Financial Stability Institute | BIS

FSI Briefs

No 30

Cyber risk stress testing for banks

Patrizia Baudino

April 2026

FSI Briefs are written by staff members of the Financial Stability Institute (FSI) of the Bank for International Settlements (BIS), sometimes in cooperation with other experts. They are short notes on regulatory and supervisory subjects of topical interest and are technical in character. The views expressed in this publication are those of the authors and do not necessarily reflect the views of the BIS, its member central banks or the Basel-based standard-setting bodies. Furthermore, the views expressed in this publication do not reflect the views of the authors' employers or firms.

Authorised by the Chair of the FSI, Fernando Restoy.

This publication is available on the BIS website (www.bis.org). To contact the BIS Global Media and Public Relations team, please email media@bis.org. You can sign up for email alerts at www.bis.org/emailalerts.htm.

ISSN 2708-1117 (online)
ISBN 978-92-9259-937-9 (online)

Cyber risk stress testing by authorities for the banking sector[1]

Highlights

- *In the context of growing frequency and sophistication, and increasing potential impacts of cyber incidents, some authorities have disclosed that they are conducting cyber stress tests to enhance firm and sector resilience to operational disruptions, such as those caused by cyber attacks.*
- *These tests benefit both authorities and firms by identifying vulnerabilities and strengthening response and recovery mechanisms as well as, in some circumstances, identifying the financial stability impacts of such disruptions.*
- *Based on recent exercises, two distinct approaches emerge, namely firm- or system-focused cyber stress tests. It is important for the authority in charge to select the approach that best reflects the institutional setup and the objectives of the stress test, ensuring consistency across all parts of the exercise.*
- *Continued enhancements and disclosure of the methodological aspects in cyber stress tests can help raise awareness and establish best practices.*

1. Introduction

In response to the increasing frequency, sophistication and potential impact of cyber incidents,[2] authorities have adopted a range of tools aimed at testing firms' preparedness for managing cyber risk.

Ideally, a comprehensive testing programme for cyber risk should be composed of vulnerability assessments, scenario-based testing, penetration tests and red team tests (see Committee for Payment Systems and Infrastructure (CPMI) and International Organization of Securities Commissions (IOSCO), CPMI-IOSCO (2016)).[3] Among these, scenario-based and penetration/red team testing offer a complementary approach to identifying weaknesses. Penetration/red team tests simulate cyber attacks on live systems to identify exploitable vulnerabilities.[4] Conversely, scenario-based stress testing, or more broadly, a stress test, assumes that firms' preventative measures have failed, and focuses on firms' cyber incident response and their recovery, ie their operational resilience.

[1] Patrizia Baudino (patrizia.baudino@bis.org), Bank for International Settlements. The author is grateful to officials in the selected authorities and the European Systemic Risk Board Secretariat for helpful discussions, to Rodrigo Coelho, Ting Yang Koh, Jermy Prenio, Caleb Wu and Hao Ying Yang for insightful comments, and to Theodora Mapfumo for administrative support.

[2] See for instance Khiaonarong and Shanyuan (2026) for a discussion of the rise of cyber events.

[3] Global standard setters have provided guidance on the concept of cyber risk and methodologies to address it. In addition to the 2016 report by the BIS Committee for Payment Systems and Infrastructure (CPMI) and the International Organization of Securities Commissions (IOSCO), see also reports by the Basel Committee on Banking Supervision (BCBS (2018)), the Financial Stability Board (FSB (2023)), the International Association of Insurance Supervisors (IAIS (2023a,b)), the BIS Committee for Payment Systems and Infrastructure (CPMI (2025)) and CPMI-IOSCO (2022). FSB (2025a) developed incident reporting, the so-called Format for Incident Reporting Exchange (FIRE), to improve incident reporting, including cyber incidents.

[4] An example of such tests is, in the European Union, the Threat Intelligence Based Ethical Red Teaming (TIBER-EU). This framework provides comprehensive guidance on how authorities, entities, threat intelligence providers and red team testers should work together to test and improve the cyber resilience of entities by carrying out controlled cyber attacks (see ECB (2025)). In a similar way, in the United Kingdom, authorities adopt the CBEST framework (Bank of England (2024b)). For examples from other jurisdictions, see Prenio et al. (2019).

While cyber stress tests cannot fully replicate the impact of a real-life cyber incident, they provide authorities and firms with valuable insights into the effectiveness of their response processes. In particular, the static nature of such exercises allows firms to work through their planning and preparation, and assess its effectiveness. This, together with the extended timespan over which a stress test is conducted, gives firms and authorities room to identify critical arrangements in their response strategies, assess possible weaknesses in their design and reflect on their suitability.

The relative novelty of cyber stress tests means that experience of conducting them is somewhat limited at the present time.[5] Moreover, disclosure is currently very restricted, both in terms of the number of publishing authorities and the extent of the information that is released. This cautious approach reflects the need to preserve confidentiality around the scope and findings of the exercises, to avoid exposing participating firms to malicious attacks.

Nonetheless, the Bank of England, the Danish Financial Supervisory Authority (DFSA) and the European Central Bank (ECB) Banking Supervision have recently published reports on their cyber stress tests (Bank of England (2025), DFSA (2024) and ECB (2024)).[6] This FSI Brief reviews the main aspects of these three exercises, which were selected on the basis of the relatively more extensive disclosure and range of approaches they represent. They also exhibit a relatively high degree of comparability due to their shared focus on banks and the banking sector, and were nearly simultaneous.[7]

Drawing on these examples, the Brief highlights critical considerations for authorities when designing and implementing cyber stress testing exercises. Section 2 defines a cyber stress test for the purposes of this paper. Section 3 introduces the two approaches authorities can adopt when conducting a cyber stress test, ie either system or firm focused. Sections 4–6 present the main building blocks of a cyber stress test and discuss the choices authorities need to take about them. Section 7 concludes.

2. Defining a cyber stress test

In principle, authorities can cover cyber risk in a stress test in two ways (ESRB (2022)).[8] In one, cyber risk is included within existing financial stress testing, putting emphasis on financial losses stemming from a

[5] The International Monetary Fund (IMF) has recently published a collection of good practices in cyber risk regulation and supervision, drawing from its financial surveillance and technical assistance work (Gaidosch et al, 2026). Furthermore, the IMF has supported financial authorities in enhancing their preparedness to address cyber risks. This effort is part of the work conducted in collaboration with these authorities under the Financial Sector Assessment Programs (FSAPs), where cyber stress testing is included as a key area of analysis. For example, this approach was applied in the recent euro area FSAP (IMF, 2025a).

