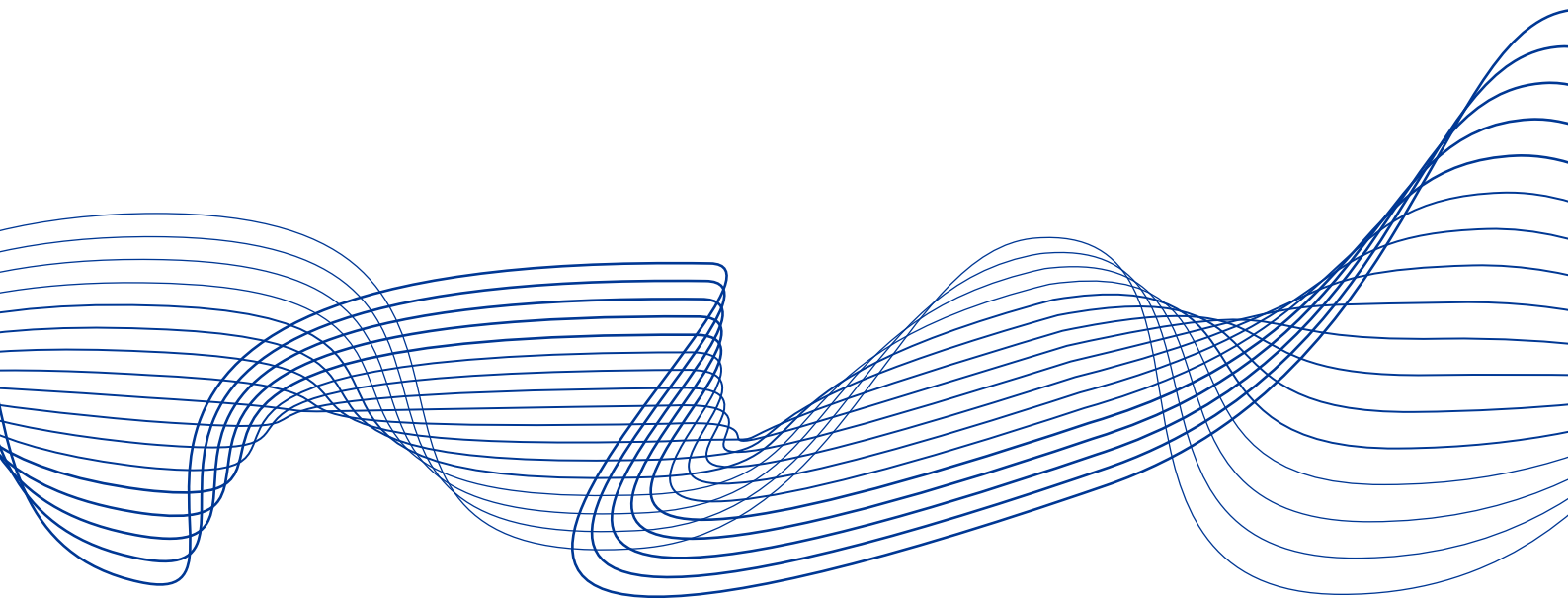
Mitigating systemic cyber risk

January 2022



ESRB
European Systemic Risk Board
European System of Financial Supervision

Contents

Executive summary

The constantly evolving cyber risk landscape and recent increase in cyber incidents are indicators of a greater threat to financial stability within the European Union. In the worst case, a cyber incident could affect operational systems in the financial system and impair the provision of critical economic functions, trigger financial contagion or lead to an erosion of confidence in the financial system. If the financial system is not able to absorb these shocks, financial stability is likely to be put at risk and a systemic cyber crisis could unfold (ESRB, 2020).

Of particular importance is the need to overcome the risk to financial stability stemming from a coordination failure during the response to an incident. A cyber incident's scale, speed and propagation call for a swift response from firms and financial authorities in order to preserve financial stability. Financial authorities in the EU need to coordinate among themselves, at global level and with parties that they do not usually interact with, such as cyber authorities. The risk of a coordination failure by authorities also exists. Uncoordinated action could contradict or even jeopardise the response of other authorities, lead to an erosion of confidence in the functioning of the financial system and thereby amplify the shock for the financial system. In the worst case, financial stability may be threatened.

This report identifies the need for the establishment of a pan-European systemic cyber incident coordination framework (EU-SCICF) to mitigate the risk of a coordination failure. The objective behind such a mechanism is to increase the level of preparedness of financial authorities in the EU and to define a coherent and thus more effective response to a cyber incident. The EU-SCICF should help bridge any coordination and communication gaps between financial authorities themselves, with other sector authorities and with other key actors at international level. As such, it should complement existing coordination and communication protocols. To ensure the non-duplication of frameworks, the EU-SCICF should correlate with the existing financial crisis framework and EU cyber incident landscape.

European financial authorities are well placed to support the implementation of an EU-SCICF. Successful management of a systemic cyber crisis will depend on the capabilities of each financial authority to interact with other financial and cyber authorities at European level. Here, the principles underpinning the EU-SCICF mechanism should serve as a reference point for the required capabilities of European financial authorities.

A new set of macroprudential tools is required to address systemic cyber risk. An all-encompassing set of tools should address both cyber and financial risk stemming from cyber incidents. It should complement the existing strategies and instruments of microprudential and oversight authorities in this domain. While macroprudential authorities are familiar with addressing financial risk, addressing cyber risk is somewhat new. Consequently, the current macroprudential policy framework has limited capacity to develop specific mitigants and needs to be amended. Moreover, a better understanding of systemic cyber risk is required.

This report presents a strategy for developing the capabilities needed to mitigate the risk of financial instability in the event of a cyber incident. It reviews the current macroprudential framework and suggests how it could be adapted to better address the risks and vulnerabilities

stemming from systemic cyber risk. Furthermore, the report sets out how macroprudential authorities should improve their analytical and monitoring capabilities and discusses mitigants which could contribute to financial stability.

A monitoring and analytical framework for systemic cyber risk needs to be implemented in order to help design and calibrate this new set of macroprudential tools. The report presents an overview of monitoring concepts that require further reflection by the ESRB on their implementation. Systemic cyber resilience stress tests are identified as a valuable tool to test how systemic institutions in the financial system would respond to and recover from a severe but plausible cyber incident scenario. To draw conclusions from systemic cyber resilience stress tests on financial stability, macroprudential authorities need to define an acceptable level of disruption to operational systems providing critical economic functions. To increase the understanding of vulnerabilities and contagion channels in the financial system, systemically important nodes at financial and operational level need to be identified – including third-party providers through cyber mapping.

The ESRB intends to explore a monitoring and analytical framework for systemic cyber risk and required tools to address this risk in its future work. In doing so, it could provide advice for the legislative review of the EU macroprudential framework, as requested by the European Commission.[1]

[1] See European Commission (2021b).

1 Introduction

The coronavirus (COVID-19) pandemic has highlighted the importance technology plays in allowing the financial system to operate. Authorities and institutions have had to adapt their technological infrastructure and risk management frameworks to a sudden increase in remote working. According to Europol (2020), this remarkable shift towards remote and hybrid working has increased the overall exposure of the financial system to cyber threats and allowed criminals both to devise new modi operandi and adapt existing ones to exploit the situation. Against this background, the number of cyber incidents reported to ECB Banking Supervision in 2020 increased by 54% compared with 2019.[2] The SolarWinds incident was also notable in 2020, forcing several US federal agencies to shut down their affected systems immediately.[3] This forced action was remarkable in the sense that the SolarWinds software was not seen as business-critical in many cases. The SolarWinds incident highlights in particular the large scale and thereby potential systemic impact of cyber incidents.

While cyber risk has increased, the financial system has to date not experienced a cyber incident[4] that impairs financial stability (systemic cyber risk[5]). However, rating agencies see cyber risk rising for all sectors and have already started to incorporate cyber risk into their credit rating models.[6] Successful cyberattacks on hospitals during the COVID-19 crisis in Europe and the attack on the Colonial Pipeline in the United States have the potential to be replicated within the financial industry.

Cyber incidents, including cyberattacks, could pose a systemic risk to the financial system given their potential to disrupt critical financial services and operations and thereby impair the provision of key economic functions (Figure 1). A cyber incident could cause operational disruption, inflict reputational damage on the financial system and result in financial loss. Amplification of the initial shock could occur either through operational or financial contagion or through an erosion of confidence in the financial system. If the amplification mechanism is triggered, the original shock is likely to be transmitted through the financial system and may even entangle financial institutions that were unaffected by the initial cyber incident. While the later stages of a systemic cyber crisis can resemble a more traditional financial crisis, the impairment of the financial system's operability adds a new dimension to crisis management, including systemic mitigant activation.

Financial authorities from microprudential supervision and financial market infrastructure (FMI) oversight continue to incorporate cyber resilience into their supervisory frameworks and approaches to supervision. At an institutional level, these initiatives reduce both the probability of a cyber incident occurring ex ante and the impact ex post if one does occur. The

2 See ECB (2021a).

3 The SolarWinds attack is also known as the Sunburst attack. For more information, see CERT-EU (2021).

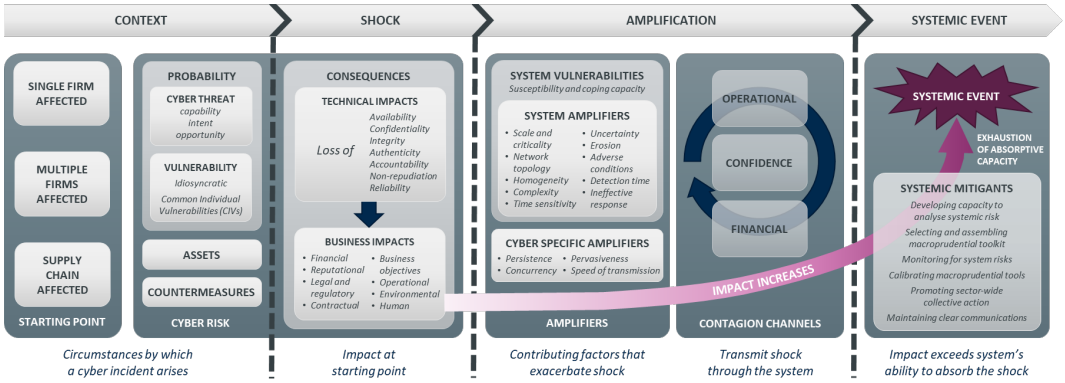
4 This report adopts the definition of a cyber incident employed by the FSB (2018), i.e. an event that jeopardises the cyber security of an information system or the information the system processes, stores or transmits; or violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not.

5 Similar to the definition of cyber risk employed by the FSB (2018), systemic cyber risk is defined as the combination of the probability of cyber incidents occurring and their impact on financial stability. For more details, see ESRB (2020).

6 Moody's (2021).

recent European Commission proposal on digital operational resilience (Digital Operational Resilience Act, DORA)[7] also envisages the inclusion of critical information and communication technology (ICT) third-party service providers that financial institutions depend on in order to deliver their critical functions. This approach marks an important step towards a comprehensive oversight framework of critical entities providing ICT services to the financial system. The systemic dimension of cyber risk is referenced in the current DORA proposal. It indicates that EU financial authorities, including the ESRB, may identify common cyber vulnerabilities and risks across sectors.[8] These initiatives assist in reducing the potential threat to financial stability that arises from the aggregate impact of cyber risk at individual institutions. From a system-wide perspective, such initiatives should be complemented by tools that mitigate the propagation or amplification of risk, thus limiting the systemic impact of a cyber incident.

Figure 1
Systemic cyber risk model



Source: ESRB (2020).

The operational dimensions and the potential scale and speed of cyber shock propagation require the strengthening of system-wide resilience against cyber risk. Macroprudential authorities, in conjunction with others, can contribute to this. It is the responsibility of macroprudential authorities to address and deal with the broader consequences of a cyber incident for the whole financial system. Such a task may require expanding or adjusting the macroprudential toolkit to ensure financial stability in the event of a major cyber incident. A precondition for this is a comprehensive understanding of the vulnerabilities and financial stability risks associated with major cyber incidents. Furthermore, the speed of shock propagation requires macroprudential authorities, in close cooperation with other authorities involved in cyber crisis management, to ensure a high level of preparedness to act quickly in times of crisis. Against this background, the ESRB report on systemic cyber risk asked macroprudential authorities to reflect on and

7 **Proposal for a regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014** (COM(2020) 595 final).

8 See DORA proposal, Article 43.

operationalise their responses, coordination and communication plans in the event of a systemic cyber event.[9]

This report presents a strategy for developing the capabilities needed to mitigate the risk of financial instability in the event of a cyber incident. It reviews the current macroprudential framework and suggests how it could be adapted to better address the risks and vulnerabilities stemming from systemic cyber risk. Furthermore, the report sets out how macroprudential authorities should improve their analytical and monitoring capabilities and discusses mitigants which could contribute to financial stability. The work by macroprudential authorities should aim to interact with and complement existing microprudential and oversight initiatives to increase the overall mitigation capabilities for systemic cyber risk.

