments. However, that would add further complexity to the scenario and may prove challenging for an initial pilot test.

A scenario could also test the ability of the financial system to absorb a shock following a severe disruption at a critical third-party ICT service provider. CyRST could deepen understanding of potential systemic cyber risk in this case. However, whether this scenario would have a system-wide impact would depend on the individual arrangements in Member States.

2.4 Next steps

Firms and authorities need to ensure that they have the required level of preparedness and resilience for the financial system to respond to and recover from a severe but plausible cyber incident. This is increasingly important as the financial system becomes more reliant on technology to provide financial services. Furthermore, the likelihood that a cyber incident will affect the European financial sector is increasing. Being prepared and resilient applies to firms and authorities individually, collectively and on an ongoing basis. In particular, authorities need to be able to test the ability of firms and the financial system to respond to and recover from such scenarios so that they can assess firms' overall level of preparedness and resilience. In this way, authorities can identify any further work required to implement appropriate mitigation measures. There is a gap in the current analytical toolkit used to assess cyber risk and CyRST could help fill this gap. The Bank of England and the Danish FSA conducted exploratory CyRST throughout 2022 and will continue to do so in 2023.

Against this background, the ESRB encourages authorities to use the CyRST approach to pilot system-wide cyber resilience scenario testing as soon as possible. Such pilots could complement other analytical tools that the authorities use and would help them learn about CyRST and deepen their understanding of the risks to system-wide cyber resilience. This is both important and urgent, given the increased likelihood that a cyber attack will affect the European financial sector and because it will take time to pilot CyRST, identify the risks and implement appropriate mitigating measures. The ESRB will continue to work in this area as a hub for sharing progress and good practice and will update the conceptual approach based on what the authorities learn from their more detailed work on the pilots.

3 Systemic impact tolerance objective (SITO)

This section develops the concept of a systemic impact tolerance objective (SITO) and sets out elements that authorities should consider when defining SITOs. Up to a point, the financial system can tolerate disruptions to the delivery of a key economic function that results from a cyber incident, without such disruptions turning into a systemic event that threatens financial stability.[22] The point at which the impact tolerance of the financial system is breached, and a system-wide cyber incident turns into a systemic event, is unknown. Defining SITOs can assist authorities by, among other things, serving as a yardstick against which they can assess their own coordination and action capabilities. As the tolerance of the financial system to disruptions is likely to differ depending on which key economic function is impaired, there is no single SITO and authorities need to define SITOs at the level of key economic functions. This section is designed to support authorities in this task.

3.1 SITO – concept and main purpose

SITOs define the point at which the tolerance of disruption of the financial system is deemed to be breached and are distinct from the impact tolerance levels of individual institutions. SITOs should be a reference for authorities when assessing and developing their coordination and action capabilities that constitute the third layer of defence set out in the introduction (see also Figure 2). This is illustrated in Figure 5, which depicts the SITO as the point at which a cyber incident moves from the amplification phase to the systemic event phase.[23] In contrast, impact tolerance levels for individual institutions are more closely related to the second layer of defence (see Box 4).[24]

SITOs can assist authorities in several ways, including as a yardstick against which they can assess their own coordination and action capabilities. During a cyber incident, SITOs could assist authorities in assessing when a cyber incident poses a risk to financial stability. SITOs are also an important yardstick against which authorities can assess their response and recovery capabilities. Moreover, Section 3.3 considers how SITOs can be used to assist authorities in identifying an "intervention ladder" for response and recovery measures, including when SITOs are breached. Finally, authorities can use SITOs to anchor expectations on the maximum acceptable level of disruption to key economic functions at financial institutions, which in turn may inform institution-specific impact tolerance levels.[25]

---

22 See the ESRB (2022) **report on Mitigating Systemic Cyber Risk**.

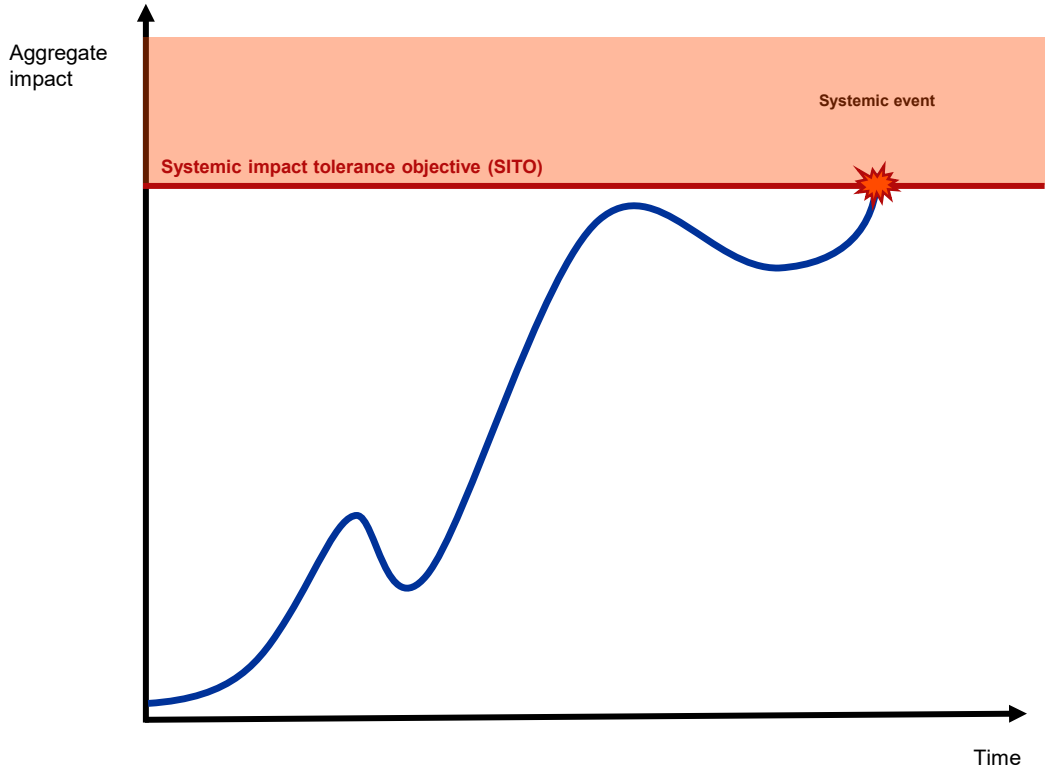
23 See Section 2.2.2 of the **ESRB's 2022 report on mitigating systemic cyber risks**.