[6] The Bank of England is considered among the first authorities to disclose findings of its cyber stress tests, starting in 2023 (Bank of England (2023b)). For both the DFSA and the ECB, the exercises covered in this Brief are the first of their kind (references to the ECB Banking Supervision exercise are marked as ECB for convenience but are to be understood as having been performed by the supervisory side of the ECB). For comparability, the description of the Bank of England exercises refers to the one conducted in 2024 unless explicitly noted.

[7] Only a few other authorities have released some disclosure about their recent cyber risk stress tests. For instance, the central banks of Portugal (Banco de Portugal (2024)), and, more extensively, Slovenia (Poljšak and Bračković (2025)). Both are based on the ECB-led exercise discussed in this paper, and complement it with a system-wide analysis, at the domestic level. The Reserve Bank of Australia (2024) reported conducting a cyber attack exercise focusing on the country's high-value payments system. For references to earlier cyber stress tests, see Crisanto et al (2023). Examples of how authorities manage cyber risks are discussed by the Financial Stability Board (FSB) in its recent peer reviews (FSB (2025b,c)), and by the International Monetary Fund (IMF) in its Article IV missions (IMF (2025b)), as well as FSAPs as mentioned above.

[8] There is a growing literature covering conceptual frameworks for cyber stress tests. This includes a report on fundamental elements of cyber exercise programmes by financial authorities by the Group of Seven (G7 (2020)), a handbook for cyber risk stress testing for critical sectors, including banks, by the European Union Agency for Cybersecurity (ENISA (2025)), and several

cyber attack. For instance, liquidity stress tests could be extended by including cyber attacks among the triggers of a liquidity shortage (IMF (2024)).[9]

Alternatively, cyber risk is treated separately from other factors, and the analysis focuses on the very early phase of a cyber crisis cycle. In this case, the stress test – cyber stress test proper – aims to assess the operational capability of the firms, and possibly of the financial system at large, in the event of a cyber incident. Given the specific focus on operational aspects, these exercises are more amenable to "playing out" the stress scenario directly involving the firms, in a table-top format. The three examples discussed here fall into this second category.

Next, designing a cyber stress test requires a different framework to that of solvency and liquidity stress tests, which have become a well established part of authorities' toolkit. Among the most relevant differences are the lack of a single quantitative indicator to measure the impact of the stress factors, and the recognition that balance sheet indicators are not suitable yardsticks. Incidentally, because of their qualitative nature, it could be argued that "scenario-based testing" may be the more suitable terminology (CPMI-IOSCO (2016) and IMF (2025a)).[10]

Cyber stress tests are typically not devised as pass/fail exercises, even when conducted under the supervisory purview of the relevant authority. Instead, and especially considering that cyber stress tests have only been conducted over the past few years and there is not yet a well established framework to conduct them, authorities often treat them as learning opportunities and exploratory in nature.

Moving away from a quantitative focus in cyber stress tests also has implications for deriving an assessment at the system, rather than at the firm, level. Contrary to solvency or liquidity stress tests, the system-wide perspective does not stem from aggregating some metric of distress across firms. Rather, it stems from reviewing the extent to which firms' operational responses have sufficient capabilities to respond, recover and mitigate the impacts of disruptions that could affect the financial system as a whole.

Separately, the lessons from cyber stress tests can be applied more broadly than those from only cyber incidents, as their format is suitable for studying a wide range of shocks to operational resilience.[11] This is because, from the authorities' perspective, the defining starting point is that a disruption has occurred and preventative measures have failed.[12] Nonetheless, the growing occurrence of cyber attacks has made stress tests specifically designed for cyber risk an increasingly valuable component of authorities' toolkit. Moreover, while cyber incidents may be as significant a trigger of operational stress as cyber attacks, the latter are considered to be more demanding, as they are likely to be more intense to last longer.

reports for cyber stress tests for the financial sector – mostly from a macroprudential perspective – by the European Systemic Risk Board (ESRB (2020, 2022, 2023, 2024)). Related research papers include, from a US perspective, Kotidis, and Schreft (2022) and Eisenbach et al (2021); from the IMF, Khiaonarong et al (2025), and from the ECB, with a macroprudential focus, Vermeulen et al (2025).

[9] Duffie and Younger (2019) present such a scenario, where uncertainty around the nature of a cyber attack dries up liquidity in the financial system, affecting both banks and non-banks. Hoarding of liquidity and non-banks' lack of access to the central bank's liquidity lines can trigger a systemic crisis.

[10] For consistency with the terminology in the three reports covered in this Brief, the term "stress test" is used here too.

[11] Stresses to operational resilience with a different cause could also be studied via these stress tests, eg a power outage due to physical infrastructure shortcomings, a faulty update in software or the unexpected cancellation of a banking licence due to geopolitical risk.

[12] Following the terminology adopted in the three reports discussed in this Brief, the words "cyber risk" and "cyber stress tests" are used throughout.

3. Two approaches to cyber stress testing

The main decision for the authority in charge of a cyber stress test is to define whether the exercise is to focus on the operational resilience of the financial system or of individual firms. Both approaches have merit and should be selected by the authority in charge depending on the institutional setup in its jurisdiction and the objectives of the stress test. The choice should be spelled out clearly and from the outset to ensure consistency throughout the conduct of the exercise. This reflects the fact that, in a well designed cyber stress test, choosing one or the other approach drives the design of almost all elements of the exercise.

In a system-focused exercise, the analysis builds on the contribution by individual firms, with the aim of assessing the resilience of the financial system as a whole. In a firm-focused exercise, the objective is to assess how firms would respond to and recover from cyber security incidents and detect deficiencies in those firms' operational resilience frameworks.[13]

Exercises that adopt a system-wide perspective consider some additional objectives, such as helping participating firms to assess how the operational disruption of their services could have a financial stability impact, through financial, operational and confidence channels. Such exercises can enhance firms' understanding of the system-wide repercussions of their atomised responses, and the disruptions these may cause. Considering that firms have traditionally focused their analysis on the impact of a shock on their own resilience and less on the system as a whole, these exercises can help to increase firms' awareness of such implications, as well as familiarise them with the authorities' tolerance for disruptions to operations in the financial system that may stem from the response of individual participants.

Furthermore, each firm may prioritise restoring its own operational capacity and may not fully account for the externalities its own decisions could impose on the rest of the financial system. Studies have shown that firms have incentives to underinvest in cybersecurity in comparison with the socially optimal level because of asymmetric information between themselves and their customers (see eg Anand et al (2022) and Ahnert et al (2022)). A system-wide stress test can highlight relative weaknesses of firms' cyber responses to a common shock and identify possible needs for remediation.