Of particular importance is the need to overcome the risk to financial stability stemming from a coordination failure during the response to an incident. The report identifies the need for a future pan-European systemic cyber incident coordination framework (**EU-SCICF**). The objective of a future EU-SCICF is to enable swift communication and coordination among financial supervisory and oversight authorities and with other authorities in this field to avoid a coordination failure.

9 See ESRB (2020), Section 4.2, p. 42.

2 A strategy to mitigate systemic cyber risk

Macroprudential authorities can contribute to mitigating the probability of a cyber incident triggering a systemic cyber crisis and threatening financial stability. Systemic cyber risk can be addressed by systemic mitigants which reduce the likelihood of a cyber incident occurring in the first place or, where it does occur, decrease its impact through the mitigation of risk amplifiers and contagion channels. Here, microprudential and oversight authorities have developed specific tools, and the implementation of corresponding mitigants may fall within their responsibility.[10] While these ex ante preventive microprudential tools address a cyber incident in the early phases of a systemic cyber crisis (see Figure 1), they do not address the amplification and contagion of such a crisis once it has occurred. Thus, the toolkit for systemic cyber crises needs to be complemented by macroprudential tools.

Existing macroprudential tools are not designed specifically to manage the impact of a cyber incident and thus have limited capability to serve as systemic cyber risk mitigants. Applying existing tools directly in the context of systemic cyber risk may overburden these tools by forcing them to fulfil a role they are not designed for. As a consequence, some systemic cyber risk aspects may remain unaddressed. Furthermore, their design and calibration rely on the assumption of functioning operational systems, which may not be the case in a systemic cyber crisis. A cyber incident with high speed and large scale of shock propagation may render the use of existing microprudential and macroprudential tools (operationally) ineffective. To limit the build-up of systemic cyber risks, systemic mitigants specific to cyber risk need to be developed and implemented at EU level.

A limited set of existing macroprudential tools to address systemic cyber risk calls for new tools that address the systemic risk component. Such new tools can provide backstops before a cyber incident evolves into a conventional systemic event. Of particular use are macroprudential tools that help prevent the cyber incident from spilling over from the operational to the financial level or from affecting confidence in the financial system.

Macroprudential policy can build on and complement the existing microprudential and oversight regulatory framework on cyber resilience by addressing the systemic component of cyber risk. For example, banking regulation calls for system recoveries according to business needs, and regulations of FMI payment systems define operation resumption times.[11] Macroprudential authorities could, in close cooperation with supervisory and oversight authorities, define operational resilience[12] requirements that ensure financial stability in severe but plausible cyber incident scenarios, thus helping to identify and address such cyber vulnerabilities.

---

10 For example, such collaboration between microprudential and macroprudential authorities is envisaged for the designation of critical ICT third-party service providers for which the impact on financial stability is also considered. See DORA proposal, Article 28.

11 See EBA (2019) and **Regulation (EU) 2021/728 of the European Central Bank of 29 April 2021 amending Regulation (EU) No 795/2014 on oversight requirements for systemically important payment systems (ECB/2021/17) (OJ L 157, 5.5.2021, p. 1)**. For further details, see ENISA (2021a).

12 Following IOSCO (2020), the term operational resilience refers to the ability of regulated entities, other firms such as service providers, and the financial market as a whole to prevent, respond to, recover, and learn from operational disruptions. BCBS (2021) defines operational resilience as the ability of a bank to deliver critical operations through disruption.

While macroprudential authorities are familiar with addressing financial risk, addressing cyber risk is somewhat new. At the same time, conventional macroprudential concepts such as systemic relevance, concentration risk, interconnectedness and contagion effects carry importance in the context of cyber risk but may need to be applied in new ways to capture cyber aspects. Overall, macroprudential authorities need to increase their analytical and monitoring capabilities for systemic cyber risk to develop, calibrate and activate adequate mitigants.

A macroprudential strategy for mitigating systemic cyber risk needs to be developed and implemented. At EU level, this should be incorporated into the ESRB macroprudential policy framework.[13] Following the ESRB's macroprudential strategy (see Figure 2), the macroprudential framework should be amended in three ways to ensure financial stability in the event of a systemic cyber crisis:

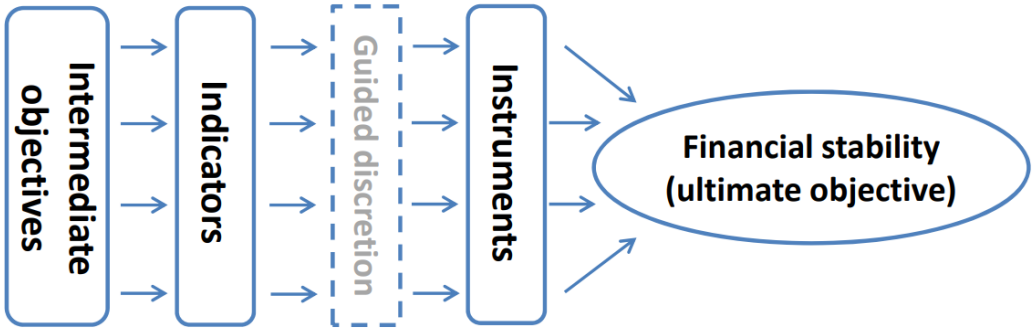
1. the inclusion of systemic cyber risk aspects in the intermediate objectives (IOs) of the ESRB policy framework such that it provides the conceptual and formal basis to address systemic cyber risk (Section 2.1);

2. the development of an analytical framework and monitoring indicators to guide the activation and evaluation of systemic cyber risk tools or, if required, the development of principles for guided discretion in the activation of tools (Section 2.2);

3. the development, calibration and activation of systemic cyber risk-specific instruments that ensure a sufficient level of financial and cyber resilience and mitigate the different contagion channels associated with a systemic cyber crisis as outlined in the cyber risk model (Section 2.3).

Of particular importance is the need to overcome the risk to financial stability stemming from a coordination failure during the response to an incident. Such a future pan-European systemic cyber incident coordination framework (EU-SCICF) is discussed in Section 3.

Figure 2
Macroprudential strategy



Source: ESRB (2014).

[13] See ESRB (2021b).

2.1 Inclusion of systemic cyber risk aspects in the intermediate objectives

The EU macroprudential policy framework should explicitly consider the cyber-specific risk amplifiers that differ from the risk amplifiers of a more traditional financial crisis. The IOs serve as the conceptual basis for the development of systemic risk indicators, the analysis of existing tools' appropriateness in addressing systemic cyber risk and the development of further mitigants (see Figure 2).

The existing IOs mostly aim to increase the financial loss-absorbing capacity of and to shore up confidence in the financial system. Existing macroprudential tools developed based on the IOs provide backstops for financial and reputational contagion and therefore mitigate certain amplification channels of a cyber incident. To expand their capabilities and help prevent a cyber incident from evolving into a systemic cyber crisis, the amendment of the IOs to include cyber-specific aspects should be considered. Where the need for the development of macroprudential tools to address systemic cyber risk is identified, such an amendment could provide a conceptual basis for this work.

While cyber risk is not explicitly addressed by any existing IO, some of their reasonings and related market failures can be used to address amplifiers related to the financial and confidence contagion channels of a major cyber incident (see Figure 1)**.** For example, IO1 "Mitigate and prevent excessive credit growth and leverage" and IO2 "Mitigate and prevent excessive maturity mismatch and market illiquidity" already provide fundamental financial resilience-related tools that can be used to obstruct the transmission and amplification of financial shocks associated with a cyber incident.[14] The remaining IOs require amendments to link them more explicitly to systemic cyber risk amplifiers. Specifically, IO3 "Limit direct and indirect exposure concentration" could be expanded to also include large operational exposures to ICT components and third-party service providers. IO4 "Limit the systemic impact of misaligned incentives" should consider the operational impact of institutions and excessive cyber risk-taking to gain a competitive advantage, and IO5 "Strengthen the resilience of financial infrastructures" should modify the definition of "resilience", which has a different meaning in the context of cyber[15] and takes a wider perspective on financial system resilience rather than exclusively infrastructures (see Table 1). A more detailed reasoning is provided in Section 5.1.

[14] Related to this are capital requirements for operational risk in Pillar 1.

[15] The FSB (2018) defines cyber resilience as the ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents.

Table 1

Desirable features of a toolkit to address systemic cyber risk

ESRB IOs	Amendments for cyber-inclusive IOs	Category	Risk amplifiers addressed by cyber-inclusive IOs	
			Systemic amplifiers	Cyber-specific amplifiers
1. Mitigate and prevent excessive credit growth and leverage	**No amendments needed:** IO could be used to increase institutions' financial loss-absorbing capacity related to cyber incidents.	High degree of interdependence Lack of transparency Reliance on confidence	Scale and criticality Network topology Complexity Uncertainty Erosion Adverse conditions	
2. Mitigate and prevent excessive maturity mismatch and market illiquidity	**No amendments needed:** IO could be used to increase institutions' liquidity position, which might come under pressure during a cyber incident.	High degree of interdependence Lack of transparency Reliance on data Reliance on confidence Scale Speed	Scale and criticality Network topology Homogeneity Complexity Time sensitivity Uncertainty Erosion Adverse conditions	Concurrency Pervasiveness Speed of transmission
3. Limit direct and indirect exposure concentrations	**Amendments:** The scope of exposures should be expanded. Besides financial exposures, operational exposures should be included with the aim of mitigating the excessive concentration of ICT providers and their products and limiting the lack of ICT substitutability and the impact of failures by systemic participants/infrastructures	High degree of interdependence Lack of transparency Reliance on confidence Scale	Scale and criticality Network topology Homogeneity Complexity Uncertainty Erosion Adverse conditions	Pervasiveness
4. Limit the systemic impact of misaligned incentives with a view to reducing moral hazard	**Amendments:** The scope of the systemic impact should be expanded. Besides the financial impact, the operational impact of an institution should be considered. Moral hazard in cybersecurity investments should be considered. Misaligned incentives in sharing cyber threat information should be considered.	High degree of interdependence Reliance on confidence Pre-existing weakness Intent Scale Speed	Scale and criticality Network topology Uncertainty Erosion Adverse conditions Detection time Ineffective response	Persistence Concurrency Pervasiveness Speed of transmission
5. Strengthen the resilience of financial infrastructures	**Amendments:** Cyber resilience should be considered within the scope of resilience. The cyber resilience of all financial institutions should be strengthened to increase system-wide resilience (see also FSB definition of cyber resilience)	High degree of interdependence Reliance on data Reliance on confidence Pre-existing weakness Intent Scale Speed	Scale and criticality Homogeneity Time sensitivity Erosion Adverse conditions Detection time Ineffective response	Persistence Concurrency Pervasiveness Speed of transmission

Source: ESRB.

Two options appear sufficiently suitable to amend the macroprudential framework such that it serves as a conceptual framework for the development of systemic cyber mitigants: first, the incorporation of cyber risk aspects into the existing IOs where needed (IO3 to IO5) and, second, the creation of a new IO specifically formulated to address systemic cyber risk.

- **Option 1: incorporation of systemic cyber risk aspects into existing IOs (IO3 to IO5).** This approach would keep the number of IOs unchanged. Instead of a new IO specific to addressing systemic cyber risk, the list of underlying market failures could be reviewed according to their applicability to systemic cyber risk and, where needed, missing aspects amended to make the link more explicit for systemic cyber risk. In particular, the market failures through which cyber risk becomes systemic could be addressed by using the existing IOs and adjusting their scope to convert them into cyber-inclusive IOs (**see Table 1**). This should be followed by a revision of the instruments associated with each IO, taking into consideration the adequacy of microprudential instruments to address these risks. Overall, the main advantage of this approach is that it would require only slight adaptations of the macroprudential framework, with the structure of the IOs remaining unchanged. It would also reduce the likelihood of an additional IO duplicating objectives that are already included in the existing IOs, notably direct and indirect interlinkages (IO3) and excessive risk-taking (IO4). Such a lean process would likely allow the macroprudential framework to be updated relatively quickly.

- **Option 2: introduction of a new (sixth) IO specific to systemic cyber risk.** The introduction of a new IO would provide a clear distinction between cyber and financial risks. Consequently, the macroprudential framework would take into account the different sources of systemic cyber risk compared with financial risk. This new IO could be defined such that it addresses all cyber risk-related amplifiers and market failures. This distinction would eliminate the risk of overburdening the existing IOs when using them to define systemic cyber risk mitigants. In addition, a dedicated IO could be justified by the political objective of signalling the importance of systemic cyber risk in terms of the threat posed to the real economy. However, this approach may also lead to a duplication of objectives that are already included in the existing IOs, most notably the resilience of financial infrastructures (IO5).

2.2 Development of an analytical framework and monitoring indicators

A complementary set of indicators of systemic cyber risk needs to be developed to implement policies to address systemic cyber risk. The financial stability surveillance framework[16] of the Financial Stability Board (FSB) proposes certain indicators for the monitoring of cyber vulnerabilities. Table 2 outlines additional indicators and links them to the ESRB's cyber-inclusive IOs. However, further reflection on required indicators is needed when developing the monitoring framework.