24 See, for instance, **DORA proposal**, **ECB CROE** and the initiative overview provided in ESRB (2022).

25 Examples of cyber resilience expectations to be communicated to the financial system are set out in ECB (2018) and Bank of England (2022a).

Figure 5

SITO and evolution of aggregate impact of a cyber incident in time



Source: ESRB.

Box 4

Existing and upcoming initiatives for the financial sector related to impact tolerances

This box provides an overview of initiatives for the financial sector, including regulations and frameworks, that cover impact tolerances and operational resilience. The regulatory landscape in terms of cyber resilience focuses on individual institutions. Regulatory initiatives are also highly fragmented and typically cover only part of the financial sector (e.g. banking, insurance or market infrastructure). Most initiatives call on each institution to define their systems and data criticality and apply proportionate cyber resilience measures. One example of such an institution-specific impact tolerance level is the two-hour recovery time objective (RTO) provided for in the ECB's cyber resilience oversight expectations for financial market infrastructures.[26] In contrast, the "value date" – the date on which a payment is due – that the Bank of England set as its impact tolerance level for payments, is set system-wide.[27] Defining such institution-specific impact tolerance levels is important in assessing whether an individual institution has the capacity to

[26] See ECB (2018).

[27] See Bank of England (2021).

respond to and recover from a cyber incident that has impaired the provision of their services. Reflecting this, several authorities in the EU have considered institution-specific impact tolerances in the context of CyRST.[28] Table 1 provides a brief overview of other examples.

Table 1

Overview of initiatives analysed at an individual firm level

Initiative	Issuing authority	Scope	Includes references to impact tolerances
Principles for operational resilience	BIS	Banks	Yes, defined by financial institutions
Principles for financial market infrastructures	BIS	Financial sector	No
Guidance on cyber resilience for financial market infrastructures	BIS and IOSCO	Financial market infrastructures	No
Cross Industry Guidance on Operational Resilience	Central Bank of Ireland	Financial sector	Yes, defined by financial institutions
EBA Guidelines on outsourcing arrangements	EBA	Banks	No
EBA Guidelines on internal governance under Directive 2013/36/EU	EBA	Banks	No
EBA Guidelines on ICT and security risk management	EBA	Banks	No
Cyber resilience oversight expectations for financial market infrastructures	ECB	Financial market infrastructures	Yes, defined by authorities
Guidelines on information and communication technology security and governance	EIOPA	Insurance companies	Yes, defined by financial institutions
Guidelines on outsourcing to cloud service providers	EIOPA	Insurance companies	No
Guidelines on System of Governance	EIOPA	Insurance companies	No
Opinion on the supervision of the management of operational risks faced by IORPs	EIOPA	Institutions for occupational retirement provision (IORPs)	No
Opinion on market outages (to be published in 2023)	ESMA	Trading venues	No
DORA - Digital Operational Resilience Act	European Commission	Financial sector	Yes, defined by financial institutions
NIS Directive – cross-sectoral (EU 2016/1148)	European Parliament	Cross-sectoral	No

Source: ESRB.

[28] See Central Bank of Ireland (2021).

3.2 Operationalising SITOs

3.2.1 High-level guidance

This section provides authorities with high-level guidance on SITOs, including some basic principles. As the impact tolerance of the financial system is likely to differ depending on which key economic function is impaired, there is no single SITO and authorities need to define SITOs at the level of key economic functions. For economic functions where disruptions have no or few cross-border implications, SITOs may differ across jurisdictions and reflect national specificities. However, in a single market where key economic functions are typically provided cross-border, the ESRB is of the view that a consistent application should be pursued. With that in mind, this section includes some basic principles authorities should consider when defining SITOs.

A governance mechanism also needs to be agreed upon, although this aspect is not considered further in this report. Besides setting up SITOs, authorities must reflect on governance arrangements. This includes the questions regarding the responsibility for, and ownership of SITOs, which authority should update SITO levels and which governance processes are needed to share SITOs with other domestic and foreign authorities, as well as with financial institutions and service providers.

3.2.2 Principles

SITOs should be tailored to the key economic function concerned. Authorities should consider the particularities of each key economic function when defining SITOs.