The distinction between a system- versus firm-focused approach also shapes the relationship with participating firms and the degree of prescriptiveness in the exercise. In system-focused exercises, given the complexity of deriving a system-wide assessment and the absence of regulatory expectations to measure firms against, at system level, it can be expected that authorities will put more emphasis on a learning perspective, both for the authorities and the firms. Considering that authorities may not be as well placed as market participants to identify the most appropriate way of building contingency or mitigation measures to address novel or very technical vulnerabilities, the exploratory nature of the exercise may provide more room for firms themselves to provide feedback and input about the design of the exercise. Conversely, firm-focused exercises are more likely to put more emphasis on prudential aspects and possibly follow-ups; they may therefore require an arm's-length relation between firms and authorities. Nonetheless, this can be affected by the traditional supervisory culture in a given jurisdiction, allowing for a more cooperative approach where this is the norm.[14]

[13] In this context, Prenio and Restoy (2022) argue for explicitly recognising the need to perform system-level assessment, monitoring and testing of operational resilience policies.

[14] The distinction is not clear cut. For instance, the exercise in Denmark was designed as a learning opportunity, even if it had a supervisory focus and resulted in individual follow-up reports for participating firms. Accordingly, it did not trigger supervisory actions or sanctions.

Motivation for conducting cyber stress tests Table 1

Authority	Motivation
Bank of England	Operational resilience stress testing is a key part of the Financial Policy Committee's (FPC's) medium-term priorities. The operational incidents of most relevance to the FPC are those with the greatest potential to have system-wide impacts. For example, incidents that stem from risks that can be correlated across the financial system, like cyber attacks.
DFSA	The digital dependency, the threat level and the potential consequences of extensive, long-term information and communications technology disruptions mean that there is a need to strengthen operational resilience. It is necessary to ensure that firms are able to manage disruption so that the consequences are manageable for citizens and there is less risk of society coming to a halt as a result of an attack.
ECB	The ECB conducts supervisory stress tests on an annual basis in line with Article 100 of the Capital Requirements Directive. Detecting and addressing deficiencies in supervised banks' operational resilience frameworks, including those stemming from cyber risks, is one of the ECB's Single Supervisory Mechanism priorities for 2024–26.

Sources: Bank of England (2023b, 2025), ECB (2024) and DFSA (2024).

As shown in Table 1, the three selected authorities clearly indicate the motivation for their stress test and adopt either a system-wide or firm-focused approach accordingly. The exercises by the Bank of England and the ECB are examples of the first and second approaches, respectively, mirroring the institutional mandate of the authority in charge. The case of Denmark combines a primarily supervisory approach with some system-wide elements: its exercise focuses on the individual institutions' management of an extensive information and communications technology (ICT) disruption, but an additional motivation is the recognition that a severe ICT disruption has the potential to affect the financial and operational stability of the financial system. Accordingly, the authority leading the exercise is the prudential supervisor (ie DFSA), with the Danmarks Nationalbank as an advisory partner.[15]

The following subsections describe the main building blocks of the cyber stress test, ie the planning (Section 4), conduct (Section 5) and follow-up and disclosure (Section 6), and highlight the implications of choosing to adopt either a system- or firm-focused approach. Table 2 summarises those differences.

Summary of key features of a cyber stress test for banks Table 2

Feature	System-focused exercises	Firm-focused exercises
Motivation	Assess operational resilience of firms, with a focus on incidents with the highest potential for system-wide impacts.	Detecting weaknesses in the operational resilience of individual firms.
Objective	In addition to firm-level impact, consider financial stability consequences.	Assess how firms would respond to and recover from incidents.
Relationship with participating firms	Likely to be involved in a cooperative fashion.	Likely to be at arm's length.
Firms' decision to join the exercise	More likely to be voluntary.	More likely to be compulsory.

[15] After the first cyber stress test (DFSA (2024)), a second cyber stress test was conducted to investigate how a similar disruption may be managed across parties in the sector and to identify the consequences at the sectoral level. Due to the systemic focus of the second test, the DFSA carried out the test in collaboration with the Danmarks Nationalbank. A public report about the test is planned for 2026.

Sample	Relatively small number of firms, including systemic participants in the selected market/activity (both banks and non-banks); useful to include an FMI.	Relatively large number of domestic banks.
Additional scrutiny for systemic firms	Not relevant (the test is designed around systemically important firms, with other firms included to provide a broader view of the impact on the financial ecosystem).	Likely, especially if the number of banks in the sample is large.
Range of activities in scope	Same market for all participants.	Firm specific.
Resource requirements	High/specialised (for both firms and authorities).	High/specialised (for both firms and authorities).
Involved authorities	At a minimum, the authority in charge of financial stability for the banking sector; the exercise could involve corresponding authorities for the other types of participating firms (eg insurance companies, financial market infrastructures); if the exercise also covers cross-border activities, it could involve, to varying degrees, corresponding authorities abroad.	At a minimum, the supervisory authority for banks.
Initial shock in the scenario	System-wide shock; authorities may also choose to shock only a narrowly defined section of a market, or a wider one (ie either a narrow or broad scenario), but at a minimum, the disruption must have the potential to have a financial stability impact.	Firms assume the shock hits them, and not the rest of the industry.
Questionnaire to collect feedback	Relatively short and with open-ended questions.	Rather detailed and long.
Combination of firm-level results	Use of live decision-making elements; workshop with firms; authorities' discussion with firms.	Not the focus of the exercise.
Benchmarking across similar firms	Feasibility depends on the sample (how many firms from each sector are covered in the exercise).	Could be used by authorities to identify outliers.
Disclosure	Limited, only aggregate findings and main lessons.	Very limited – no firm-level disclosure; general lessons could be included in the disclosure.
Supervisory follow-up	Not expected, but firms can identify their own remediation steps when responding to the questionnaire.	Likely, although no automatic prudential implications and no additional capital or liquidity requirements.
Frequency	Potentially valuable to have successive rounds of stress tests (evolve, explore different aspects) – eg the composition of participating firms could be changed over time, as well as change in the scenario.	Potentially valuable to have more tests over time – the scenario could be changed over time.

Source: author's elaboration.

4. Planning a cyber stress test

This section reviews the elements of a cyber stress test that authorities draw out before the exercise starts. These decisions cover the scope of the exercise, both in terms of activities and the sample of firms, as well as the design of the stress scenario. Resource requirements, for both authorities and firms, also need to be estimated and provided for in advance to meet the exercises' demands for a high number of staff with specialised expertise. Finally, running a cyber stress test may require involving competent authorities from

different financial sectors, and possibly, jurisdictions, and ideally competent cybersecurity agencies. Institutional arrangements supporting such cooperation should therefore be explored in advance too.