16 See FSB (2021).

The indicators should assist in identifying existing or emerging risks, as well as guiding and evaluating policy interventions. In the event of a major cyber incident, financial stability implications need to be recognised early to allow for the timely activation of systemic cyber risk mitigants that prevent or lessen the degree of amplification of financial contagion arising from a cyber incident. For this purpose, regular monitoring of the contagion channels among operational systems and within the financial system is needed to understand the amplification mechanisms that could lead to a systemic cyber crisis. Overall, this task requires a deep understanding of the risks as well as a high level of analytical and monitoring capability for systemic cyber risk on the part of macroprudential authorities.

The indicator set should consist of financial and cyber indicators that provide information on financial and cyber vulnerabilities which may lead to the emergence of systemic cyber risk. Financial vulnerabilities could arise through capital losses or liquidity freezes and are related to the cyber-inclusive IO1, IO2 and IO4. These vulnerabilities can be analysed via financial stress tests with cyber scenarios. The cyber vulnerabilities are associated with the cyber-inclusive IO3 to IO5, and relevant indicators would provide information on the systemic attributes of institutions and financial infrastructures themselves (IO3) and institutions' cyber resilience. Financial and cyber resilience could be analysed by systemic cyber resilience scenario stress testing (see Section 2.2.1), and the systemic attributes could be analysed by network analysis, through so-called cyber mapping and the identification of systemic nodes (see Section 2.2.3).

Timely and high-quality data are important for systemic cyber risk monitoring, instrument calibration and ex post management of a systemic cyber crisis, both in terms of defining recovery strategies and improving recovery plans. A preliminary and non-exhaustive list of indicators deemed useful is presented in Table 2. Some of these data, like cyber incident reporting or financial losses due to cyber incidents, are already mandatory under several supervisory and oversight frameworks.[17] However, these data are not harmonised across financial sectors and authorities, are only available to certain financial authorities and are in some cases only collected annually. DORA seeks to introduce the harmonisation of ICT-related incident reporting across all financial sectors to financial authorities in the EU. The G7 has also proposed a common categorisation of IT incidents.[18] As proposed in DORA, data collection initiatives should be supplemented by an information-sharing framework between authorities, including macroprudential ones, to overcome the lack of data at macroprudential level and facilitate risk assessment across jurisdictions and sectors.

[17] Existing European incident reporting regimes for the financial sector are the Network and Information Security Directive, the General Data Protection Regulation, the Payment Services Directive 2 and ECB Single Supervisory Mechanism incident reporting for significant financial institutions.

[18] See Banca d'Italia et al. (2021).

Table 2

Mapping cyber-inclusive intermediate objectives into indicators

Cyber-inclusive IO	Cyber-related indicators	Methods for systemic cyber risk analysis
Mitigate and prevent excessive credit growth and leverage	No amendments envisaged at this stage	
Mitigate and prevent excessive maturity mismatch and market illiquidity	Unavailability of liquidity as shock transmitter or amplifier during a cyber incident: liquidity position in severe but plausible cyber risk scenarios; derived from liquidity stress testing with cyber scenario	Liquidity stress testing with cyber risk scenario (see Section 2.2.1). Results to be benchmarked against regulatory requirements
Limit direct and indirect exposure concentrations	Indicators for large operational exposures Indicators for operational contagion, such as operational interconnectedness and interlinkages with systemic nodes Identification of systemic nodes by size, complexity, substitutability and interconnectedness of institutions and third-party ICT providers, for example through market concentration of external IT service providers (in %), average number of cloud service providers and number of external IT service providers	Cyber mapping to identify concentration risk, contagion channels and systemically important nodes (see Section 2.3.1)
Limit the systemic impact of misaligned incentives with a view to reducing moral hazard	Indicators for systemic impact, for example market concentration of external IT service providers (in %), average number of cloud service providers and number of external IT service providers Indicators for moral hazard, such as cyber resilience spending and participation in information-sharing arrangements (DORA) Ability of structural systemic risk to absorb financial losses that may materialise in a cyber incident	The assessment to understand moral hazard can be rather qualitative (guided discretion) Financial stress testing with cyber risk scenario (see Section 2.2.1). Results to be benchmarked against regulatory requirements
Strengthen the resilience of financial infrastructures and institutions	Operational disruption in severe but plausible cyber risk scenarios; derived from cyber resilience testing ORSA and TLPT results (see Section 2.2.1) Capital requirements for operational risk in Pillar 1 (Disaster) recovery parameters and other relevant indicators at individual level Indicative examples of further quantitative indicators: number of devices with obsolete software, number of cyber incidents, estimation of financial damage (in thousands of euro) or average response time for risk management	Systemic cyber resilience scenario stress testing (see Section 2.2.1). Results to be benchmarked against a defined tolerance level for disruption (see Section 2.2.2) Development of individual indicators and thresholds

Source: ESRB.

2.2.1 Systemic cyber resilience scenario stress testing

Systemic cyber resilience scenario stress testing provides a tool to assess the impact of a cyber incident and analyse its potential amplification into a systemic event. Comparable to financial stress testing, it is designed to test the resilience of an individual institution to exogenous and endogenous shocks. Thus, like financial stress testing, systemic cyber resilience scenario stress testing can be used as an indicator for risk analysis and to gauge the need for policy action. By benchmarking test results against tolerated shock-absorbing capacities of institutions, systemic cyber resilience scenario stress tests can provide valuable information about the financial or cyber resilience of institutions and financial infrastructures for both microprudential and macroprudential authorities. The International Monetary Fund (IMF) takes a similar view, noting that stress testing offers financial authorities a tool to quantify the financial impact of a cyber incident and analyse its potential amplification into a systemic event.[19]

Two approaches exist for testing institutions' resilience in severe but plausible cyber incident scenarios. The first approach is to incorporate systemic cyber risk scenarios into existing financial stress testing to assess intermediaries' cyber-related loss-absorbing capacity. Here, the literature on stress testing in the context of cyber focuses on cyber loss analysis and liquidity stress tests, with the aim of assessing and quantifying the financial impact of a cyber incident and modelling financial contagion and amplification.[20] A second approach is to add an additional layer to the stress-testing framework, namely a systemic cyber resilience scenario stress test. This layer is a specific and separate stress test based on a severe but plausible cyber incident scenario and assesses the financial system's operational capability earlier in the cyber crisis lifecycle. For example, the Bank of England (BoE) conducts such a regular assessment through its "cyber stress test".[21] The objective is an assessment of institutions' capability to operationally absorb a cyber incident within a defined timeframe and to continue services without material economic impact (tolerance for disruption).

Systemic cyber resilience scenario stress tests at EU level allow for an assessment of systemic cyber risk originating from the operational side of institutions, rather than the financial side. A three-step implementation appears reasonable. First, tolerance levels for the disruption of systemic institutions' critical economic functions need to be defined. For other institutions that might potentially be included in the testing exercise, their self-defined tolerances for disruption can be considered. Second, operational disruption is to be assessed through systemic cyber resilience scenario stress tests with a severe but plausible cyber scenario. In doing so, certain cyber vulnerabilities in the financial system may be revealed. Third, these test results should be used for the formulation of a financial stress test scenario to analyse consequences of a cyber incident for financial stability.

Microprudential and macroprudential cyber stress tests should complement each other. A hypothetical cyber incident scenario can draw on lessons learned from various kinds of assessments, including horizontal analyses as part of the Supervisory Review and Evaluation

19 See Adelmann et al. (2020).

20 See ECB (2017), Eisenbach et al. (2021), Duffie and Younger (2019) and Bouveret (2018).

21 See Bank of England (2021).

process (SREP) in the banking sector[22], external audits, self-assessments and threat-led penetration tests (TLPTs) such as TIBER (Threat Intelligence-Based Ethical Red Teaming). Together, these outcomes can provide information about potential vulnerabilities in the financial system that can assist macroprudential authorities in defining severe but plausible scenarios for their systemic cyber resilience scenario stress test. Outcomes can provide further guidance on the design of a severe but still plausible cyber incident scenario that can be incorporated into existing financial stress testing or in business continuity and disaster recovery plans and, in the case of insurers, in institutions' own risk and solvency assessments (ORSAs). For such a task, close cooperation between microprudential and macroprudential authorities is required.

Systemic cyber resilience scenario stress tests should be appropriately coherent across sectors to enable a system-wide analysis of test results. In the current situation, the European Supervisory Authorities (ESAs) consider cyber risk to some extent in their periodical stress test exercises. For example, the central counterparties stress test (CCP stress test) of the European Securities and Market Authority (ESMA) considers cyber risk as part of operational risk (see Box 1).[23] While such tests contribute to a better understanding of the resilience of different financial sectors, they are developed with different scopes and objectives, and a lack of harmonisation may hamper the system-wide analysis of results. A coherent approach to how systemic cyber resilience scenario stress tests are conducted would contribute to bringing the different test results together for a system-wide analysis and thus allow macroprudential authorities to draw conclusions on the cyber and financial resilience of the financial system against cyber incidents. Nevertheless, systemic cyber resilience scenario stress tests should allow the required degree of flexibility in the scenario design to account for any sectoral differences.

Box 1
ESMA CCP stress test approach

The ESMA CCP stress test is an exercise that results from the legal mandate given to ESMA under the European Market Infrastructure Regulation (EMIR). The 2021 ESMA CCP stress test includes a component specifically focused on assessing operational risk, namely the operational risk affecting third-party entities on which CCPs rely to provide their services.

The objectives of the assessment of operational risk are the following:

1. Identify external third-party entities or systems that have the potential to create a business disruption or system failure leading to a material reduction, deterioration or breakdown of services of a CCP.
2. Identify potential risks for CCPs in a scenario of an operational event affecting a critical third-party service provider.
3. Assess the tools that CCPs use to manage risks from these external third-party entities.

[22] As defined in Article 97 of the CRD (Directive 2013/36/EU). For specific information on IT risk, see for example ECB (2020b).

[23] See ESRB (2021a) and EIOPA (2020).

4. Perform an interconnectedness analysis of the network of third-party entities that have the potential to create a business disruption or system failure of a potentially systemic nature.

The risks in scope for the operational risk component are any type of event that can cause a disruption for a critical third-party provider, including cyber risk.

2.2.2 Tolerance for disruption levels

Macroprudential authorities need to define their expectations against which systemic cyber resilience scenario stress test results are evaluated. While for financial stress testing financial benchmarks are applied in the evaluation, operational benchmarks should be used for systemic cyber resilience scenario stress tests. Here, the BoE (2021) notes that a need exists to form "clear baseline expectations for firms' resilience that reflected the importance of firms and the services they provide for the financial system". By benchmarking test results against these expectations, systemic cyber resilience scenario stress tests provide information about the cyber resilience of institutions and financial infrastructures and reveal vulnerabilities.

The objective of macroprudential tolerance for disruption levels is to quantify the maximum acceptable level of disruption to critical economic functions that does not pose a risk to financial stability in severe, or even extreme, but still plausible scenarios.[24] The macroprudential level of tolerance for disruptions can be set to reflect the tipping point at which the financial system is no longer able to absorb a shock and financial stability is impaired. According to the conceptual systemic cyber risk model (Figure 1), tolerance for disruptions defines the threshold between the amplification phase and systemic event phase. The quantification of tolerance for disruptions can be expressed by reference to specific outcomes and metrics. Such metrics can include the maximum tolerable duration or volume of economic function disruptions, a measure of data integrity or the number of customers affected.[25] The Central Bank of Ireland (2021) notes that tolerance for disruptions is a distinct tolerance measure. A usual measure is risk appetite, which focuses on the impact and probability of a risk event occurring. Tolerance for disruptions assumes that the risk event has already crystallised, meaning the probability element of risk appetite is removed.[26] In order to be in line with the Basel Committee on Banking Supervision (BCBS, 2021), the term "tolerance for disruptions" is used in this report, while other authorities such as the BoE et al. (2021) and Central Bank of Ireland (2021) adopt the term "impact tolerance", which refers to the same concept.[27]

Macroprudential authorities' tolerance for disruptions would complement existing work by microprudential and oversight authorities by adding a systemic dimension. Microprudential and oversight authorities already define their tolerance for disruptions as part of their statutory objectives. For example, banking regulation calls for backup procedures that allow recoveries according to business needs, while in 2018 the ECB defined its cyber resilience oversight

24 Compare BIS and IOSCO (2016) and Bank of England et al. (2021).

25 See Bank of England et al. (2018).

26 See Central Bank of Ireland (2021).

27 Compare BCBS (2021), Central Bank of Ireland (2021) and Bank of England et al. (2021).

expectations for FMIs.[28] Systemically important payment system (SIPS) regulation defines corresponding operation resumption times for critical information technology systems.[29] With a reference to financial stability, the Bank for International Settlements (BIS) and International Organization of Securities Commissions (IOSCO, 2016) ask FMIs to resume critical operations within two hours and complete settlement by the end of the day of the disruption. Notwithstanding this capability, FMIs should exercise judgement in effecting resumption so that risks to itself or its ecosystem do not escalate.[30] The objective of all these levels is to ensure a sufficient level of cyber resilience of institutions. Further considerations are needed on how tolerance for disruptions can be used to promote financial stability and be incorporated into the analysis of systemic cyber resilience scenario stress tests.