SITOs should reflect cross-economic functions and cross-jurisdictional considerations. A systemic cyber incident may affect different key economic functions at the same time and will likely involve different jurisdictions and/or sectors. A widespread cyber incident, or an incident affecting a critical ICT third-party provider who provides the same service for different key economic functions, could result in more than one key economic function becoming impaired. Authorities should also consider contagion channels that might result in more severe disruption or impairment of key economic functions and thus lead to the definition of lower SITOs in other jurisdictions compared with their own. Authorities should also consider how SITOs should operate when more than one key economic function is affected and whether there should be any prioritisation or adjustment of SITOs in such a scenario.

SITOs should be defined conservatively. The importance of key economic functions to financial stability might differ across time and across jurisdictions. Institution-specific impact tolerance might be greater outside regulatory requirement periods or during holiday seasons. Such considerations may also impact SITOs, which should nevertheless be set conservatively.

SITOs should reflect the duration and severity of the disruption. Severe disruptions to key economic functions may cause a rapid amplification and thus quickly turn into systemic cyber events. However, as amplification channels take hold, even a disruption that is not considered to be severe in isolation may – if prolonged – result in a systemic cyber event. Therefore, when defining

SITOs, authorities need to reflect on both the severity and duration of the disruption or impairment of a key economic function.

SITOs should be based on simple metrics so that they can be easily understood and communicated. Simple metrics reduce the risk of misinterpretation and facilitate understanding and communication among different authorities and, if needed, across different parts of the financial sector and across stakeholders.

SITOs should be reviewed periodically. Defining SITOs is no easy task given the absence of experience with cyber incidents that have turned into systemic events. Authorities should be mindful that – despite their best efforts – defining SITOs will include a large element of educated guesswork. Reflecting this uncertainty, authorities should periodically review SITOs and look across key economic functions and jurisdictions for any evidence, including from exercises and incidents, that could support their calibration.

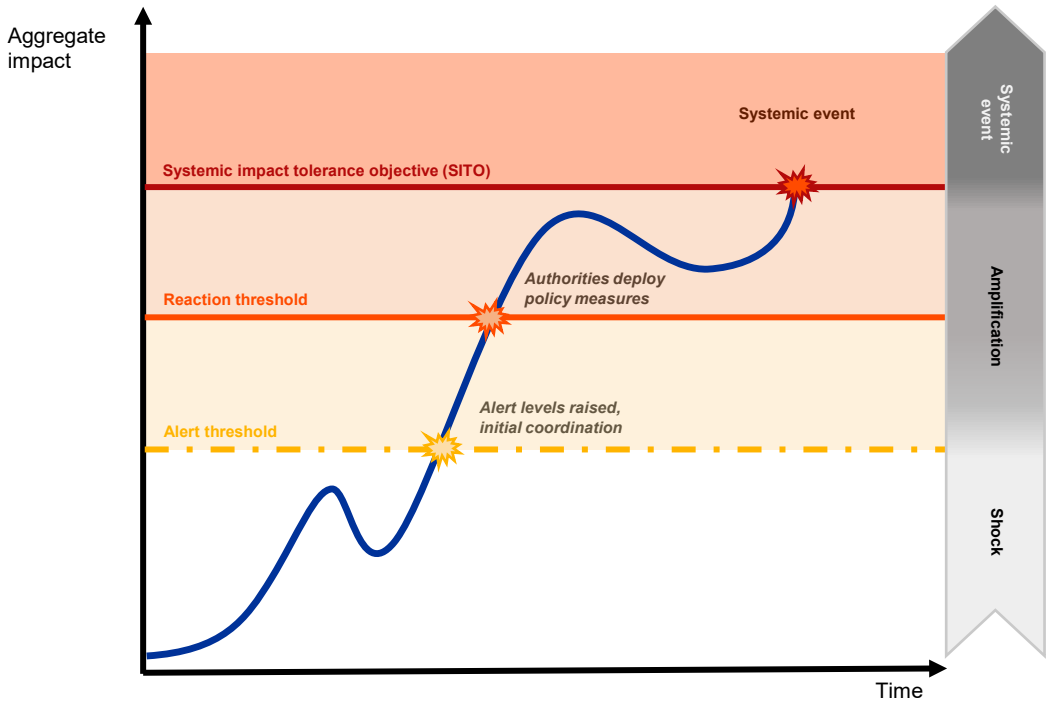
3.3 Beyond SITOs – intervention ladder thresholds

SITOs can assist authorities in identifying thresholds that form an "intervention ladder" to ensure that their coordination and action capabilities are deployed in a balanced and timely manner. Due to the scale and speed of the shock propagation of a cyber incident, its impact can increase non-linearly once amplification mechanisms are triggered. This means that authorities will want to consider deploying, or at least be ready to deploy, their coordination and action capabilities before a SITO has been breached. This might include raising alert levels, activating crisis management frameworks (e.g. EU-SCICF)[29], deploying certain policy measures or notifying other authorities, institutions and stakeholders. This is illustrated in Figure 6, which depicts alert and reaction thresholds that authorities might wish to establish at the outset and during the amplification phase of a cyber incident. Box 5 considers the relationship between SITOs and CyRST.

[29] See ESRB (2022).

Figure 6

Cyber incident impact and tolerance for different impact levels



Source: Based on ESRB (2020).

This intervention ladder can also assist authorities in deciding which measures to employ once a SITO is breached. A cyber incident has the potential to breach all three layers of defence. In this case, the cyber incident would move beyond the SITO and turn into a systemic cyber event that poses a threat to financial stability. Authorities need to prepare for this eventuality.