4.1 Scope

To start with, authorities need to determine a suitable sample of banks, considering the structure of the domestic financial sector. Striking a balance between comprehensiveness and practicality is essential. For instance, authorities can decide to include only (a sample of) systemic banks, or all banks under their supervision – a decision that will matter more in less concentrated banking sectors.

For system-focused exercises, covering essential nodes in the system is crucial, implying that not only banks, but other financial (and possibly non-financial[16]) firms should be included as well. The number of firms included in the test should cover a sufficiently large proportion of the activity/market under study.[17] Authorities may choose to supplement the participating systemic banks and other financial firms with smaller financial companies. This extension also has the benefit of giving authorities the opportunity to study whether firms of different sizes respond differently. In addition, to better capture the propagation of shocks across the financial system, including financial market infrastructures (FMIs) can be especially useful.[18]

In contrast, in a firm-focused exercise, comprehensiveness in the coverage of banks is more relevant. This not only responds to the prudential mandate of the authority in charge but also allows it to benchmark the results across firms. This step could be especially useful to help identify outliers among peers. In turn, benchmarking can alert authorities about shortcomings in either the conduct of the exercise (eg some banks may be over-optimistic in assessing the impact of the initial shock) or in the firm's response capacity (eg the recovery time may be unacceptably long in some banks). The three selected exercises provide examples of how authorities may select to implement these choices (see Table 3).

Sample of firms — Table 3

Authority	Sample
Bank of England	Universal and specialist banks, as well as representatives from insurance and building society sectors, who modelled the scenario as customers of the disrupted services. FMI joined workshop phase.
DFSA	Four banks (Danske Bank, Jyske Bank, Nykredit and Sydbank) and three data centres (JN Data, BEC and Bankdata).
ECB	One hundred and nine banks, ie those under direct ECB supervision at the time the exercise was launched, with a few exclusions for bank-specific reasons such as restructuring or change of significance status. A subsample of 28 banks underwent more extensive testing.

Sources: Bank of England (2025), ECB (2024) and DFSA (2024).

While a prudential authority may find it useful to include a large number of banks in the exercise, additional scrutiny for a subset of banks may be warranted. This would typically be the case for systemically important banks, but authorities could also apply other criteria. For instance, in the ECB exercise, banks in the narrower sample were chosen to cover different business models and geographical locations to reflect the wider euro area banking system and to ensure sufficient coordination with other supervisory activities. In Denmark, even though the exercise was of a prudential nature, by design the sample did not include all

16 For instance, such crucial non-financial firms could be third-party service providers upon which systemic banks rely.

17 Conducting the exercise in tranches, so that participating firms are grouped in different cohorts that start the exercise at staggered times, can also increase the capacity of future tests.

18 Cloud service providers are an increasingly critical component of the provision of services by financial firms. Koh and Prenio (2023) discuss possible approaches to testing their operational resilience.

banks. Rather, some banks, as well as some non-financial firms, were selected because they were considered essential to the financial infrastructure in Denmark.

A related issue concerns whether firms' participation is voluntary or compulsory. The former is more likely when the exercise has a systemic focus. There may be individual supervisory reasons why firms are not invited to an individual test, but the aim is to include all systemically important firms over time and achieve a representative sample for each test or tranche of a test. Among the examples under study, participation in the Bank of England's stress test was voluntary, but the authority has not had any issues in finding willing participants who would be able to provide a system-wide view. Participating firms completed a report, which was reviewed by their own board and was available to supervisors, although the test was not primarily supervisory in nature.

A second dimension of the scope of the exercise is the range of activities under review. While, in principle, every aspect of a firm's business could be included in the stress test, practical considerations such as feasibility and resource constraints require authorities to establish some form of prioritisation. Accordingly, authorities can opt to refine the focus of the exercise in two ways. They might limit it to specific firm exposures, such as those related to particular markets or products, or to a single jurisdiction or currency, particularly if the firm operates globally. This approach allows authorities to assess the combined impacts across the participating firms for the selected activity/market/product. Alternatively, authorities could tailor the scope on the basis of the relevance of the activity to the participating firm, for instance selecting to include only business lines that constitute the core activities of that bank.

In a system-focused exercise, the first option is more appropriate as it enables authorities to assess impacts across firms on a comparable basis (ie exposure to the selected market). This ensures firm results are comparable in cross-firm analysis. In contrast, in firm-focused exercises, prioritising each firm's core business activities is a better fit. A drawback is that, in this case, aggregation across firms and contagion analysis may not be possible.

4.2 Resources and institutional arrangements

Resource constraints are an important dimension affecting the conduct of a cyber stress test, both for the firms and the authorities. Such exercises may stretch over several months.[19] For the authorities, the tests require the involvement of staff from different departments, such as information technology, financial stability, legal and market infrastructure. Importantly, staff involved in the exercise need to have the right level of expertise and when this is not available in-house, authorities may need to rely on external consultants. As a result, there may be advantages of scale for the larger authorities, especially if they can rely on in-house expertise or draw on such expertise from connected authorities.

A similar inter-disciplinary expertise is essential for the firms. The involvement of the business units is essential to ensure rigour and buy-in from the management of the firms. Authorities also expect senior management and board members of the firms, at a minimum, to be made aware of the results, and possibly sign off the stress tests' results, to ensure adequate commitment by the firms. Moreover, they are also expected to discuss possible follow-up actions with the relevant internal or supervisory teams. Such follow-up actions may be more clearly formalised in the case of firm-focused exercises with a supervisory angle but are relevant in all cases.

Separately, the authority in charge of the cyber stress tests needs to consider whether other financial authorities may have to be involved. This is especially important for system-focused exercises, which, by design, can cover different types of firms, and possibly jurisdictions, depending on assumptions made about the nature of the initial shock and the activities in scope of the exercise. The leading authority may therefore need to liaise with the competent prudential authority for other financial firms. In addition,

[19] For instance, the ECB exercise started in January and ended in July, with extensive preparation preceding its launch.

the central bank may be involved in system-focused stress tests, given their financial stability perspective.[20] In this respect, the design of the exercise also needs to clarify whether the central bank joins the exercise only in its capacity as a market participant, or also as a policymaker that can activate an emergency response (eg emergency liquidity assistance in the event of a depositor run following a cyber attack).

Incorporating cross-border elements in a cyber stress test is even more challenging, both because of the absence of common practices across countries and confidentiality constraints. Given such limitations, only more modest approaches may currently be feasible. These could entail considering only coordination policies to inform authorities of possible challenges when responding to a cyber attack affecting several jurisdictions at the same time. Examples of such practices are the cross-border coordination exercises that G7 authorities regularly conduct. These exercises aim to strengthen the G7 authorities' communication and coordination practices in the event of a significant cross-border incident (G7 (2024)).[21] Similar arrangements exist for authorities in the European Union.[22]

Going beyond financial sector authorities, the design of a cyber stress test would benefit from involving the competent cybersecurity agency. This would enhance the realism and improve the design of stress test scenarios.