2.2.3 Identification of systemically important nodes

The identification of systemically important nodes assists authorities in their formulation of policy actions to mitigate systemic cyber risk. An overview of systemic nodes contributes to a better understanding of the network topology, whose characteristics, according to the conceptual cyber risk model, could potentially be risk amplifiers. In addition, it could provide a first indication of contagion channels. Finally, an overview of systemic nodes helps define which institutions and third-party providers serving them should be included in systemic cyber resilience scenario stress testing.

Systemic nodes are any agents fulfilling a critical financial or operational role in the financial sector. Such systemic nodes are often characterised by the importance or a lack of substitutability of the financial or operational services they provide to the financial system. Thus, a cyber incident that affects systemic nodes can lead to disruption in the financial system that is far greater than disruption at less significant nodes. The identification of critical nodes in the financial and operational network is therefore of utmost importance for the monitoring and analysis of systemic cyber risk.

Macroprudential authorities should cooperate with microprudential and cyber authorities in the identification of systemic nodes. For operational services, DORA proposes a harmonised EU-wide designation framework for critical ICT third-party service providers in the financial system. In addition, institutions should maintain and update at entity level, and at sub-consolidated and consolidated levels, a register of information for all contractual arrangements on the use of ICT services provided by ICT third-party service providers. This assessment provides financial authorities with a first centralised overview at EU level of critical nodes in the financial system. However, the assessment leaves aside the system-wide dimension and asks for an additional analysis by macroprudential authorities to identify potentially other critical nodes in the financial system that have not been reported under DORA.

---

28 See EBA (2019) and ECB (2018).

29 **Regulation (EU) 2021/728 of the European Central Bank of 29 April 2021 amending Regulation (EU) No 795/2014 on oversight requirements for systemically important payment systems (ECB/2021/17) (OJ L 157, 5.5.2021, p. 1)**.

30 See BIS and IOSCO (2016).

Comparable to the method for designating systemically important institutions (SIIs) in the financial system itself, a method for the designation of critical nodes needs to be developed for systemic cyber risk. The consideration of the operational dimension in the analysis of systemic cyber risk expands the concept of SIIs. For example, the widespread use of a limited number of ICT third-party providers by many financial institutions results in a concentration risk that, in the event of a cyber incident at one or more critical providers, could materialise into a systemic cyber crisis.[31] Approaches macroprudential authorities can draw on for the designation of critical nodes are proposed under the current DORA proposal and include, for example, operational and financial criteria for the identification of significant and cyber mature financial institutions for which TLPTs are mandatory, as well as the proposed criteria for the designation of critical ICT third-party service providers. Criteria for the identification of critical services and providers are the systemic impact, interdependencies between global SIIs and other SIIs, and the degree of substitutability. The SII framework partly applies the same categories: substitutability, interconnectedness and size, which are used as a proxy for disruption to financial markets (systemic impact).[32]

A so-called cyber map enables the identification of systemic nodes in the system by monitoring and analysing the main technologies, services and connections between financial sector institutions, service providers and in-house or third-party systems. At a conceptual level, mapping aims to highlight key financial and technological connections between financial institutions (including FMIs) and between these firms and third-party technology and service providers.[33] It can combine data on financial and operational actors in the financial system to identify systemic nodes in the system by their importance, interconnectedness and dependency on other actors. Information about the interlinkages of ICT systems and service providers of individual institutions and firms in the financial system is combined via network analysis for the identification of contagion channels. Furthermore, maps may be tailored for more specific purposes, such as designing systemic cyber resilience scenario stress tests (see Section 2.2.1), identifying and calibrating relevant risk mitigating tools, or identifying relevant institutions and authorities that need to communicate and coordinate in the event of a systemic cyber crisis. Due to the complexity of the system, maps may be tailored to monitor systemic cyber risk on a national, regional or cross-border level.

Cyber maps for macroprudential purposes are at an early stage. Currently there are several initiatives at both the national and cross-border level to develop cyber maps. Box 2 provides concrete examples of approaches taken in Germany and Norway. Owing to the clear need for an enhanced monitoring of systemic cyber risk, macroprudential authorities should start working on cyber maps, focusing particularly on defining the objectives of the mapping exercises and bringing together relevant authorities and institutions that need to be involved in developing maps of sufficient detail and scope. However, the creation and maintenance of these cyber maps is resource-intensive because of current challenges in combining data of the financial system and their third-party providers. Thus, for a first set of maps, it may be necessary to limit their scope. By

---

31 Commission staff working document – **Impact Assessment Report** accompanying the document Proposal for a Directive of the European Parliament and of the Council amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341 (SWD(2020) 203 final).

32 Individual indicators in the category “substitutability/financial institution infrastructure” are assets under custody, payments activity and underwritten transactions in debt and equity markets (BCBS, 2013).

33 See Adelmann et al. (2020) and Banka Slovenije (2021).

additionally including information on financial and cyber vulnerabilities, these cyber maps could provide further insights into potential contagion channels.

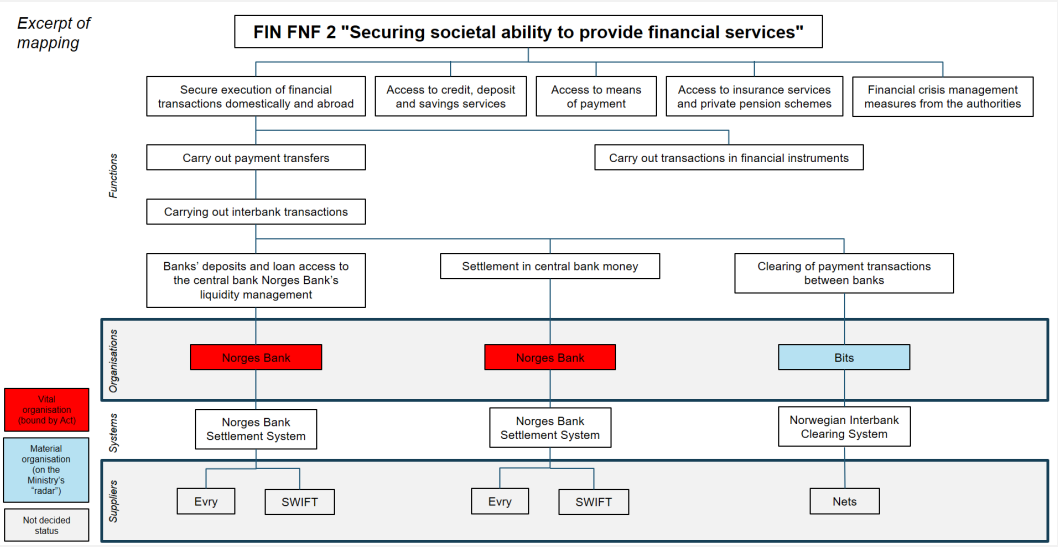
Data limitations hampering the implementation of cyber maps need to be overcome. There are numerous challenges involved in the development of cyber maps. There is a lack of comprehensive and timely data on operational linkages, such as common third-party providers, common exposures to hardware and software packages, and common exposures to clients, retail partners and counterparties. To some extent, these data are considered in the DORA proposal, for instance through institutions' register of information as described above. It is of utmost importance for the monitoring of systemic cyber risk in the financial system that these data are shared with macroprudential authorities in consideration of existing legal requirements.

Box 2
Cyber mapping approaches

Cyber maps can be built based on a functional or an institutional approach:

1. The functional approach is based on the idea that certain functions in and for the financial system are critical, for instance for financial stability. In the functional approach, the core critical functions are defined and granulated according to the purpose of the map, after which the institutions providing these functions are identified as well as the systems these institutions rely on to provide the functions. Based on this map, transmission channels, critical providers and systems can be identified. An excerpt of the mapping of fundamental national functions for the payment system in Norway (Figure A) provides an example of such an approach developed for safety and security purposes.

Figure A
Illustration of a cyber map based on the functional approach

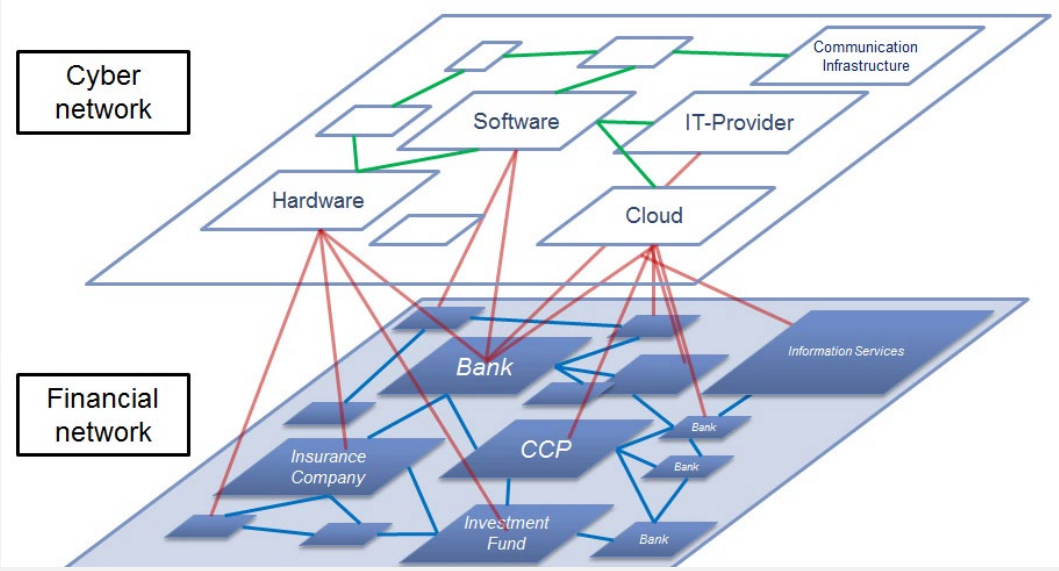


Source: Norges Bank.

2. The institutional approach is based on the idea that the structure of the financial sector, financial relationships and respective processes can be mirrored by a respective "cyber network". A cyber network can be regarded as a virtual layer of the financial network consisting of all ICT components that are used by financial institutions to run their businesses. Institutions use software, hardware, other ICT components and ICT (third-party) service providers to offer their financial services. By mapping the financial network (i.e. financial system) to the cyber network, one can identify linkages between third-party ICT providers that are used by SIIs. In turn, this approach allows common ICT providers (e.g. cloud providers) in the financial sector to be disclosed. With this information, both the concentration risk within the cyber network and the transmission channels of cyber risk to the financial system can be substantiated. Figure B provides a stylised example of this approach from the Deutsche Bundesbank.

Figure B

Illustration of a cyber map based on the institutional approach



Source: Deutsche Bundesbank.

2.3 Development of systemic mitigants

2.3.1 Maintaining an elevated level of cyber resilience for systemic nodes across the entire financial system

Systemic nodes in the financial system should operate with elevated levels of cyber resilience. In the financial system, critical economic functions are to a large extent provided by SIIs or critical/core financial infrastructures and to an increasing extent supported by third-party service

providers, which may become systemically important for the financial system as a result.[34] In financial regulation, this systemic importance is addressed by the SII designation framework. In the context of systemic cyber risk, the capital add-on for SIIs can be translated into higher operational requirements for cyber resilience. Against this background, Adelmann et al. (2019) conclude that "smaller and lower-capacity firms should focus on strengthening cyber hygiene, and the largest and most globally connected firms and key system nodes should be subject to heightened standards commensurate with their size, scale, interconnectedness and risk profile."[35]

Further analysis is needed on how macroprudential policy should complement existing microprudential and oversight regulations on cyber resilience. Under the current DORA proposal, all institutions should identify relevant determinants of operational, including cyber, resilience based on their expected impact on market efficiency. Due to the microprudential focus of the DORA proposal, the systemic impact on financial stability is not considered in its entirety. Here, macroprudential authorities can coordinate with microprudential and oversight authorities to provide guidance on the required cyber resilience of economic functions, institutions (e.g. SIIs) and sectors, as defined for central counterparties (CCPs) and central securities depositories (CSDs) under the DORA proposal.[36] This first of all requires evidence on the financial system's capacity to absorb a cyber incident within a defined timeframe and without material economic impact (tolerance for disruption) in severe but plausible cyber incident scenarios (see Section 2.2.2).

To increase the level of cyber resilience, financial authorities should explore potential means to ensure system-wide financial data integrity and availability even during a systemic cyber crisis. For individual institutions, this is of particular importance as many recovery and resolution plans are contingent on the essential data being available or recoverable. From a system-wide perspective, a high level of cyber resilience can dampen the operational amplifiers of a cyber incident. A technological example in the field of immutable backup systems is data vaulting.[37] This concept is still relatively new to financial authorities, which should build up their experience with and knowledge of these solutions and, where beneficial, collaborate with the financial industry on system-wide approaches.