Box 5

Relationship between SITOs and CyRST

SITOs and CyRST are complementary analytical tools. While they are independent of each other, they can also support and inform each other. For example, an authority could establish a SITO and use CyRST to, among other things, test whether the financial system can respond and recover before a SITO is breached or whether additional contingency measures are required. Conversely, the outcome of CyRST could be one of the inputs authorities use when calibrating SITOs.

3.4 Next steps

The ESRB advocates the use of SITOs and will continue its work in transitioning from a conceptual approach to a practical basis for implementing them. Specifically, the ESRB will

identify a key economic function[30] where disruptions have cross-border implications and define appropriate SITOs at the EU level so as to ensure consistency across the region/sector and across authorities. The ESRB will work with authorities across the EU to identify where a consistent approach is required and to decide on an approach for setting SITOs where there is a need to consider cross-border implications. The ESRB recognises that where disruptions have no or few cross-border implications, SITOs may differ across jurisdictions to reflect national specificities.

[30] A list of key economic functions is provided in ESRB (2020).

4 Financial crisis management tools and systemic cyber events

This section reviews existing financial policy tools, evaluates their adequacy for responding to potentially systemic cyber incidents and identifies gaps that need to be closed. A disruptive cyber incident that affects the European financial system is inevitable.[31] Authorities therefore need to be prepared for a potentially systemic cyber event. CyRST and SITOs, as described in Sections 2 and 3, are designed to be part of authorities' analytical toolkits. However, authorities also need policy tools for managing and intervening when cyber incidents that put financial stability at risk occur. Of particular use are tools which (i) ensure that the financial system continues to provide key economic functions, (ii) preserve confidence in the functioning and stability of the financial system, and/or (iii) address the risk stemming from liquidity problems or financial losses associated with a potentially systemic cyber event. While this section focuses on financial policy tools, operational resilience crisis management tools are also needed to mitigate a system-wide or systemic cyber incident and are likely to be used before, or in conjunction with, financial policy tools.

4.1 Financial policy tools considered

This section assesses whether financial policy tools designed to prevent or mitigate general risks to financial stability could also be effective when such risks are the result of a cyber incident.[32] The section aims to help authorities with their contingency planning and to provide a foundation for improved coordination in activating and using financial policy tools across authorities and vis-à-vis financial institutions. Five tools have been considered.

- **Capital buffers** such as the counter cyclical buffer (CCyB) and the systemic risk buffer (SyRB) – whether or not authorities release them during a cyber incident – provide banks with additional loss-absorbing capacity above regulatory minima.[33]
- **Deposit insurance** could play an important role as it is designed to reduce the risk of bank runs.[34]
- **Recovery and resolution frameworks** are designed to prevent the failure of institutions or, where failure occurs, minimise negative repercussions by ensuring the resolution objectives

31 ESRB (2020).

32 Financial crises may have purely financial causes, such as in the 2007-09 global financial crisis, but financial policy tools may also be used to handle the financial consequences of non-financial events such as the onset of the COVID-19 pandemic in early 2020. A cyber incident that threatens financial stability would be another example of this.

33 See, the discussion of capital buffers in the ESRB's 2022 **Review of the EU Macroprudential Framework for the Banking Sector – A Concept Note**.

34 See, for instance, Preamble 3 of the **Deposit Guarantee Scheme Directive (DGSD)**.

are met and by preserving critical financial and economic functions and financial stability.[35] These frameworks could therefore also play a role in a cyber incident.

- **Moratorium powers and ad hoc bank holidays** may be used during resolution events to give authorities the necessary time to evaluate losses and assets, thus increasing confidence in the institutions after reopening.[36] Powers to suspend obligations or termination rights complement temporary stays, giving resolution authorities room for manoeuvre without suppliers or creditors triggering defaults in response to the call for resolution. Governments could also decide to impose ad hoc nationwide bank holidays as a crisis management tool, although this is not provided for in current regulations.[37]

- **Central bank provisions of liquidity** could also mitigate risks to financial stability by supporting solvent but illiquid institutions and systemically important markets.[38]

Some Member States have developed payment system contingency solutions that can keep payments running when wholesale systems are down or bank account data are unavailable.[39] These solutions are more operational in flavour than the financial policy tools above. However, the solutions do have a financial element, as they entail either (i) the provision of credit between institutions and to their customers or (ii) obliging institutions to hold liquidity buffers and recommending that the public hold liquidity buffers.

The dispersion of financial policy tools across authorities requires effective coordination between authorities and with firms. The tools are scattered across macroprudential authorities, central banks, deposit insurers, payment system authorities, financial institutions and other private entities. This requires effective coordination between authorities and with firms, although the practicalities of this aspect are not considered in this report.

4.2 Key findings

The effectiveness of existing financial crisis management tools in responding to a cyber incident depends on the severity of the impact on the financial system and the speed with which it propagates. In general, authorities have a host of crisis management tools at their disposal if authorities, financial infrastructure and some financial institutions remain operational during a cyber incident. This is addressed in Section 4.2.1. In situations where financial infrastructure, financial institutions and the authorities themselves are largely operationally impaired, there is little authorities can do. There are, however, payment contingency measures that may help to mitigate the fallout of such a severe cyber incident. These tools are considered in Section 4.2.2.

---

35 See, for instance, Preamble 5 of the **Bank Recovery and Resolution Directive (BRRD)**.

36 For instance, Article 33a of the BRRD gives resolution authorities the power to suspend banks' obligations for a limited period.

37 On the use of bank holidays, see, for example, Laeven and Valencia (2018).

38 See, for instance, Bindseil (2014) for a detailed discussion on central bank liquidity in normal and crisis situations.