4.3 Scenario design

The stress test exercise begins with a suspected cyber attack, which is of a higher intensity than in a regular incident management, in line with the typical severe but plausible nature of shocks in any stress test.

In a cyber stress test, the scenario is based on a qualitative narrative describing the disruption. Realism in the assumptions is useful, as it enables firms to adopt their own data to model the impacts. For instance, uncertainty around the cause of disruption can add realism to a scenario and ensure firms consider both malicious and non-malicious causes. However, although technical, the scenario cannot be as detailed or prescriptive as in solvency or liquidity exercises, given the more qualitative nature of a cyber stress test and the individuality of each firm's technology and operational processes.

Disclosure about the scenario in authorities' public reports can also be expected to be considerably more limited, reflecting the risk of exposing firms' vulnerabilities to malicious agents (see Table 4 for a description for the three cases under study).[23]

[20] For instance, this was the case in the second Danish test, which was carried out in collaboration between the DFSA and Danmarks Nationalbank.

[21] As part of the group's efforts to improve cross-border coordination in the event of a cyber attack, the G7 finance ministers and central bank governors adopted non-binding guidance on the structure and key elements of a coordinated collective response to cyber incidents in the financial sector (G7 (2025)).

[22] The Systemic Cyber Incident Coordination Framework (EU-SCICF) was set up to facilitate communication and coordination among EU authorities and to liaise with other key stakeholders at international level, in case of cyber incidents posing a risk to financial stability. See www.eu-scicf.com/.

[23] As shown in Table 4, there is very limited disclosure about the scenario. DFSA (2024) provides slightly more information, which highlights how the scenario was composed of different phases representing a progressive aggravation of the shock. In particular, in the first phase, bank customers saw incorrect amounts being deposited on and withdrawn from their accounts. As the reason was unclear, firms' task at that stage was to identify the cause, to correct the error and to decide how to continue operations and serve customers. In the second phase, a supply chain attack took place, ie a third-party provider of critical IT operations was under attack. According to the guidance by the DFSA, the provider would need about a week to develop a solution that made the systems work again. This meant that key functions at the affected banks were unavailable for at least seven days. Firms were not allowed to assume they could restore the systems themselves. For examples of hypothetical scenarios for a cyber stress test for financial firms, see ESRB (2022).

Narrative of a scenario Table 4

Authority	Sample
Bank of England	The scenario focused on UK markets. Firms were asked to test three variations of the scenario: (i) a suspected cyber attack; (ii) a confirmed cyber attack; and (iii) a longer cyber attack scenario, each affecting the data integrity of transactions settlement. A central scenario is used to model financial impacts, but variations in scenario severity can be tested through (less detailed) variation questions which replace specific scenario assumptions.
DFSA	Specific, extensive, long-term ICT disruption.
ECB	Scenario in which all preventive measures failed and a cyber attack severely affected the databases of each bank's core systems.

Sources: Bank of England (2025), ECB (2024) and DFSA (2024).

A system-focused stress test requires a scenario built around a sector-wide shock. Guidance also needs to restrict firms from assuming they can restore normal operations independently, to reflect the interconnections in the financial system that are at the core of these exercises. As different firms take up different roles in the scenario (eg some are providers of the affected services; others are users of these services), more than one narrative has to be prepared, to represent such different roles. Pre-test engagement with firms reduces the risk that a firm can not apply a scenario to its own business model and systems. In contrast, in firm-focused exercises, the scenario can be less detailed. At the cost of ignoring second-round and contagion effects, a manageable approach is to require firms to assume that their core business is affected by the shock, but the rest of the financial system is unaffected.

Separately, in a system-focused exercise, authorities also have the option of adjusting the degree to which the scenario may be narrow in scope, ie the narrative includes disruptions across more than one market or jurisdiction, or only a single one is covered. A benefit of a narrow scope of the scenario is that its description can be more precise, and firms may find it feasible to quantify the impact. However, such narrow scope is also likely to reduce the overall impact of the shock in comparison with a real-life situation, in which more segments/markets would be affected either directly or via contagion.

To increase the usefulness of the scenario, authorities can employ different strategies. One is to include alternative specifications of an initial disruption. Increasing the intensity of the shock – for instance by extending its duration or disclosing its nature incrementally – across the various specifications can help to identify critical thresholds.[24] Another approach is to vary the agent directly targeted by the cyber incident. In one specification, each firm is asked to consider itself as the direct target; in following rounds, it will be other firms.[25]

When preparing the scenario, either for a firm- or system-focused exercise, authorities may decide to draft an initial version and share it with participating firms for discussion. Feedback from the firms can help ensure that the scenario is relevant to their specific circumstances. In an exploratory test, the use of firm expertise to identify the most impactful aspects of a broad scenario can also help to identify impacts that are not known or anticipated in advance. This collaborative approach can be particularly effective when only a small number of firms are involved. The adoption of such a collaborative approach may also reflect the traditional approach to bank supervision of a given jurisdiction.

[24] Other levers to adjust the severity of the scenario include assumptions about the time given to the firms to respond to the attack; the range and volume of targeted data; and the length of time before the threat is contained.

[25] While increasing the intensity of the stress factor (eg the duration and intensity of the shock, or the number of affected entities) allows for a comparison across such specifications, varying the agents directly hit by the shock makes the comparison harder, as each specification reflects the unique features of the firms that have been hit.

5. Conduct and results of a cyber stress test

The active phase of a cyber stress test begins when firms are given the scenario and activate their response to the initial shock. From that point, authorities start reviewing the quality of the response plans, and how well they can minimise the confidence, operational and financial impacts for the firms, and, if in scope, the financial system. Authorities test firms' ability to manage the shock at various levels, such as the activation of response plans and analysis to identify the services that would be affected and how; communication with external stakeholders,[26] including the management of reputational risk, and implementation of contingency processes and mitigation plans.

Over the length of the exercise, authorities can engage closely and repeatedly with the firms, including to ensure that they correctly understand the scenario and the type of feedback required. The exercise may also be split into separate phases, with firms being requested to submit responses after each phase. Conducting the exercise in phases can also increase its realism. For instance, in the DFSA exercise, the phasing was also used to validate that the scenario worked as intended and that there was a shared understanding of it.