2.3.2 Tools to increase financial resilience in a systemic cyber crisis

Financial tools can complement tools on cyber resilience. The adaptation of financial tools to systemic cyber risk will contribute to loss-absorbing capacity in the event of a systemic cyber event. According to the chronology of the systemic cyber risk model (Figure 1), these tools are likely to be applied in the amplification phase and thus relatively late in crisis mitigation and are only applicable to institutions included in the scope of financial regulation. The operational risk amplifiers and contagion channels of a systemic cyber crisis remain unaddressed. This calls for specific tools on

34 See ECB (2021b).

35 See Adelmann et al. (2019).

36 A sector-wise approach may make it possible to address the risk stemming from several small, interlinked institutions ("too connected to fail").

37 Another technological example that could provide benefits in data and system availability may be found in distributed ledger technology (DLT) and blockchain. This type of technology builds on continuous sharing of data and code among the participating nodes and provides technological standards that aim to create distributed systems whose global functionality is not affected by outages of a limited number of participating nodes.

cyber resilience, especially as the design and calibration of financial tools relies on the assumption of functioning operational systems, which may not be the case in a systemic cyber crisis. Among its consequences, a cyber incident may render the use of financial macroprudential tools (operationally) ineffective.

Currently, the question of whether existing capital and liquidity requirements should be made contingent on systemic cyber risk remains unclear. A potential issue with this approach is that it could overburden these instruments, while cyber resilience requirements are likely to be more effective in mitigating systemic cyber risk. First and foremost, however, a deeper understanding of the impact of operational disruption on the provision of economic functions and the potentially resulting financial losses that could occur in a systemic cyber risk event is required.[38] Systemic cyber resilience scenario stress tests may be a relevant method to determine operational disruption in systemic cyber events (see Section 2.2.1).

[38] Cyber risk quantification at the systemic level is at an earlier stage of development. Although there are large uncertainty margins around current estimates, these are likely to narrow as data and modelling approaches continue to improve. Estimates of potential losses are high. For example, through Monte Carlo simulations, Bouveret (2018) estimates the 95% Value-at-Rsik (VaR) loss to be USD 147 billion for financial institutions globally (14% of global net income). Bouveret conducts a further experiment in which the mean cyberattack frequency is set to two times its historical peak. Under this scenario, the 95% VaR loss rises to USD 352 billion (34% of net income). Aldasoro et al. (2020) study cyber-related losses in the financial system and point to a VaR of more than 4% of gross income, though these are skewed and thus bear the risk of tail events.

3 A pan-European systemic cyber incident coordination framework for financial authorities

A rapid response from authorities is needed to mitigate the potential negative effects of cyber incidents on financial stability. The underlying shock originates in a novel way compared with traditional financial and liquidity crises faced by financial authorities. It requires new coordination networks and mechanisms with parties that financial authorities do not usually interact with. To enable prompt coordination, these structures need to be in place before the occurrence of a systemic cyber crisis. Due to the speed and scale of shock propagation, any development and implementation of these structures in times of crisis will be too late.

3.1 The need for a pan-European cyber incident coordination framework

Early coordination and communication in the event of a cyber incident that has the potential to become systemic can assist in ensuring the early detection of such an incident, maintain confidence in the financial system and limit contagion effects on other financial institutions, thus preventing the incident from becoming systemic. Against this background, the ESRB (2020) highlighted the importance of rapid and effective communication and coordination between authorities.[39] To reduce the time required to resolve an impending crisis, the implications of a cyber incident for financial stability need to be understood quickly. Aside from financial aspects, the overall risk assessment must include the scale and impact of operational disruption, as this may influence the choice of (macroprudential) tools. Likewise, financial stability may also influence the choice of operational mitigants by cyber experts.

Communication and coordination between (financial) authorities in the event of a systemic cyber crisis can become complex. The financial authority universe is composed of microprudential and macroprudential supervisors, oversight authorities and central banks, which differ in their mandates and geographical and sectoral focus. This heterogeneity among financial authorities, together with the complexity, interconnectedness and cross-border nature of the financial sector itself (including different existing crisis-management frameworks), could hamper communication and coordination efforts in the event of a systemic cyber crisis. Challenges in communication and coordination during a systemic cyber crisis are likely to occur at a time when a swift and coordinated reaction is needed to ensure effective crisis management, and uncertainty will likely be pervasive.

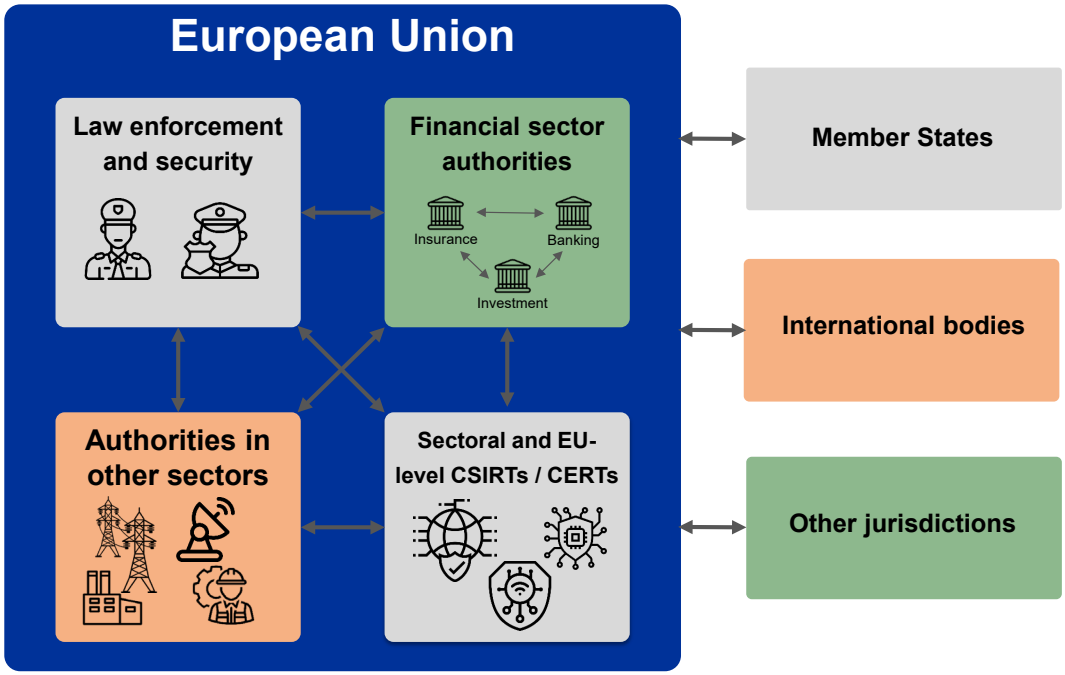
Financial authorities need to be prepared to interact with other (financial) authorities to manage a cyber incident. In the event of a systemic cyber crisis, crisis-management protocols at national and European levels will likely be triggered. For cyber authorities, these protocols will seek to support the resolution of the technical aspects of the cyber incident itself. For financial authorities, which need to deal with the economic consequences of a cyber incident for the financial system, it is about managing the impact on financial stability caused by the disruption to financial

[39] See ESRB (2020), p. 3.

services. In addition, financial authorities need to coordinate with others, including cyber authorities, to ensure that their responses consider the different facets of a systemic cyber crisis (see Figure 3). Such orchestration needs close and swift coordination and open communication between financial authorities themselves and with cyber authorities in order to, inter alia, build situational awareness.

Figure 3

Potential interactions between authorities at EU level during a systemic cyber crisis



Source: ESRB.
Notes: For illustration purposes only. No claim for completeness.

To mitigate the risk of a coordination failure, financial authorities need to increase their level of preparedness for a systemic cyber crisis by enhancing their communication and coordination capabilities at EU level. Financial authorities' preparedness goes beyond information sharing. It also requires a coherent (but not necessarily standardised) plan for information sharing, incident communication and external communication as well as a collective and consistent response to systemic cyber incidents. A balance needs to be reached between agility and consistency: some jurisdictions, for example, may experience unusual consequences, thereby requiring novel and innovative action in response. However, any agile approach calls for close coordination to ensure that all required financial authorities are involved.

While several initiatives on cyber risk exist at EU level[40], none of them cover all financial authorities in the EU. In the context of cyber risk, recent initiatives by the European Commission already foster EU-wide coordination for large-scale cybersecurity incidents at European level and across sectors to increase response effectiveness. These include the **European Commission blueprint on coordinated response to large-scale cybersecurity incidents and crises**

[40] One example is the **Euro Cyber Resilience Board for pan-European Financial Infrastructures**.

(Commission blueprint) published in 2017 and the establishment of a **Joint Cyber Unit (JCU)**[41]. A comparable level of coordination is required from financial authorities that will enable them to define and operationalise a rapid response to address the financial consequences of a major cyber incident. Moreover, it would assist effective interaction with cyber authorities regarding their response, which may likewise have repercussions for financial stability. In this context, the DORA proposal requests that financial authorities develop crisis-management and communication channels to enable an effective and coordinated response at EU level in the event of a major cyber incident.[42]

A pan-European systemic cyber incident coordination framework (EU-SCICF) for European financial authorities would increase their level of preparedness for managing the impact of a cyber incident on the financial system, thus maintaining financial stability. This framework could be built on one of the envisaged roles of the ESAs under the DORA proposal to gradually enable an effective EU-level coordinated response in the event of a major cross-border ICT-related incident or related threat having a systemic impact on the EU financial sector as a whole. To be effective, a predefined framework needs to be commonly shared, remain sufficiently flexible and provide clear guidance to all authorities involved. In addition, it needs to be tested and practised regularly. Thus, a periodical review and rehearsal should be implemented as well.

An EU-SCICF should facilitate financial authorities in the EU to coordinate globally. As a significant number of EU financial institutions operate globally, a major cyber incident will likely not be limited to the EU or might be triggered outside the EU. In such cases, it will require global coordination. Therefore, the framework should also offer interfaces, established for example through a Memorandum of Understanding for all framework participants, which enable communication and coordination with authorities' frameworks other than those of European financial authorities. The framework should facilitate liaison between the authorities that handle the technical aspects of the cyber incident and financial authorities. This would allow the former to also consider financial stability implications, while also helping financial authorities form a proper understanding of the situation and undertake adequate measure to ensure financial stability.

A future EU-SCICF should be designed not to replace existing frameworks but to bridge any coordination and communication gaps between financial authorities themselves, with other sector authorities and with other key actors at international level. As such, it should complement pre-existing coordination and communication protocols. To the extent necessary, the framework should overcome any friction in coordination between financial authorities and seek to ensure an information flow so as to facilitate the coordination of a cyber incident. As the proposed framework has a non-duplication objective, the positioning of the EU-SCICF in the existing financial crisis framework and EU cyber incident framework landscape needs to be considered. One option is to embed the EU-SCICF in the existing financial crisis framework by including preparedness for a systemic cyber crisis as a further objective in financial stability-focused EU frameworks. Another option would be to create a framework with a specific focus on systemic cyber crises. In the latter

---

41 The **Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents (OJ L 239, 19.9.2017, p. 36)** calls for EU-wide cooperation on (i) the investigation of technical causes of the incident and identification of technical measures; (ii) operationalisation of identified measures; and (iii) at the political level, decisions on the use of other instruments.

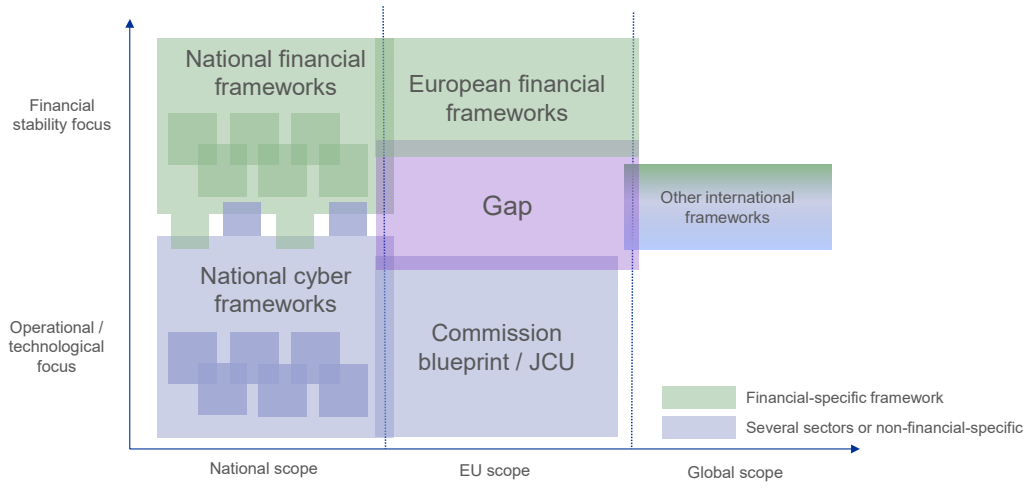
42 See DORA proposal, Article 43.

case, it is important to bear in mind that a situation with many different frameworks could lead to uncertainty and disagreement over which framework to follow.