39 As described in Box 4 and the **Risk and Vulnerability Report of the Norwegian Financial Supervisory Authority (Finanstilsynet)** (2022) (currently only in Norwegian).

4.2.1 Scenarios where financial policy tools could be effective

In scenarios where some financial institutions are in operation and financial infrastructure, authorities and central banks are also still operable, several of the financial policy tools set out above might mitigate the potential threat to financial stability.

4.2.1.1 Capital buffers

A release of capital buffers may enhance the ability of the financial sector to provide credit to the economy in a severe cyber incident. In a system-wide cyber incident (or when such an incident has turned into a systemic event), some banks could be operationally unable to provide credit to the economy. Even banks that remain operational could face large financial losses, either because of severe credit impairments or owing to theft and ransom. These capital constraints would impair banks' ability to provide credit to the real economy. Macroprudential authorities may therefore consider releasing capital buffers so that banks still in operation would be able to provide more credit than they otherwise would be able to.

Authorities should reflect on whether capital releases need to be larger than is usually the case for non-cyber-related cyclical situations. This would give operable banks a larger capacity to provide credit in situations where many banks are out of operation. This may require calibrating the use of capital buffers specifically for cyber risk, which is neither currently done nor foreseen.

4.2.1.2 Deposit insurance

Deposit insurance ensures that depositors have access to money once their deposits become unavailable, which reduces the risk of runs against banks that are still in operation. Deposit insurance schemes reimburse eligible depositors when their funds become unavailable. In practice this often means that the credit institution is under national insolvency proceedings, i.e. the credit institution has failed but has not been put in resolution.[40] While there are no examples of such a scenario in the EU, a cyber incident can also lead to deposits at affected banks being unavailable if their systems become operationally impaired. Seeing that depositors of banks that are operationally impaired do not have access to their deposits may affect the confidence of depositors of banks that remain operational. This could lead to runs on those banks. If restoring access to deposits is not possible, and there are no prospects that it will be possible in the near future, the authorities may want to be able to determine that deposits are unavailable, such that they can reimburse depositors under insurance guarantee schemes. This might help restore confidence that deposits are safe and thus reduce the risk of runs against unaffected banks in such situations.

There is a need for clarity on whether operational unavailability stemming from a cyber incident would be sufficient to enable the relevant authorities to trigger a deposit payout. According to the Deposit Guarantee Scheme Directive (DGSD), authorities need to decide if the specific conditions have been met before determining that deposits are unavailable and discern

[40] See Article 2, definition (1) of the **Bank Recovery and Resolution Directive (BRRD)**.

whether unavailability is directly related to the institution's financial circumstances. The review by the European Commission of the conditions under which deposit insurance can be paid out should provide clarity on whether a cyber incident would constitute sufficient grounds under the DGSD. The European Banking Authority's opinion to the European Commission[41] points out that it makes little difference to depositors whether their deposits are unavailable for financial or other reasons. It also states that bank runs may occur on healthy institutions owing to a general loss of confidence in access to deposits unrelated to insolvency. Thus, as the European Banking Authority (EBA) has recommended, more clarity is needed on how to treat cases where lack of access to funds is not directly linked to the institution's financial circumstances, but stems from other reasons, such as a cyber incident.

4.2.1.3 Recovery and resolution frameworks

Recovery and resolution frameworks seek to reduce the likelihood of failure and ensure continuity of critical functions if failure occurs, preserve financial stability and minimise spillover effects. Recovery plans are triggered upon hitting certain predefined thresholds, while resolution plans and tools are to be deployed when financial institutions, deemed important for the public interest, are failing or likely to fail.

The recovery and resolution framework can be adapted to a cyber incident scenario. When a cyber incident unfolds, the consequences can materialise so rapidly that recovery plans may not be implementable in time. Operational continuity plans will be activated earlier and will therefore be more relevant for preventive purposes. The recovery plan and ICT business continuity policy of financial institutions should be well integrated in the crisis management governance of institutions. In the same vein, DORA lays the foundation for increased coordination, communication and joint crisis management exercises involving competent authorities, resolution authorities, the ECB, the Single Resolution Board, the ESRB and ENISA in response to cyber attack scenarios.

Resolution tools and powers aim to ensure the continuation of critical functions of institutions that are failing or likely to fail. Resolution authorities, with the input of the institutions concerned, need to identify critical services, including critical IT services. In this identification process, the institution needs to report whether the contract is resolution-proof (i.e. a resolution action will not trigger termination of the contract) and determine the time to substitution. Having substitution options for critical IT services could be an option in overcoming an incident affecting service providers.

4.2.1.4 Moratorium powers and bank holidays

Moratorium powers allow authorities to stop transactions such as payments and could be applied to financial institutions that have been impaired by a cyber incident. They allow the authorities to value the assets of a financial institution and to assess whether it is failing or likely to fail. In the case of a cyber incident, a moratorium may also buy institutions time to perform remedial

41 See European Banking Authority (2019).

actions on the IT infrastructure, thereby increasing the public confidence in the institution. Resolution authorities' powers to suspend termination rights could be used to the same effect: allowing more time to assess the situation and make a decision without spreading externalities to third parties or to the wider economy. Governments could also decide to impose ad hoc nationwide bank holidays as a crisis management tool, although this is not provided for in current regulations.[42]

Moratoria and ad hoc bank holidays that last a long time risk eroding public confidence, which could trigger adverse effects. They can have major consequences for an institution's customers and – if the institution is systemically important – for the wider economy. Therefore, a prolonged moratorium or an extended period of ad hoc bank holidays might reduce the public's confidence in authorities and hence in the institutions under their jurisdiction.