Over time, as authorities and firms gain more experience with cyber stress tests, these exercises could be extended to incorporate live decision-making elements in some portions of the test.[27] This enhancement is especially relevant to test collaboration across firms, which is harder to effectively replicate in a static context.[28]

Due to the qualitative nature of a cyber stress test, firms can provide descriptive feedback through a questionnaire designed by the authorities. The length and level of detail of these questionnaires can vary. When the exercise focuses on individual firms, the questionnaire may be more detailed and possibly longer to support the prudential authority in conducting its assessment. In contrast, for system-focused exercises, open-ended questions are more suitable, as this format maximises the benefit of engaging firms in exploring the impacts of a scenario. It also better accommodates the different types of participating firms (ie not only banks).

Irrespective of the approach, qualitative answers may be better suited to grasp the impact of a cyber attack in terms of operational resilience.[29] In particular, qualitative replies are likely to better reflect the firms' own interpretation and the range of potential impacts. In contrast, financial modelling can only represent a single interpretation of a disruptive impact and may be highly subjective, based on assumptions across a very wide range of variables that could be impacted during a cyber attack that impacts a firm's business.

Authorities can apply some quality controls on the reliability of such qualitative answers via benchmarking among peers, or discussions in dedicated workshops with the firms. Moreover, to support their responses to the questionnaire, firms can be expected to provide documentation to be analysed by the supervisory authority.

Banks considered to be of systemic importance can be subject to additional scrutiny, including requests for additional documentation to support their result, and may be subject to challenge by the

[26] In firm-focused exercises, communication can be limited to informing about the resilience of individual firms. In system-focused exercises, communication also needs to address the resilience of the financial system as a whole. Authorities are therefore likely to be involved in such communications.

[27] Another approach is to link the cyber stress tests through a common scenario to other real-time exercises.

[28] The second test conducted in Denmark involved such live elements, to test how actors impacted by ICT disruption would collaborate in the response and recovery.

[29] The primarily qualitative nature of the questionnaire should not preclude authorities from collecting information on the modelling of financial impact. This information, which is expected to be more limited than in financial stress tests, can help to complement the primary, qualitative feedback from the firms.

authorities. For instance, in the ECB exercise, the 28 banks in the narrow sample were subject to on-site inspections to validate their responses. In the case of the Bank of England, systemic importance is investigated in its tests by focusing on identifying the range and relative importance of factors that determine the extent to which a cyber event may impact financial stability.

Some elements of the response may be presented using metrics of operational continuity, eg information on how and how quickly firms estimate they could restore normal ICT operations (disconnections/reconnections), or on how (and to what extent) firms could maintain critical business functions affected by the cyber incident.[30] Long recovery times or immature and unproven processes will be unsatisfactory to both authorities and firms and may prompt firms to upgrade their response systems.[31] For instance, early findings indicate that, among banks that were part of the ECB cyber stress test in 2024, those that had underinvested in cybersecurity prior to the exercise increased their cyber security investment afterwards by significantly more than the others (Abidi et al (2026)).

Authorities can also study the distribution of the results across banks to identify relevant patterns. For instance, authorities can request each bank to provide information on the most affected business lines (eg lending, deposit taking and wholesale funding).[32] This could shed light on links between vulnerabilities that emerged during the stress test and other characteristics of the banks, such as their business model or concentration of exposures to specific service providers. In this respect, findings in the literature show that certain characteristics can expose banks to cyber attacks, such as their size, their exposure to geopolitical tension, the quality of internal governance or the strength of cyber-related legislation in the jurisdictions in which they operate (IMF (2024)).

When the exercise includes a system-wide assessment of the impact, combining firm-specific results is essential. Authorities can achieve this by requiring participating firms to not only provide data but also attend workshops with the authority and other firms to discuss their responses.[33] Through these arrangements, firms and authorities can jointly analyse the operational, financial and confidence-related impacts. Authorities may also review firms' responses alongside materials such as plans for business continuity, ICT recovery and communication, to identify key learning points and best practices for individual organisations and across all participants. Although these processes are not designed to yield a single aggregate figure to estimate the overall impact, they can nonetheless provide valuable insights into the system-wide severity of the cyber incident.

Finally, system-focused stress tests could include contagion and second-round effects – this can help to assess the efficacy of the combined first-round response by the participating firms. However, as in traditional solvency and liquidity stress tests, this extension of the analysis is complex, and it may be even

[30] For a discussion of critical business functions, see BCBS (2021).

[31] In particular, firms will be concerned about both recovery point objective (RPO) and recovery time objective (RTO), and the stress test can help to shed light on shortcomings of both. Ideally, authorities would need to be able to challenge firms' results that may present a tendency towards meeting RTOs and RPOs by default as well as staying within business continuity objectives.

[32] Following this step, authorities could attempt a quantification of the economic impact by calculating losses attached to the most relevant business lines. This computation, which goes beyond the operational resilience focus of a cyber stress test, is not straightforward. One of the challenges in this step is that attempts to measure the quantitative impact produce only modest losses following a cyber attack (IMF (2024)). Modelling such events is also complex, as cyber attacks are relatively rare and their impact may not always be disclosed. Moreover, an appropriate assessment of the economic consequences would have to include both direct and indirect impacts, with the latter being particularly difficult to estimate.

[33] Preserving the confidentiality of such discussions is essential, and firms may be required to sign non-disclosure agreements in advance.

more so in a cyber stress test, given the lack of well established practices and the exercise's qualitative nature, but some attempts have already been outlined in the literature.[34]

6. Follow-up and disclosure

Following the completion of the exercise, authorities may provide participating firms with individual reports about their performance during the exercise and possible areas for improvements. These firm-specific reports are confidential to preserve the integrity of the firm.

In addition to receiving individual reports, firms may be expected to undertake some remedial action, even if the stress tests do not conclude with a pass or fail outcome. In firm-focused exercises, because of the emphasis put on firm-specific preparedness, supervisors may continue engaging with the firm in their regular supervisory activities. For instance, in the ECB case, the outcome was expected to feed into the Supervisory Review and Evaluation Process (SREP) of the same year, but it would not imply changes in capital requirements or supervisory scoring. In contrast, the DFSA exercise, even if led by the supervisory authority, did not result in any direct supervisory actions, as the DFSA prioritised the learning aspect of the stress test.