3.2 Communication and coordination frameworks landscape

Compiling a landscape of existing and proposed financial and cyber frameworks provides an overview of the potential gaps the EU-SCICF needs to fill in a (potential) systemic cyber crisis. Identified gaps provide a reference as to what the purpose of the framework should be and which key elements it should contain. When compiling the landscape, several dimensions were considered.

Figure 4
Crisis communication and coordination frameworks



Source: ESRB.

Figure 4 shows a schematic view of the crisis communication and coordination framework landscape. The frameworks are depicted along the two dimensions geographical scope (x-axis) and focus (y-axis), and a third dimension showing the sectoral focus is added by different colours. Element overlaps indicate that some connection or communication elements exist in those frameworks. The absence of an overlap between frameworks does not imply that no communication or connection between them exists or that no communication between them will occur during a crisis. It simply indicates that that particular communication is not addressed in the framework.

National financial frameworks include the different national and sectoral frameworks that are activated to ensure financial stability locally in the event of a cyber crisis. The local focus of these frameworks may include interaction with other European frameworks or authorities (e.g. notification or reporting processes). Depending on national implementation, these frameworks may overlap with national technical frameworks for cyber incidents that affect the financial system.

European financial frameworks are those that have been established exclusively by European authorities and are aimed to ensure financial stability in the EU. Like the national financial stability frameworks, these frameworks traditionally do not envisage interaction with technical or operational frameworks or initiatives. An example of this is the ESRB framework.[43]

Other international financial frameworks with global scope cover jurisdictions outside the EU or that may partially interact with frameworks at EU or Member State level in the event of a systemic cyber crisis. Their main goal is to ensure an adequate level of coordination between G7 members during a cyber crisis. They do not focus on technical or operational resolution since both will be under each jurisdiction's remit.

National cyber frameworks focusing on the technical and operational resolution of cyber incidents are typically cross-sectoral initiatives. Examples are frameworks derived from national implementations of the Network and Information Security Directive (NIS Directive) or other national regulations aimed at protecting critical technical infrastructures at national level, which may include cyber incident-related aspects. In some EU countries, **national financial sector cyber frameworks** have also been established, which facilitate intelligence and information sharing on cyber threats and vulnerabilities between financial entities, and in some cases with authorities, as provided for in the DORA proposal.

Commission blueprint and JCU[44]. The European Commission recommendation on a coordinated response to large-scale cyber incidents and crises, also called the Commission blueprint, was issued in 2017 to improve the crisis management of cyber events affecting two or more Member States or causing disruption too extensive for a single Member State to handle on its own.[45] It aims to improve situational awareness and coordination and provide consistent communication to the public. The JCU builds on the Commission blueprint and is the future tool planned by the European Union to enhance cooperation among different actors so as to prevent, deter and respond to cyberattacks. Both initiatives share most of their goals with the proposed framework and include aspects outside the technology realm (e.g. political, public communication or diplomacy). They lack specific sectoral coordination and are mainly focused on the resolution of the technical crisis. Financial stability is neither in the scope of the Commission blueprint nor the JCU, and the frameworks do not cover any actions to solve a systemic cyber crisis in the financial system.

The DORA proposal has a microprudential focus and is mainly designed to enhance the operational resilience and ICT risk management of financial institutions and establish the corresponding oversight framework. The DORA proposal is related to a cyber incident coordination framework. The article refers to "crisis-management and contingency exercises involving cyberattack scenarios with a view to develop communication channels and gradually enable an effective EU-level coordinated response in the event of a major cross-border ICT-related incident". This could be a legal basis and justification for the establishment and further development of the EU-SCICF.

---

43 **Regulation (EU) No 1092/2010 of the European Parliament and of the Council on European Union macro-prudential oversight of the financial system and establishing a European Systemic Risk Board (OJ L 331, 15.12.2010, p. 1)**.

44 **Commission Recommendation (EU) 2021/1086 of 23 June 2021 on building a Joint Cyber Unit (OJ L 237, 5.7.2021, p.1)**.

45 See **Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents (OJ L 239, 19.9.2017, p. 36)**.

A clear gap exists for a framework which combines an operational or technological focus with a financial stability focus at EU level. The gap likely results from the fact that systemic cyber risk is not yet part of the macroprudential framework (see Section 2). Therefore, no relationship between financial stability frameworks and initiatives dealing with cyber incidents has been perceived as necessary. Another factor relates to the scope cyber frameworks have, which usually include multiple sectors and a focus on technical aspects. If left unaddressed, the coexistence of cyber and financial stability frameworks without a sufficient level of interaction with each other bears the risk of a coordination failure among authorities. This communication and coordination gap at EU level between financial authorities needs to be addressed by an EU-SCICF.

To expand this landscape, the European Systemic Cyber Group (ESCG) explored existing and upcoming initiatives, including regulation and frameworks, that could have some connection with the proposed preparation work for the future establishment of an EU-SCICF. Table 3 presents a brief overview of the main axes of its analysis of the different initiatives.

Table 3
Overview of analysed initiatives

Initiative	Geographical focus	Sectoral focus	Regulatory scope	Relevance to ESCG work
DORA	European Union	Financial sector	Microprudential[46]	High
NIS	European Union	Cross-sectoral	N/A	Medium
NIS2	European Union	Cross-sectoral	N/A	Medium
Commission blueprint / JCU	European Union	Different sectors	N/A	High
FSB	G20	Financial sector	Microprudential	Low
G7-CIRP	G7	Financial sector	Macroprudential	High

Source: ESRB.

3.3 Key elements of the pan-European systemic cyber incident coordination framework

A pan-European systemic cyber incident coordination framework should be based on three major pillars: (i) communication and information sharing among financial authorities, (ii) coordination among financial authorities, and (iii) communication with the public. These three pillars are aligned with the objectives highlighted by the recent European Commission recommendation on establishing the JCU.[47] By outlining these key elements, this report aims to define the required level of coordination and communication between different stakeholders (financial authorities, international authorities and the general public) to contribute to the level of

[46] The oversight framework proposed by DORA does have a systemic aspect to its objectives, though in a simple summary table "microprudential" seems reasonable.

[47] Recital (23) of the European Commission Recommendation on building a Joint Cyber Unit.

preparedness of financial authorities that is needed at EU level to limit the impact of a cyber incident on financial stability.

As both the financial system and the cyber landscape are constantly subject to change, the key elements should be regularly reviewed and amended to ensure the framework is clearly understood by all and fit for purpose. Thus, it is necessary to regularly test and update the framework. These tests and the results they provide are essential to improving the framework, in particular in a multilateral and sector-wide context. Therefore, the three pillars are supported by principles on testing and evolving the framework.

3.3.1 Communication and information sharing among financial authorities

To assist coordination during a systemic cyber crisis that affects different jurisdictions or sectors, financial authorities involved need a common level of understanding of the situation to assess the impact and potential measures within their jurisdiction.

- **Use of a common vocabulary.** A commonly used lexicon and taxonomy[48] will ensure that information sent between decision-makers is similarly understood and interpreted by both sender and recipient. The lexicon and taxonomy need to be as consistent as possible with other frameworks and jurisdictions. If necessary, authorities should ensure that a translation between lexicons and taxonomies exists to ensure a consistent understanding of exchanged information. It seems appropriate that authorities use existing taxonomies and lexicons. Examples of such lexicons are the FSB cyber lexicon used by financial authorities globally and the glossary provided by the European Union Agency for Cybersecurity (ENISA), which is intended to facilitate cyber-related work in the EU network of computer security incident response teams (CSIRT network).[49] Defining agreed formats for information sharing could also reduce confusion and translation efforts (i.e. which data should be shared using which templates).

- **Classification of cyber incidents.** To support a proper framework activation, a cyber incident needs to be classified in a timely manner depending on its severity. The taxonomy should refer to thresholds and criteria relating to the severity classification of a cyber incident, as proposed by DORA, and in addition to a further layer of triggers and circumstances when such incidents tend to become systemically relevant for the financial system. Systemic incident classification criteria should consider the incident's (potential) reach and impact in the financial system and on the larger economy. These thresholds and criteria should be as consistent as possible with those used by national authorities and cybersecurity agencies to allow the frictionless mapping between classifications used by different authorities.

- **Secure and reliable information-sharing channels.** Reliable and secure channels and tools reduce barriers to sharing confidential information. These channels should be used on a

[48] A cyber lexicon provides a dictionary for commonly used terminology to promote consistent wording in communication. A taxonomy provides a schema which, based on predefined rules, allows coherent incident classification.

[49] See FSB (2018) and ENISA (2021b).

routine basis to ensure their operability when a major cyber incident arises. Backup systems or fall-back solutions should be identified and available in case primary communication means are rendered inoperative because of the incident.

- **Establishment of points of contact.** Communication handbooks, to be regularly updated, should provide guidance on which persons from which authorities to contact and about which content. They should ensure both swift communication during a cyber crisis and that the appropriate recipients receive the correct information. This applies not only to communication between financial authorities but also communication with other authorities (e.g. cyber) both at national and international level.

- **Upfront management of confidential information sharing.** Confidential information sharing could be limited by financial regulation, national security regulations or privacy legislation. Authorities should consider these constraints in their communication strategy and exchange information accordingly. Clarity on what information can be shared with whom should exist before an incident occurs to facilitate timely information sharing during a systemic cyber crisis. Policymakers and regulators should take into account the possible unintended consequences of limiting necessary information sharing in a cyber crisis and provide appropriation clarifications or make legislative adjustments. In this regard it is noted that the European Commission recommendation on building a JCU proposes a shift in information/data-sharing arrangements: "*All relevant actors in the EU need to be prepared to respond collectively and exchange information on a 'need to share', rather than 'need to know', basis.*"[50] Financial authorities need to reflect on how their information-sharing paradigms comply with the "need to share" proposal.

- **Collaboration with financial sector cyber intelligence and information-sharing initiatives. There may be a need to better understand and explore whether the envisaged** framework needs, and if so how, to ensure collaboration with financial sector cyber intelligence and information-sharing initiatives that have been established at national and/or EU level, and involve financial entities or authorities accordingly. Examples of such initiatives are also referenced in the current DORA proposal and have already been established through the Cyber Information and Intelligence Sharing Initiative (CIISI-EU) of the Euro Cyber Resilience Board (ECRB) and in several Member States.[51]

3.3.2 Coordination among financial authorities

Financial authorities must be prepared to deal with the financial consequences of a cyber event. Therefore, an effective EU-SCICF should be in place before any cyber incident develops into a systemic event. The definition of clear action plans between financial authorities is necessary to ensure proper coordination among the authorities involved in the financial, technical and operational aspects of crisis management. Regarding the coordination among financial

50 See European Commission (2021a).

51 See ECB (2020a).

authorities, interfaces between existing international and domestic frameworks also need to be considered.

Key elements of good coordination for financial authorities are:

- **Proper activation and escalation processes and situational awareness.** Authorities should be made and become aware of a cyber incident as early as needed to ensure proper crisis management and to mitigate the risk of inaction. Therefore, the framework needs to provide clear guidance to financial authorities on when the framework should be activated. All financial authorities should be allowed to activate the framework. An escalation mechanism should allow the activation of different parts of the framework depending on the gauged severity of the incident. Predefined systemic incident impact thresholds, such as those proposed in the Commission blueprint, may be appropriate for triggering activation and escalation. Reclassification of any incident according to new information and impact changes should be possible to take account of the fast-paced nature of cyber incidents.

- **Clear responsibilities of framework participants.** The framework should set out guidance on who should lead the response following activation and the basis for participation in the response. Overall, it is of utmost importance to clarify how the responsibility for crisis coordination and leadership will be assigned to and tasks distributed among financial authorities. Participation is likely to be guided by the level of impact on the financial sector and subsectors in different Member States. In addition, financial authorities should have flexibility in terms of the modalities of participating in the EU-SCICF based on their assessment of the local situation and impact on the financial sector.

- **Clear and predefined action plans.** With swift action being a critical factor in counteracting a cyber incident, coordination requires clear guidelines for dealing with cyber events. The framework should include high-level action plans to respond diligently to predefined types of incidents and scenarios, avoiding potential friction in the activation and coordination stages. In the event of an incident, initial actions, proportional to the severity of the event or depending on the framework escalation phase, should be automatically triggered. These action plans should be a means to respond quickly to certain types of events rather than universal formulas, but they also should be flexible enough to allow authorities to adapt them to different contexts that may be associated with the same type of incident.

- **Interfaces for cross-sectoral and global coordination.** The interaction with existing frameworks and authorities needs to be considered (see Section 3.2). Interfaces with international frameworks should be considered to enable global collaboration.

3.3.3 Communication with the public and the media

Coherent communication by financial authorities can be a trust-building measure in a potential systemic cyber crisis. Beyond the magnitude of potential financial losses, uncertainty and the loss of confidence are critical catalysts in triggering financial instability.[52] In such a

[52] See ESRB (2020).

situation, coherent and timely communication and dissemination of accurate information are important.[53] It is the role of financial authorities to conduct confidence-building communication with the public and thus mitigate a cyber incident's amplification through the confidence contagion channel (Figure 1).