4.2.1.5 Central bank provisions of liquidity

The ESRB does not prejudge the actions central banks might take in response to a cyber incident. Central banks have different mandates, and each central bank will manage its balance sheet accordingly. Reflecting this, whether a central bank would be willing to provide extra liquidity during a cyber incident depends on how a specific situation interacts with its mandate. This subsection therefore considers how central bank liquidity provision could help mitigate risks from a cyber incident and what operational and practical challenges could hamper a central bank's ability to provide liquidity.

Central bank liquidity provision during a cyber incident would mitigate risks to financial stability by supporting solvent but illiquid institutions and systemically important markets. In a system-wide cyber incident, solvent financial institutions may face liquidity problems owing to the inability of other institutions to make and receive payments.[43] Furthermore, loss of confidence can increase risk premia and reduce the willingness to invest and lend. This may lead to liquidity strains for financial institutions and reduce liquidity in financial markets. Market access may be impaired not only for the financial institutions affected by a cyber incident but also for other market participants. Both channels may reduce the financial sector's ability to perform functions such as making payments and providing credit. Central bank liquidity provision during a cyber incident would mitigate risks to financial stability. For instance, in the United States, research shows that access to the Federal Reserve liquidity facilities was successful in mitigating the impact of a cyber incident on the banking sector.[44]

Liquidity provision by central banks during a cyber incident may be hampered by operational and practical challenges. First, it could be that not all central banks have the operational capacity and legal frameworks in place to provide liquidity beyond the banking sector. Central banks typically only transact directly with banks, although some central banks also transact with a wider range of financial counterparties such as broker dealers and central counterparties.[45]

---

42 For a historical example, albeit not related to a cyber incident, see Jabaily (2013).

43 See, for instance, Eisenbach et al. (2020).

44 For an analysis of a specific cyber event that led to liquidity problems in the Federal Reserve Funds Market and the use of Federal Reserve liquidity tools, see Kotidis and Schreft (2022).

45 See, for example, the section on "Eligible participants" in the **Bank of England Market Operations Guide**.

Second, it could be that not all central banks are able to quickly provide liquidity in a foreign currency. Liquidity provision in foreign currency presupposes that a central bank has sufficient holdings in that foreign currency or can quickly activate a swap or repo line with the central bank of issue.[46] Third, a lack of data may complicate the standard steps that central banks typically follow when providing emergency liquidity to financial institutions. Such steps include assessing an institution's solvency and valuing and taking legal ownership of collateral. Fourth, extraordinary central bank liquidity provision to individual institutions may take a long time, especially if the affected institutions have not prepared for it and/or if many institutions are affected at the same time. Fifth, coordination problems owing to different responsibilities across authorities – including central banks – may delay or hamper pre-announcements of liquidity provisions or other forms of communication aimed at reassuring the public. Cyber-specific crisis management exercises at central banks could, however, be expanded to test the ability of central banks to provide liquidity to the financial system when facing operational and practical challenges that arise from a cyber incident.

4.2.1.6 Coordination and communication among authorities

The use of financial policy tools calls for increased coordination and communication among authorities. Even within a Member State, the financial policy tools described above are not necessarily in the hands of a single authority. And a cyber incident is likely to affect and require action from multiple jurisdictions. Therefore, relevant authorities in the EU will need to coordinate among themselves and with authorities outside their usual interactions. Unless authorities are prepared for these interactions, they might be at risk of taking inconsistent actions that contradict or jeopardise other authorities' responses. To address this risk, the ESRB issued a recommendation in 2022 on the establishment of a pan-European cyber crisis management framework to improve crisis coordination among authorities.[47]

4.2.2 Severe scenarios where traditional financial policy tools are inefficient

Traditional financial policy tools may be ineffective in severe cyber scenarios, though measures exist to protect some limited critical payment functions. In scenarios where large parts of the financial system have been impaired by a cyber incident and most (if not all) financial infrastructures are out of operation, the availability of financial tools is far more limited. However, even in these scenarios, measures can be activated to protect certain critical payment functions.

Cash holdings by the public as a general contingency measure can maintain payments for necessities in a large range of scenarios. If the public holds some cash as a liquidity buffer and

---

46 The ECB is part of a swap line network consisting of standing bilateral arrangements with five other major central banks (the Bank of Canada, the Bank of Japan, the Swiss National Bank, the Bank of England and the Federal Reserve System). In response to the coronavirus (COVID-19) crisis, the ECB swiftly reactivated existing swap lines with a number of central banks and also set up new ones, as well as new bilateral repo lines with several non-euro area central banks. See **ECB central bank liquidity lines**.

47 See Recommendation of the European Systemic Risk Board of 2 December 2021 on a pan-European systemic cyber incident coordination framework for relevant authorities (**ESRB/2021/17**).

contingency measure, some retail payments can still be made in the most severe cyber incidents and even situations involving an electricity outage. This is a general recommendation from security authorities, at least in some jurisdictions. Certain jurisdictions also insist that banks be able to distribute cash to the public under severe disruptions. This may pose specific challenges in a cyber incident, owing, for instance, to data availability.