In system-focused exercises, the follow-up with participating firms may focus on ensuring that all firms and financial market infrastructures consider the findings from the stress test alongside findings from their own operational resilience testing and lessons from real incidents. For instance, the Bank of England expected all firms to consider the implications of these findings for their own businesses, reflect on how planning and preparation for potential financial stability scenarios could be improved, and integrate those lessons into a continuous improvement cycle. As the exercise was not designed as part of a supervisory cycle, there was no expectation that those enhancements would be directly assessed afterwards by the prudential authority. However, these materials could be used by firms and supervisors as a reference in their ongoing operational resilience work. Overall, in its various cyber stress tests, the Bank of England tends to prioritise follow-up in the form of sector-led initiatives, which are designed to improve systemic resilience, inform ongoing sector initiatives or reduce the risk to financial stability.[35]

Going beyond reporting to participating firms, disclosure around cyber stress tests can be expected to be very limited, especially in firm-focused exercises.[36] This reflects the sensitive nature of both the information collected for the analysis and of the results. While concerns of triggering a self-fulfilling crisis also arise in the context of liquidity stress tests, the risk of malicious attacks in relation to cyber risk further increase the need for caution.

[34] For instance, Kotidis and Shreft (2022) simulate a cyber attack to quantify its impact. They study how the initial shock reduces some firms' ability to process payments (first-round effect), causing other banks to receive fewer payments (second-round effect), leaving them at risk of having too few reserves to send their own payments (a potential third-round effect). Eisenbach at al (2021) model contagion effects of a cyber attack on the five largest US banks, to quantify spillover on other banks. Among the selected exercises, the Bank of England (2025) describes the channels through which the initial shock could propagate across the financial system and lead to financial instability.

[35] For instance, this follow-up could take the form of guidance on planning for disconnection and reconnection to FMI systems.

[36] In some cases, disclosure may be the result of a transparency requirement imposed by legislation on the authority leading the exercise, even if only high-level information on the findings is required. For instance, EU law requires the ECB to carry out stress tests on supervised banks at least once per year. The ECB publishes the outcomes of these tests to enhance transparency and market discipline, integrating them into the SREP. When conducting thematic stress tests, such as the one conducted in 2024 for cyber risk, the ECB may communicate only aggregate findings and a conclusion. In the 2024 thematic stress test, the ECB limited its disclosure over the outcome by stating that banks had response and recovery frameworks in place, but areas for improvement remained. The ECB also mentioned that the stress test had helped increase banks' awareness of the strengths and weaknesses of their cyber resilience frameworks.

Nonetheless, some public disclosure can be beneficial. Sharing key takeaways from the stress test can be useful to firms that did not participate in the exercise – as well as firms in other critical sectors – enabling them to evaluate and enhance their cyber contingency planning. resources from the stress test can be developed into a toolkit for firms to conduct their tabletop exercises It also signals authorities' interest in cyber resilience, and reinforces the message to board members of financial firms that preparation is important and expected by the authorities.

To emphasise these points, and to remind firms and the general public of the complexity and importance of addressing cyber risk, authorities could publish general lessons from the stress tests. This solution applies to both firm- and system-focused exercises. For instance, the DFSA published five key lessons on cyber risk that are relevant to any firm, irrespective of whether it joined the cyber stress test. These cover the importance of making conservative assumptions about the time required to restore normal operations; the critical role of ex ante preparation; the need to recognise that the impact of the initial shock builds-up over time, making it essential to include a sufficiently long time horizon in the exercise to fully capture its effects; the crucial role of communication, both internally and with external parties such as customers and counterparts, and the importance of internal coordination among different business areas, as well as between them and IT departments, to enable an effective response.

For system-focused exercises, public disclosure can help firms to better identify and address the externalities that weak cyber responses by individual firms can impose on the system as a whole. In particular, the test gives firms an opportunity to better understand the authorities' expectations regarding the need to consider financial instability during operational resilience planning and preparations, and consider how to preserve financial stability when responding to a cyber incident. For instance, the Bank of England highlights the importance of internalising the system-wide impact in firms' responses, and the need to prioritise actions that preserve financial stability (Bank of England (2025)). To guide firms' understanding of the authorities' preferences, it developed its impact tolerance for critical payments, based in part on the findings of its 2022 cyber stress test (Bank of England (2023a)).[37]

Separately, depending on existing prudential practices in a given jurisdiction, authorities may draw on their findings from a cyber stress test to developed a toolkit for financial firms to conduct their own tabletop exercises.

Finally, as it is likely that the quality of firms' responses will improve across vintages, authorities may wish to repeat cyber stress tests. Different vintages need not be the same, thus preserving the novelty factor for repeat participants. Authorities themselves are also likely to enhance their own preparedness for conducting such tests and refine their approach over time. In this way, they can make the exercise more valuable and, consequently, more appealing to firms. This matters even more when participation is voluntary and authorities need to maintain the industry's buy-in. In addition, either repeating the tests, or conducting them in tranches increases their capacity, giving more firms an opportunity to join them.

7. Concluding reflections

While still in its early stages, cyber risk stress testing has emerged as a useful tool for authorities and financial firms to enhance operational resilience in the face of increasingly frequent and sophisticated cyber attacks, in combination with other tools at authorities' disposal to monitor and enhance operational

[37] For instance, authorities may encourage firms to select workarounds or replacement of services that prioritise completing transactions that are critical for financial stability, even if this implies not serving customers in a chronological order. The Bank of England (2025) highlighted how the Financial Conduct Authority's statement on treating customers fairly was a direct response to a perceived barrier to acting with financial stability in mind.

resilience. Moreover, dedicated stress tests can be employed to address a range of shocks to operational resilience, beyond cyber incidents or cyber attacks.

There is as yet no established template for authorities to design and conduct these exercises, but it is already possible to define two distinctive approaches, ie focusing either on the impact at the individual firm level or on the broader repercussions across the (domestic) financial sector. Both approaches have merit and come with unique challenges. Crucially, when planning a cyber stress test, authorities should choose the approach that best aligns with their objectives and design the key features accordingly. This ensures internal consistency across the building blocks of the exercise, which is essential to deliver useful lessons for firms and authorities.

Continued enhancements and disclosure of the methodological aspects in cyber stress tests can help raise awareness and establish best practices. These may also help increase investment in cyber resilience across firms, reducing the risk that the "weakest link" endangers the stability of the whole financial system. Repeating cyber stress tests over time, rather than treating them as a one-off, can not only enhance firms' responses but also strengthen authorities' capabilities to design and execute these exercises. Iterative testing can provide valuable insights into evolving risks and ensure that stress tests remain relevant and effective, including by meeting new regulatory priorities and adapting their scope by exploring new areas of potential vulnerability.