Key elements of external communication are:

- **Coherent communication by financial authorities with the public to preserve confidence.** The framework should provide a coordination mechanism with predefined guidance for financial authorities involved in the crisis response to agree, where required, on a common level of information and sequence of external communication. Within this framework, each authority should communicate in line with its own mandate. Such coordination mechanisms would help in defining which information can be shared with the public.

- **Predefined communication lines for timely communication.** Predefined plans can save time during the communication process and thus allow timely confidence-building communication. External communication should be facilitated by predefined materials (e.g. communication playbooks for certain predefined scenarios indicating sample lines at different stages of the incident and considering both proactive and reactive messages). Given the wide range of potential types and consequences of cyber incidents, predefined materials should be flexible enough to allow their adaptation to different scenarios.

- **Proper communication and countering of fake news.** As part of public communication, a strategy should also be defined for public and social media. To mitigate unjustified mistrust in the financial system, authorities should identify, consider and to the extent possible counter possible fake news or misinformation campaigns that may be active and could erode trust in the financial system during a cyber incident.

3.3.4 Testing and developing the pan-European systemic cyber incident coordination framework

Authorities and financial institutions must be prepared and ready to react in a timely manner to a cyber incident based on predefined frameworks and protocols. Testing the framework with dry-run exercises will allow authorities to evaluate their readiness and preparedness for a systemic cyber crisis at EU level. Authorities can familiarise themselves with agreed rules and procedures, increasing their experience and potentially reducing their response time. Testing the framework will also enable its continuous improvement and development. For effective crisis intervention, the framework's evolution will need to reflect changes in regulation, dependencies and market structures.

Test scenarios should be severe and plausible enough to enable learning. Testing and improving the framework requires the implementation of various scenarios and exercises. Characteristics such as scope, number of participants, complexity, objectives and frequency may

[53] See also the **Annex to the European Commission Recommendation on coordinated response to large scale cybersecurity incidents and crises** (C(2017) 6100 final).

vary with the purpose of the testing exercises. In any case, increasing the number of participants in exercises increases coordination complexity and thus provides a more realistic scenario.

The following points should be considered:

- **Appropriate framework-testing exercises.** Exercise design should consider dependencies between different institutions, service providers, financial market infrastructures and authorities to test the effect of these interdependencies on cyber crisis dynamics. Critical third-party service providers should also be considered for exercises. The increasing dependency of the financial sector on third-party providers can make the latter and their crisis-management procedures critical elements in a cyber crisis. Their involvement can vary from real-time participation to simulated participation in the script of the exercise, depending on the exercise's scope and level, since real-time interactions may add too much complexity. Specific roles for framework-testing tasks, such as creating the scenarios and the events of the exercise, analysing the results of the exercise and sharing them with the participants, should be defined.

- **An assessment of each of the exercises should result in lessons learned.** One of the goals of these exercises is to identify potential improvements to policies, procedures, operations and systems, as well as to enhance the efficiency of future exercises. Lessons learned from the exercises should be summarised, taking account of feedback from participants, and shared with participants on a timely basis, and action plans should be agreed on to implement recommended improvements.

- **Exercises should test cross-jurisdictional and relevant third-country coordination.** European authorities should conduct crisis simulation exercises for the purpose of testing the interaction of the EU-SCICF with different authorities' national crisis-management frameworks. This strategy should also consider the involvement of financial institutions and the involvement of and impact on authorities outside the EU with linkages to the EU financial system.

3.4 Initial steps for the development and implementation of the pan-European systemic cyber incident coordination framework

A stepwise framework implementation is suggested. The overall amount of work involved in the implementation of the framework makes it reasonable to conduct a stepwise implementation approach.

Given the importance of effective communication in addressing the risk of a coordination failure, the first elements to be designed and implemented are the key foundations of good communication. The initial focus should be the need for communication channels among financial authorities. Agreeing on a common minimum set of information that will be needed for the framework to operate should be one of the first tasks: the question to be answered is "what has to be shared, how will it be shared, by whom with whom, and when?".

The following proposed steps are intended to provide guidance for financial authorities responsible for the development and implementation of the future EU-SCICF. All steps are equally important, which means that the ordering of the steps is not intended as a proposal of which steps are to be taken first.

1. Define a common vocabulary.
2. Address confidentiality in information sharing upfront.
3. Set up secure and reliable information-sharing channels.
4. Establish points of contact.
5. Ensure proper activation and escalation processes through situational awareness.
6. Define clear responsibilities for framework participants.
7. Consider interfaces for cross-sectoral and global coordination.

Financial authorities in the EU are well placed to support the implementation of the EU-SCICF. Successful management of a systemic cyber crisis will depend on the capabilities of each authority to interact with other financial and cyber authorities at European level. Here, the EU-SCICF principles should serve as a reference point for the required capabilities of European financial authorities.

The future framework needs to be properly developed, maintained and updated, given the constant evolution of technology, the financial sector and the cyber threats it faces. The suggested stepwise approach of designing the framework focuses on basic communication elements first. Once these basic elements are set out, the framework can incorporate the remaining elements proposed in Section 3.3 as well as improve the already established capabilities. The actual implementation of the future framework would involve a formal policy choice, also taking stock of the implementation of DORA. Framework definition should include reviews and features that prevent it from becoming a static mechanism, as this would risk its components becoming outdated and hence not fit for purpose during a systemic cyber crisis.

As the framework will only be activated during systemic cyber crises, consideration should also be given to exercising the framework from its design stage to assess its fitness for purpose, identify lessons learned and support its ongoing development. For example, as an initial step, a “call tree” exercise could be conducted to clarify who would be involved in different jurisdictions when responding to a cyber incident involving the financial sector. In addition, responsibility for framework maintenance could be independent from leadership during framework use.

4 Conclusion

The report discusses the capabilities of financial authorities to mitigate systemic cyber risk. Capabilities to monitor and analyse the financial and cyber risk associated with a systemic cyber crisis are needed to develop and calibrate specific tools to address systemic cyber risk. In addition, financial authorities need to be prepared for the management of a systemic cyber crisis. Swift coordination among financial authorities at EU level to tackle a major cyber incident can help to contain its impact on financial stability, maintain confidence in the financial system and limit contagion effects on other financial institutions, thus preventing a major cyber incident from becoming a risk for financial stability.

Of particular importance in mitigating systemic cyber risk is the need to overcome the risk to financial stability stemming from a coordination failure during the response to an incident. The report identifies the need for a pan-European systemic cyber incident coordination framework for financial authorities (EU-SCICF) to address the risk of a coordination failure. The main objective of the EU-SCICF would be to increase the level of preparedness of financial authorities to respond effectively to a major cyber incident that poses a systemic risk to the EU financial sector. The EU-SCICF's key elements are based on the ESRB's assessment of framework characteristics that would be needed, prima facie, in order to address the risk of a coordination failure.

A pan-European framework such as the EU-SCICF does not exist yet and needs to be developed and established. The ESRB recommends incorporating this task into one of the envisaged roles of the ESAs under the DORA proposal. The EU-SCICF would introduce a macroprudential focus in addition to the proposed DORA focus on individual institutions. Given the risk to financial stability in the EU stemming from cyber risk, preparatory work for the gradual establishment of the EU-SCICF should, to the extent feasible, start even before the required legal framework for its establishment is fully applicable.

The work on additional required (macroprudential) tools to mitigate systemic cyber risk needs to continue. The report outlines the main concepts of a monitoring framework for systemic cyber risk. Systemic cyber resilience scenario stress tests are identified as a valuable tool to test how systemic institutions in the financial system would respond to and recover from a severe but plausible cyber incident scenario. To draw conclusions from systemic cyber resilience scenario stress tests on financial stability, macroprudential authorities need to define an acceptable level of disruption to operational systems providing critical economic functions.

The ESRB intends to support future work on systemic cyber risk and the required tools to address this. Findings of this work may also provide advice for the legislative review of the EU macroprudential framework as requested from the ESRB by the European Commission.[54]

[54] See European Commission (2021b).

Annexes

A1 Assessment of the ESRB's intermediate objectives and existing macroprudential instruments

IO1: mitigate and prevent excessive credit growth and leverage.

While this objective seeks to address cyclical risks, systemic cyber risk is perceived as a structural risk that can materialise at any stage in the economic cycle.[55] No direct causal link exists between systemic cyber risk and excessive credit growth and the build-up of leverage in the financial system. However, a direct link exists between a financial institution's level of capitalisation and its ability to absorb financial losses that may materialise in a cyber incident and, ultimately, confidence in the institution and its ability to extend credit to the real economy. Thus, capital-related countercyclical macroprudential instruments will not be able to remediate operational failures but may play a mitigating role in the transmission and amplification phases of the shock. The same applies to structural capital instruments in IO4.

IO assessment: IO1 is only of limited use for the development of systemic cyber risk mitigants.

Macroprudential instruments associated with IO1 that address cyclical risk appear irrelevant in the context of systemic cyber risk (e.g. loan-to-value, loan-to-income and debt service-to-income requirements and sectoral risk weights). More generally, all capital-related macroprudential instruments could help to preserve confidence during crises and mitigate cyber risk amplification related to financial losses triggered by a cyber incident. However, a deeper understanding of the potential financial losses that could occur in a systemic cyber crisis is required.[56] At the current juncture, it remains unclear if macroprudential capital requirements should be made contingent on systemic cyber risk. This may overburden these instruments, while more direct (non-capital-related) requirements on cyber resilience are likely to be more effective in mitigating systemic cyber risk.

IO2: mitigate and prevent excessive maturity mismatch and market illiquidity.

A cyber incident can impair market liquidity and lead to an unexpected materialisation of funding risk related to not even necessarily excessive maturity mismatch. A cyber incident can lead to a direct loss of or loss of access to assets, thus disrupting an institution's capacity to fund its operations. Disruptions can be caused by liquidity/fund thefts, irrevocable deletion or corruption of records at a market infrastructure, or operational disruption of infrastructure or a critical third-party. The disruption could propagate the liquidity shortages to other institutions or infrastructures connected to those affected or may disrupt operations and cause a loss of confidence in financial institutions or whole market segments. The contagion effects could be proportional to the systemic relevance of the entities affected, especially in the case of critical financial infrastructures that facilitate the flow of liquidity. Importantly, IO2 does not address the specific nature of the liquidity shock and, like capital under IO1 and IO4, instruments to address liquidity risk will not be able to

[55] Nevertheless, there are certain conditions that may exacerbate the frequency of cyberattacks and worsen their impact, such as geopolitical tension, other types of widespread crisis (economic or otherwise), impactful historical events (elections, wars, pandemics), which are either expected and/or have a lasting duration.

[56] See Adelmann et al. (2020) and footnote 42.

remediate the operational root cause of a cyber incident. Nevertheless, a cyber incident may have specific characteristics that could make the use of liquidity instruments more challenging.

IO assessment: the role of liquidity in terms of the transmission and amplification of a cyber incident should be explored further.

Liquidity buffer tools are assessed as relevant systemic risk mitigants. However, these tools are not specifically attuned to cyber risk but target sources of liquidity risk more broadly. These tools set a floor of liquid assets to be held and so increase the absorption capacity of liquidity shocks due to sudden outflows (net of inflows). Since cyber incidents can cause such sudden outflows, liquidity buffer tools could mitigate financial losses related to intermediary failures or asset fire sales driven by illiquidity. Furthermore, these tools would likely help to sustain confidence in the system if intermediaries are able to demonstrate that they can overcome cyber-related liquidity shortages. In the investment fund sector, the suspension of redemptions is the only liquidity instrument available to authorities in Europe and could be activated during a systemic cyber crisis.

Proposal: consider the calibration of liquidity buffers in the context of systemic cyber risk, e.g. in liquidity stress-testing exercises. Implementation of any required buffer could be considered through a macroprudential add-on to the prudential minimum requirement.[57]

IO3: limit direct and indirect exposure concentration.

In the case of systemic cyber risk, contagion arises not only at the financial but also at the operational level. While direct exposures emerge through shared data or significant business relationships, indirect exposures arise through the interconnectedness of various information systems or common service providers and operational systems. The existence of sector-wide technology components and service providers creates common (technological) vulnerabilities. The currently missing operational dimension in IO3 should be considered in the context of cyber risk. Also, the inclusion of a reference to operationally relevant large exposures would be needed, since cyber risk amplifiers are not always related to an intermediary's balance sheet size but also to its operational and financial substitutability. Financial exposure concentration is still of relevance. A cyber incident's severity could be exacerbated if intermediaries' (short-term) funding relies on only a few other institutions. Although it might reduce the likelihood of a (technically) failing counterparty, it may increase the impact in the event of a failure. In addition, cyber risk can also be a source of credit risk related to exposures to non-financial corporations, whose ability to fulfil their credit obligations may depend heavily on their own operating ICT systems.

IO assessment and proposal: the scope of IO3 could be expanded to also include operational exposures and may provide a basis for the development of systemic cyber risk mitigants.

IO4: limit the systemic impact of misaligned incentives with a view to reducing moral hazard.