In some jurisdictions, contingency measures – such as reserve solutions in payment terminals and cash holdings at banks – can be activated if part of the payment system is unavailable. If the public have credit cards, they will still be able to access some payment services during a cyber incident. These contingency measures typically aim to provide payment opportunities to the public in the wake of severe operational disruptions. They are also relevant in situations where payments cannot be made due to a cyber attack. Specifically, payment terminal contingency solutions, as described in Box 6, may cover a larger range of scenarios, provided that electricity or batteries are available. These solutions can function even with a lack of deposit information, closed financial institutions and impaired infrastructure and are triggered automatically.

By enabling the availability of payments, these measures may also enhance public confidence in the financial system. Maintaining trust in the financial system and banks may reduce the risk of liquidity shortages at banks that are unaffected by the cyber incident.

Few measures are unconditionally available when a cyber incident has proliferated beyond the financial infrastructure and all financial institutions are out of operation. The payment tools described above are typically limited for use in paying for consumer goods, and to some extent only for necessities. Furthermore, cash as a contingency measure in a range of scenarios requires the individual consumer to have cash at hand and/or access to cash withdrawal services.

Box 6
Reserve solutions in payment terminals

A cyber incident can impair banks and financial infrastructure systems to the extent that payments cannot be processed in a normal way. In some jurisdictions within the European Economic Area (EEA), contingency solutions are currently in place for situations in which bank deposit information and/or financial infrastructure such as settlement systems are unavailable or corrupted. This box describes such contingency solutions that operate in Norway.[48]

The Norwegian reserve solution is implemented by BankAxept AS, which also operates the system for Norwegian domestic debit card scheme BankAxept. The solution is embedded in the payment terminals (point of sale terminals), which handle both debit and credit cards. They can be found at places of purchase such as shops, service stations, hotels and restaurants in Norway. However, the solution only works for the BankAxept card scheme and not for others.

This solution ensures that debit card payments can be processed without the verification of a personal identification number (PIN)[49] and account data for up to six hours. The cardholder can

[48] For backup arrangements to secure daily payments in the event of serious disruptions to society or emergency conditions that would prevent the use of normal payment systems in Finland, see the **press release from the Ministry of Finance of Finland**.

[49] New cards have PIN control in the chip and from June 2023 all BankAxept cards will have offline PIN control.

make the payment and the merchant is guaranteed settlement. The cardholder must sign for the transaction and there is a limit (NOK 1,500/EUR 150) on the size of such transactions. For amounts exceeding the set limit, the merchant must call the bank to authorise the transaction. However, the absolute maximum amount for any such purchase is NOK 10,000 (EUR 1,000). The solution does rely on electricity but does not require that payment terminals are online. There are certain requirements regarding the storage capacity and processing speed of the payment terminals. Payments will be processed as normal when contact with banks and settlement systems resumes. The solution imposes no extra costs on the merchant.

The solution was used on 16 May 2022, when there was a significant number of retail transactions owing to Norwegian Constitution Day on the following day. A network incident affected 90,000 payment terminals in Norway for several hours and a substantial portion of transactions that day were processed using the reserve solution.

An extended version of the payment terminal solution has been in place since 2021, and it is able to cope with extreme incidents in which payment terminals remain out of contact with infrastructure and banks for up to seven days. This extended version is only available to providers of necessities such as groceries, medicines and fuel, and only for merchants with a regional or nationwide presence. There is again a limit on each individual transaction and a special procedure for authorising amounts above the limit, yet once again there are no costs to the merchant and settlement is guaranteed. The solution can result in a substantial amount of credit to bank customers and between the banks that participate in BankAxept. The potential use of these types of solutions is limited, but may be very helpful in extreme situations where access to payments is impaired over a long period.

4.3 Next steps

The effectiveness of financial policy tools relies on their operational availability and on the availability of a minimum set of critical functions in the financial system. This underscores the importance of the operational resilience of financial institutions and authorities. Work is also needed on the interaction and interdependencies between financial crisis management tools and other operational crisis management tools. Reflecting this, the ESRB will consider which operational policy tools are most effective in responding to a system-wide cyber incident and identify gaps across operational and financial policy tools. It will also consider whether tools beyond existing financial and operational tools are needed to effectively respond to a systemic cyber event.

5 Conclusion

The geopolitical situation has increased cyber risk, calling for a step change in enhancing cyber resilience. The risk of a cyber incident turning into a systemic event was already identified by the ESRB in previous years. The war in Ukraine, the broader geopolitical landscape and the increasing use of cyber attacks have significantly heightened the cyber threat environment. Beyond incidents without a malicious motive, there is an increased risk of cyber attacks on the EU financial system by states or state-sponsored actors. The ESRB's initial response has been to enhance cyber threat intelligence sharing across all ESRB member institutions and the Bank of England. Yet the current cyber threat environment calls for a step change in the EU's efforts to enhance cybersecurity including by operationalising the approaches to cyber resilience considered in this report.

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

- **The ESRB encourages authorities to use the CyRST approach to pilot system-wide cyber resilience scenario testing as soon as possible.** Such pilots would help authorities learn about this analytical tool and deepen their understanding of the risks to system-wide cyber resilience. This is both important and urgent given the increased likelihood of a cyber attack affecting the European financial sector and because it will take time to pilot CyRST, identify the risks and implement appropriate mitigating measures. The ESRB will continue to work in this area as a hub for sharing progress and good practice, and for updating the conceptual approach based on what the authorities learn from their more detailed work on the pilots.