Part of firms' responses to a cyber incident is effective communications to internal and external stakeholders, including with the aim of managing reputational risk. In the event of a system-wide shock, firms' communications will need to be supplemented by the authorities to provide an assessment of the resilience of the system as a whole. Although cyber stress tests conducted so far may emphasise communications plans by the firms, a complete test would need to include complementary plans by the authorities.[38]

Looking ahead, practical considerations, mostly related to confidentiality constraints, may make further developments challenging. Yet while authorities may continue to develop their existing approaches, there are several areas for further development in cyber stress testing. For instance, future tests could incorporate cross-border and wider cross-sectoral disruptions, to better reflect the interconnected nature of the financial system. Broad participation, including non-bank financial institutions and critical third-party providers, is beneficial, to ensure a comprehensive view of systemic vulnerabilities. Firm-focused exercises may also benefit from the introduction of some systemic elements in their design, given the high risk of transmission of cyber shocks across the financial system.

References

Abidi, N, L Gambacorta, C Kok, L Madio, I Miquel-Flores and A Partida (2026): "Disciplining digital risk: evidence from cyber stress tests", *ECB Working Paper Series*, forthcoming.

Ahnert, T, M Brolley, D Cimon and R Riordan (2022): "Cyber risk and security investment", *Staff Working Paper,* no 32, Bank of Canada, July.

Anand, K, C Duley and P Gai (2022): "Cybersecurity and financial stability", *Deutsche Bundesbank Discussion Paper,* no 8, March.

Banco de Portugal (2024): "Cyber resilience test: the instrument and experience of the Banco de Portugal", Box 4, *Financial Stability Report*, November.

[38] There are several examples of such coordinating arrangements. For instance, in the United Kingdom, the Authorities' Response Framework (Bank of England (2024c)), which connects the Bank of England, including the Prudential Regulation Authority, with the Financial Conduct Authority and His Majesty's Treasury. In the European Union, there is the EU-SCICF, as already mentioned.

Bank of England (2023a): *Financial policy summary record of the Financial Policy Committee meeting on 23 March 2023*, March.

——— (2023b): *Thematic findings from the 2022 cyber stress test*, March.

——— (2024a): *Financial stability in focus: the FPC's macroprudential approach to operational resilience*, March.

——— (2024b): *CBEST threat intelligence-led assessments: implementation guide for CBEST participants*.

——— (2024c): *Co-ordinating the response to disruption of financial services*, April.

——— (2025): *Thematic findings from the 2024 cyber stress test*, July.

Basel Committee on Banking Supervision (BCBS) (2018): *Cyber-resilience: range of practices*, December.

——— (2021): *Principles for operational resilience,* March.

Committee on Payments and Market Infrastructures (CPMI) (2025): *CPMI work programme and strategic priorities for 2025-27*.

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

——— (2022): *Implementation monitoring of the PFMI: level 3 assessment on financial market infrastructures' cyber resilience: level 3 assessment on financial market infrastructures' cyber resilience*, November.

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

Danish Financial Supervisory Authority (DFSA) (2024): *Cyber stress testing*.

Duffie, D and J Younger (2019): "Cyber runs", *Hutchins Center Working Paper,* no 51, Brookings Institution, June.

Eisenbach, T, A Kovner and M J Lee (2021): "Cyber risk and the US financial system: a pre-mortem analysis", *Staff Report,* no 909, Federal Reserve Bank of New York.

European Central Bank (ECB) (2023): *ECB banking supervision: SSM supervisory priorities for 2024–2026*.

——— (2024): *ECB concludes cyber resilience stress test*, press release, 26 July.

——— (2025): *TIBER-EU framework: how to implement the European framework for threat intelligence-based ethical red teaming*, January.

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

——— (2022): *Mitigating systemic cyber risk*, January.

——— (2023): *Advancing macroprudential tools for cyber resilience*, February.

——— (2024): *Advancing macroprudential tools for cyber resilience – operational policy tools: a review of national and pan-European frameworks*, April.

European Union Agency for Cybersecurity (ENISA) (2025): *Handbook for cyber stress tests*, May.

Financial Stability Board (FSB) (2023): *Cyber lexicon – updated in 2023*, April.

——— (2025a): *Format for incident reporting exchange (FIRE) – final report,* May.

——— (2025b): *Peer review of Spain*, November.

——— (2025c): *Peer review of the Netherlands*, November.

Gaidosch, T, E Islam, T, Khiaonarong, R Ravikumar and C Wilson (2026) "Good practices in cyber risk regulation and supervision", *IMF Departmental Paper*, no. 01, International Monetary Fund.

Group of Seven (G7) (2020): *G-7 fundamental elements of cyber exercise programmes*, December.

——— (2024): *G7 Cyber Expert Group conducts cross-border coordination exercise in the financial sector*.

——— (2025): *G7 fundamental elements of collective cyber incident response and recovery in the financial sector*, September.

International Association of Insurance Supervisors (IAIS) (2023a): *Global insurance market report (GIMAR) – special topic edition: cyber*, April.

——— (2023b): *Issues paper on insurance sector operational resilience*, May.

International Monetary Fund (IMF) (2024): "Cyber risk: a growing concern for macrofinancial stability", *Global Financial Stability Report*, Chapter 3, April.

——— (2025a): "Euro area: publication of financial sector assessment program documentation – technical note on cyber risk and financial stability – selected issues in regulation and supervision", *IMF Country Report*, no 213, July.

——— (2025b): "Norway: 2025 Article IV consultation – press release and staff report", *IMF Country Reports*, no 248, August.

Khiaonarong, T, K Korpinen and E Islam (2025): "Using simulations for cyber stress testing exercises", *IMF Working Paper,* no 85, International Monetary Fund.

Khiaonarong, T and Z Shanyuan (2026) "*The rise of cyber events and digital fraud in the financial sector", IMF Working Paper*, no 62, International Monetary Fund.

Koh, T Y and J Prenio (2023): "Managing cloud risk – some considerations for the oversight of critical cloud service providers in the financial sector", *FSI Insights on policy implementation,* no 53, November.

Kotidis, A and S Schreft (2022): "Cyberattacks and financial stability: evidence from a natural experiment", *Finance and Economics Discussion Series*, no 25, Federal Reserve Board.

Poljšak, B and M Bračković (2025): "Cyber stress tests 2024", *Short Economic and Financial Analyses*, Bank of Slovenia, January.

Prenio, J and F Restoy (2022): "Safeguarding operational resilience: the macroprudential perspective", *FSI Briefs,* no 17, August.

Prenio, J, J Yong and R Kleijmeer (2019): Varying shades of red: how red team testing frameworks can enhance the cyber resilience of financial institutions*, FSI Insights on policy implementation*, no 21, November.

Reserve Bank of Australia (2024): *Assessment of the Reserve Bank information and transfer system*, June.

Vermeulen, R, M Sydow, C Brousse, F Cascao, J Fique, C Marques, J Nyholm and F Virel (2025): "Cyber resilience stress testing from a macroprudential perspective", *Macroprudential Bulletin 27*, European Central Bank, March.