The ESRB's 2020 report on systemic cyber risk concluded that institutions may have an incentive to not allocate sufficient resources to cybersecurity and instead allocate resources to more "visible" areas (i.e. focusing on profits and growth) at the expense of preparing for operational disruptions.[58]

---

57 See ESRB (2018), p. 9.

58 See ESRB (2020).

For instance, small firms may consider the relevant IT investments as disproportionally large and be disincentivised to make them, although the firms themselves may pose the same cyber risk to other financial institutions as larger firms. Another example of misaligned incentives could be the fear of reputational impact, such that institutions may have a disincentive to share information with other entities after they have suffered a cyber incident, thus reducing opportunities to improve the management of existing vulnerabilities. SIIs and systemically important technology companies (SI-techs) may be too big or interconnected to fail, however an implicit bailout guarantee is less likely, as a transfer of funds or liquidity provision will not directly remediate the operational root cause of a cyber incident. Cyber risk-related "bailouts" may take place through measures on the operational side, for example through increased or timelier allocation of limited incident-solving resources.

Moral hazard effects should be considered when designing or using any macroprudential tool or other measures employed by authorities and governments to deal with a systemic cyber crisis. Depending on the sharing of costs between the institutions and authorities, moral hazard effects may arise. If institutions do not bear the full costs of the cyber risk they take, and hence make insufficient investments in cyber resilience, systemic risk from cyber may emerge. Moreover, if a competitive advantage can be gained through higher cyber risk-taking, for instance by not investing sufficiently in resilience or having backup providers, other competitors will be less incentivised to make the socially optimal investment in their cyber risk resilience. This problem may be particularly valid for cyber insurance.

IO assessment: IO4 may provide scope for the development of systemic cyber risk mitigants and points to the need to further explore the concept of "too interconnected to fail". Structural capital buffers, for instance SII buffers and systemic risk buffers (SRBs), increase intermediaries' capital positions and are therefore appropriate in absorbing financial losses in the context of a cyber incident. These buffers address structural systemic risk, like cyber risk, so that operational importance can be considered as an additional determinant of the buffer size calibration. However, further analysis is needed as to whether such an amendment is needed, or the operational dimension is already covered by related indicators such as interconnectedness with other institutions, substitutability or complexity. Systemic cyber resilience scenario stress tests may be a relevant tool to determine systemically important intermediaries. Conceptually, overlaps with the framework for the designation of core financial infrastructure may exist and need to be further explored.

At the current juncture, it remains unclear if macroprudential capital requirements should be made contingent on systemic cyber risk. This may overburden these instruments, while more direct (non-capital-related) requirements for cyber resilience are likely to be more effective in mitigating systemic cyber risk.

Proposal: expand the definition of systemically important intermediaries in the context of operational availability. This assessment should include financial intermediaries and third-party providers. Indicators and tools to determine operationally important firms would need to be developed. In this context, systemic cyber resilience scenario stress test results and critical downtimes of operational systems are potential indicators.

Proposal: Integrate cyber scenarios into stress test exercises to assess capital losses related to cyber events.

IO5: strengthen the resilience of financial infrastructures.

The reasoning of IO5 does not explicitly consider exogenous events, such as cyber incidents, that could threaten financial stability. Moreover, in the context of cyber, a pure focus on the resilience of financial infrastructure omits other financial institutions or even third-party technology providers. These institutions could function as shock amplifiers if they provide crucial functions that are difficult to substitute (see Figure 1). The definition of "resilience" should be adapted to the cyber context, where it is slightly different in that it refers to withstanding, containing and rapidly recovering from cyber incidents and thereby protecting the confidentiality, integrity and availability of information (data). Due to the speed and scale characteristics of cyber incidents, interconnectedness plays a crucial role in defining the systemic risk arising from cyber incidents; therefore, these two aspects should be considered in designing appropriate mitigation tools. Other aspects that may need to be further explored in the context of this objective encompass the identification of mitigants that are considered critical from a macroprudential perspective because they contribute to the resilience of assets without which an institution cannot operate, as well as potential effects of the operational impact of a cyber incident on other types of mitigants (especially those of a financial nature that are included in the toolbox of IO1 and IO2).

Initial assessment: the scope of IO5 could take a broader perspective on financial system resilience (beyond infrastructures), thereby providing a suitable basis for the development of systemic mitigants.

Proposal: consider the inclusion of any entity with appreciable (operational) "significance" or "centrality" in the financial system in systemic cyber resilience scenario stress tests.

A2 Scheme with key elements of the pan-European framework

		Key elements of the framework		Evolution of the framework
		Communication	Coordination	Testing
Stakeholders	Financial authorities	(i) A common vocabulary should be used. To ensure the appropriateness of the information exchanged, steps should be taken to ensure its uniformity and its easy understanding. (ii) A cyber incident needs to be classified in a timely manner depending on its severity. (iii) Reliable and secure channels and tools for information sharing reduce barriers that may arise when sharing highly confidential information.	(i) Authorities should be made aware of a major cyber incident as early as needed to ensure proper crisis management and to mitigate the risk of inaction. (ii) An escalation mechanism should allow the activation of different parts of the framework depending on the gauged severity of the incident. (iii) With swift action being a critical factor in counteracting a cyber incident, coordination requires clear guidelines for dealing with cyber events. (iv) Interfaces with international frameworks should be considered to enable global collaboration.	(i) Test scenarios should be realistic to enable learning. (ii) Exercise designs should consider dependencies between different institutions, service providers, financial market infrastructures and authorities. (iii) Exercises should test cross-jurisdictional coordination.
	Public	(i) Coherent communication by financial authorities with the public will preserve confidence (ii) Communication impact can be increased by aligning institutions' communication (iii) Predefined communication lines will ensure timely communication. (iv) Fake news should be countered (v) Public communication should also take into account a strategy for public and social media.	(i) The framework should provide a coordination mechanism with predefined rules for financial authorities involved in the crisis response. (ii) Coordination activities between the authorities must take place in such a way as to maintain public confidence.	

Source: ESRB.

References

Adelmann, F., Elliott, J., Ergen, I., Gaidosch, T., Jenkinson, N., Khiaonarong, T., Morozova, A., Schwarz, N. and Wilson, C. (2020), "**Cyber Risk and Financial Stability**: It's a Small World After All", IMF Staff Discussion Notes, No 20/07, International Monetary Fund, December.

Adelmann, F., Gaidosch, T., Morozova, A. and Wilson, C. (2019), "**Cybersecurity Risk Supervision**", Departmental Paper Series, No 19/15, International Monetary Fund, Monetary and Capital Markets Department, September.

Aldasoro, I., Gambacorta, L., Giudici, P. and Leach, T. (2020), "**Operational and cyber risks in the financial sector**", BIS Working Papers, No 840, Bank for International Settlements, February.

Banca d'Italia, Autorité de Contrôle Prudentiel et de la Résolution, Commissione Nazionale per le Società e la Borsa, Deutsche Bundesbank, European Central Bank, Federal Reserve Board, Financial Conduct Authority, Ministero dell'Economia e delle Finanze, Prudential Regulation Authority and U.S. Treasury (2021), "**Proposal for a common categorisation of IT incidents**", Markets, Infrastructures, Payment Systems Series, No 6, Banca d'Italia, May.

Banka Slovenije (2021), **Financial Stability Review**, April.

Bank for International Settlements and International Organization of Securities Commissions (2016), **Guidance on cyber resilience for financial market infrastructures**, June.

Bank of England, Prudential Regulation Authority and Financial Conduct Authority (2018), "**Building the UK financial sector's operational resilience**", Discussion Paper Series, No 01/18, Bank of England, July.

Bank of England (2021), **Financial Policy Summary and Record of the Financial Policy Committee Meeting on 11 March 2021**.

Bank of England, Prudential Regulation Authority and Financial Conduct Authority (2021), "**Operational resilience: Impact tolerances for important business services**", Responses to Bank CPs relating to FMIs, March.

Basel Committee on Banking Supervision (2013), **Global systemically important banks: updated assessment methodology and the higher loss absorbency requirement**, Bank for International Settlements, July.

Basel Committee on Banking Supervision (2021), **Principles for Operational Resilience**, Bank for International Settlements, March.

Bouveret, A. (2018), "**Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment**", IMF Working Papers, No 18/143, International Monetary Fund, June.

Central Bank of Ireland (2021), "**Consultation on Cross Industry Guidance on Operational Resilience**", Consultation Paper Series, No 140, Central Bank of Ireland, April.

CERT-EU (2021), **Multiple Vulnerabilities in SolarWinds Orion**, January.

Duffie, D. and Younger, J. (2019), "**Cyber Runs**", Hutchins Center Working Paper Series, No 51, Hutchins Center on Fiscal & Monetary Policy at Brookings, June.

Eisenbach, T.M., Kovner, A. and Lee, M.J. (2021), "**Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis**", Federal Reserve Bank of New York Staff Reports, No 909, Federal Reserve Bank of New York, May.

European Banking Authority (2019), **EBA Guidelines on ICT and security risk management**, November.

European Central Bank (2017), **Cyber resilience and financial market infrastructures**.

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

European Central Bank (2020a), "**Major European financial infrastructures join forces against cyber threats**", ECB press release, 27 February.

European Central Bank (2020b), **Annual report on the outcome of the SREP IT Risk Questionnaire**, June.

European Central Bank (2021a), "**IT and cyber risk: a constant challenge**", Supervision Newsletter, 18 August.

European Central Bank (2021b), **Financial Stability Review**, May.

European Commission (2020), "Impact assessment report accompanying the document proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act)", Commission Staff Working Document, No 295, November.

European Commission (2021a), "**EU Cybersecurity: Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents**", European Commission press release, 23 June.

European Commission (2021b), **Review of the EU Macroprudential Framework – Call for advice**, July.

European Insurance and Occupational Pensions Authority (2020), "**EIOPA sets out strategies on cyber underwriting and SupTech**", EIOPA press release, 11 February.

European Systemic Risk Board (2014), **Flagship Report on Macro-prudential Policy in the Banking Sector**, March.

European Systemic Risk Board (2018), **The ESRB handbook on operationalising macroprudential policy in the banking sector**.

European Systemic Risk Board (2020), **Systemic cyber risk**, February.

European Systemic Risk Board (2021a), **Adverse scenario for the European Securities and Markets Authority's 2021 EU-wide central counterparty stress test**, June.

European Systemic Risk Board (2021b), **Policy framework**.

European Union Agency for Cybersecurity (2021a), **EU Cybersecurity Initiatives in the Finance Sector**, March.

European Union Agency for Cybersecurity (2021b), **Glossary**.

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

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

Financial Stability Board (2021), **FSB Financial Stability Surveillance Framework**, September.

Goh, J., Kang, H., Koh, Z.X., Lim, J.W., Ng, C.W., Sher, G. and Yao, C. (2020), "Cyber Risk Surveillance: A Case Study of Singapore", IMF Working Papers, No 20/28, International Monetary Fund, February.

Heijmans, R. and Wendt, F. (2020), "Measuring the Impact of a Failing Participant in Payment Systems", IMF Working Papers, No 20/81, International Monetary Fund, June.

International Organization of Securities Commissions (2020), "**Principles on Outsourcing**", Consultation Report, No 01/2020, May.

Moody's (2021), **Sunburst attack on public and private entities raises credit risks as extent of breach unfolds**.

Imprint and acknowlegements

This report was approved by the ESRB General Board on 2 December 2021. It was prepared by the European Systemic Cyber Group, chaired by Francesco Mazzaferro of the European Systemic Risk Board and Paul Williams of the Bank of England under the auspices of the ESRB Advisory Technical Committee. Substantial contributions were made by:

Alexander Harris	Francesco Mazzaferro (Co-chair)
ESMA	ESRB Secretariat
Aiofe Langford	Francesco Sciamanna
Central Bank of Ireland	Banca d'Italia
Alexandros Kaliontzoglou	Gabriella Biró
Bank of Greece	Magyar Nemzeti Bank
Boris Augustinov	Hannah Green
European Commission	Bank of England
Borut Poljšak	Jose Munera
Banka Slovenije	Banco de España
Carla Marques	Julien Dotter
Banco de Portugal	Banque de France
Christoph Fricke (Secretary)	Kiethan Vijayabalan
ESRB Secretariat	ESRB Secretariat
Christoph von Busekist	Maarten Willemen
Deutsche Bundesbank	De Nederlandsche Bank
Christophe Macé	Márcio Mateus
Banque de France	Banco de Portugal
Claudiu Negrea	Paul Williams (Co-chair)
Banca Naţională a României	Bank of England
Claus Sengler	Ruaxandra Gabriela Adam
European Central Bank	European Commission
Constantinos Christoforides	Thiebaut Meyer
European Central Bank	Banque de France
Daniela Lo Monaco	Thomas Lauterbach
Banca d'Italia	BaFin
Dina Batista	Tom Keating
Banco de Portugal	Central Bank of Ireland
Ezgi Delikanli	Viktorija Grybauskaitė
Deutsche Bundesbank	Lietuvos bankas
Fiona van Echelpoel	Wolfgang Sommerfeld
European Central Bank	European Central Bank
	Ylva Søvik
	Norges Bank

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 978-92-9472-254-6, doi:10.2849/99500, DT-05-22-016-EN-N