- **The ESRB advocates the use of SITOs and will continue to transition from a conceptual approach to a practical basis for implementing them.** Specifically, the ESRB will identify a key economic function[50] where disruptions have cross-border implications and define appropriate SITOs at the EU level so as to ensure consistency across the region/sector and authorities. The ESRB will work with authorities across the EU to identify where a consistent approach is required and to decide on the approach for setting SITOs where there is a need to consider cross-border implications. The ESRB recognises that where disruptions have no or few cross-border implications, SITOs may differ across jurisdictions to reflect national specificities.

- **The ESRB will consider which operational policy tools are most effective in responding to a system-wide cyber incident and identify gaps across operational and financial policy tools.** This work will build on the analysis of financial crisis management tools described in this report.

[50] A list of key economic functions is provided in the ESRB 2020 report on **systemic cyber risk.**

References

Bank of England (2021), "**Operational resilience: Impact tolerances for important business services**"*, Policy Statement*, Prudential Regulation Authority, March.

Bank of England (2022a), "**Operational resilience: Impact tolerances for important business services**", *Supervisory Statement*, Prudential Regulation Authority, March.

Bank of England (2022b), "**Prudential Regulation Authority statement on the 2022 cyber stress test: Retail payment system**", December.

Bank of England, "**Bank of England Market Operations Guide: Our tools**".

Bindseil, U. (2014), *Monetary Policy Operations and the Financial System*, Oxford University Press, Oxford.

Central Bank of Ireland (2021), "**Cross Industry Guidance on Operational Resilience**", December.

Danish Financial Supervisory Authority (2022), "**Project on cyber stress test**", *Press release*, June.

Danmarks Nationalbank (2022), "**Financial sector forum for operational resilience (FSOR)**", November.

Eisenbach, T.M., Kovner, A. and Lee, M.J. (2020), "**Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis**", Staff Reports, Federal Reserve Bank of New York, May.

European Banking Authority (2019), "**EBA publishes Opinion proposing to further strengthen depositor protection in the EU**", *Press release*, October.

European Central Bank (2018), "**Cyber resilience oversight expectations for financial market infrastructures**", Frankfurt am Main, December.

European Central Bank (2022), "**Central bank liquidity lines**", Frankfurt am Main.

European Parliament (2014), **Deposit Guarantee Scheme Directive (DGSD)**, April.

European Parliament (2014), **Bank Recovery and Resolution Directive (BRRD)**, May.

European Parliament (2022), **Digital Operational Resilience Act (DORA)**, November.

European Systemic Risk Board (2020), "**Systemic cyber risk**", Frankfurt am Main, February.

European Systemic Risk Board (2022), Recommendation of the European Systemic Risk Board of 2 December 2021 on a pan-European systemic cyber incident coordination framework for relevant authorities (**ESRB/2021/17**).

European Systemic Risk Board (2022), "**Review of the EU Macroprudential Framework for the Banking Sector – A Concept Note**", Frankfurt am Main, March.

European Systemic Risk Board (2022), "**Mitigating systemic cyber risk**", Frankfurt am Main, January.

Europol (2020), "**Internet Organised Crime Threat Assessment (IOCTA)**".

Financial Stability Board (2018), "**Cyber Lexicon**", November.

Financial Supervisory Authority of Norway (2022), "**The risk and vulnerability report**", *Press release*, May (only in Norwegian).

Jabaily, R. (2013), "**Bank Holiday of 1933**", *Federal Reserve History*, November.

Kotidis, A. and Schreft, S.L. (2022), "**Cyberattacks and Financial Stability: Evidence from a Natural Experiment**", *Finance and Economics Discussion Series* (FEDS), Federal Reserve Board, Washington.

Laeven, L. and Valencia, F. (2018), "**Systemic Banking Crises Revisited**", *IMF Working Paper*, No 18/206, September.

Prenio, J. and Restoy, F. (2022), "**Safeguarding operational resilience: the macro-prudential perspective**", *FSI Briefs*, Financial Stability Institute, Bank for International Settlements, August.

Imprint and acknowledgements

This report was approved by the ESRB General Board on 1 December 2022. 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

Aoife Langford
Central Bank of Ireland and Workstream lead

Borut Poljšak
Banka Slovenije

Carla Marques
Banco de Portugal

Catherine Brodie
ECB

Christoph Fricke
ESRB Secretariat and Secretary to the ESCG until August 2022

Christoph von Busekist
Deutsche Bundesbank

Constantinos Christoforides
ECB

Daniela Lo Monaco
Banca d'Italia

Diana Vieira
EIOPA

Francesco Mazzaferro
ESRB Secretariat and Co-chair of the ESCG

Francesco Sciamanna
Banca d'Italia

Hanna Freystatter
Suomen Pankki – Finlands Bank

Jeremiasz Nowakowski
Narodowy Bank Polski

Joanna Bibby-Scullion
Bank of England

José Munera
Banco de España and Workstream lead

Lea Joensen Farø
Danish FSA

Marie Schelde Holde
Danish FSA

Michael Scharf
ECB

Olaf Weeken
ESRB Secretariat

Olav Johannessen
Finanstilsynet

Pascal Jourdain
Banque de France

Paul Williams
Specialist Advisor

Sara Batres
ESRB Secretariat and Secretary to the ESCG from September 2022

Signe Marie Degn
Danmarks Nationalbank

Simon Schumacher
BaFin

Stephanie Galati
EIOPA

Theresa Nabel
BaFin

Vadim Kravchenko
ECB

Ylva Søvik
Norges Bank and Workstream lead

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 978-92-9472-325-3, doi: 10.2849/74787, DT-07-23-053-EN-N