Bank of England

Duncan Mackinnon
Executive Director
Supervisory Risk Specialists

Nathanaël Benjamin
Executive Director
Financial Stability Strategy & Risk

9 July 2025

Dear SMF 24 or equivalent,

Thematic findings from the 2024 Cyber Stress Test

Operational resilience stress testing is a key part of the Financial Policy Committee's (FPC's) medium term priorities[1] and we are writing to share the findings of the Bank of England's 2024 Cyber Stress Test (CST24) with you.

CST24 was a voluntary, exploratory test which asked providers and users of wholesale services to model the impact of a suspected cyber attack affecting transaction settlement. Participants provided data and attended workshops to discuss how they would respond. Together, we analysed the operational, financial, and confidence impacts.[2] The findings are relevant to both participant and non-participant firms ('firms') and financial market infrastructure firms ('FMIs') across a range of scenarios and can be used to:

- improve individual firm and sector response and recovery capabilities;

[1] The Financial Policy Committee's medium-term priorities (2023–2026) | Bank of England
[2] Financial Stability in Focus: The FPC's macroprudential approach to operational resilience | Bank of England

- mature firms' understanding of the potential impacts to financial stability from operational disruption; and
- inform firms' impact tolerances for financial stability where appropriate.

We are sharing test materials in the annexes of this letter to support firms to plan for and mitigate potential financial stability impacts.

We would like to thank participant firms for their open and constructive engagement and acknowledge the progress they have already made in further understanding the impacts of operational disruption to their services. We also welcome the industry collaboration already in progress to implement the test findings, including embedding new understanding into firm Impact Tolerances and firm and sector playbooks.

Scenario

We asked participants 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. Participants included universal and specialist banks, as well as representatives from insurance and building society sectors, who modelled the scenario as customers ('customer firms') of the disrupted services. The scenario focused on UK markets, but we note that in a real incident, the impact to operations and financial markets may be broader.

Key findings

Financial Stability Decisions

It is important for systemic firms[3] to consider the FPC's tolerance for disruption to payments and settlement, and how the decisions they make in response to operational disruption may affect financial stability.

The test found that participants had mature scenario modelling, and response and recovery capabilities. However, most participants did not have a mature understanding of the FPC's Impact Tolerance or how the potential impacts could, in some scenarios, create financial instability. Further consideration therefore needs to be given to the actions firms might take to protect financial stability and to manage the systemic risk from operational disruption scenarios.

FPC's payments Impact Tolerance states that firms should be able to complete payments by the end of their intended value date, and in circumstances where that may not be possible or desirable, firms should plan, prepare and test for such situations,

[3] PRA and Bank's Operational Resilience policies require "Other Systemically Important Institutions (OSIIs)" and "relevant Solvency II firms" to consider financial stability.

and invest so that their response can effectively mitigate any impact on financial stability until service delivery is restored.[4]

Deciding on the most appropriate response will always be judgement-based. Each scenario will be different and while it is not possible to rehearse every decision, firms may need to consider their appetite for response and recovery strategies in a range of scenarios, as well as their role as systemic risk managers and the actions they can take to mitigate impacts on financial stability.

The materials in Annex 1: 'Financial stability impact planning tools', may provide a structure for firm or cross-firm planning and preparation for financial stability impacts and can be adapted and applied to a range of services and scenarios.

Financial Stability Mitigation

The test explored how participants could mitigate the operational, confidence, and financial impacts of the scenarios, on UK financial stability.

Operational mitigation

The ability to process high-impact transactions using workarounds can help to maintain financial stability by enabling key markets to continue to function. In the test scenario, some participants chose not to process any transactions during the disruption because it would make reconciliation more difficult, which may delay the resumption of business services; or because they saw Financial Conduct Authority (FCA) rules on Treating Customers Fairly (TCF) as a barrier to prioritising some customers above others.

The FCA has confirmed its view that '*a failure to maintain market integrity or financial stability can have a significant impact on customers. Where that is the case, firms should consider prioritising payments that minimise the impact on market integrity and/or financial stability. Doing so is unlikely to breach TCF requirements. On the contrary, rigidly processing payments in the order they were submitted – without consideration of the wider impact on customers – is more likely to breach TCF requirements.*

Firms may therefore wish to consider whether they have the data and processes in place to identify and prioritise transactions where this could play an important role in maintaining financial stability.

Some participants had not tested all available workarounds for processing payments; it is important for firms to work with their Financial Market Infrastructures (FMIs) or central counterparties to ensure ongoing awareness of available mitigation options and ensure that new options are adopted, tested and factored into system upgrades as new technology becomes available.

[4] Financial Policy Summary and Record - March 2023 | Bank of England.

Complex and bespoke services mean that wholesale payments may not be substitutable or portable, however it is important for counterparties and customer firms to understand the impacts of infrastructure being disrupted and explore mitigations if their service provider is unavailable for an extended period.

Confidence mitigation

Sector coordination and communication is a critical component of good response and recovery. Clear and timely communications mitigate financial stability impacts by maintaining confidence that any disruption is being managed effectively. The sector has well-established fora for sector coordination and all participants demonstrated good understanding and awareness of the Sector Response Framework (SRF) processes.

In the test, participants identified that customer relationship managers or other incident 'first responders' may not be familiar with the SRF or with their firm's own operational resilience contingency procedures, and further work to improve awareness of these playbooks would be beneficial to ensure clear and accurate communication to customer firms. [5]

Financial mitigation

While capital is a highly fungible mitigant to losses, it does not mitigate the impacts of operational disruption. Ensuring firms have liquidity to transact is a key mitigant to impacts from failed settlement. While transactions would still be executed in the market, in the test scenarios, customer firms with transactions that did not settle on the anticipated date would then not have the liquidity they expected. Where customer firms needed liquidity to fund other activity, disruption could impact other markets or services (including through asset 'fire sales').

In the test scenarios, service providers were able to provide credit, however this would have limits and providers did not have sufficient understanding of their customer firms' funding position or expected demand for liquidity to confirm that they would be able to meet these needs in a longer duration incident. Firms would therefore benefit from considering their ability to understand customer firms' demand for liquidity and their own appetite to provide it, including how this appetite may change over time.

In a longer duration incident, the point at which market participants no longer wanted to execute trades because of concerns about the ability to settle those transactions (or resolve the backlog of unsettled trades) or began to withdraw from participation in the market, would represent market dysfunction and risk financial instability. The potential for a loss of confidence could also significantly amplify the scenario impacts.

[5] The Sector Response Framework (SRF) is a series of Sector Response Groups, FMI Crisis Committees, and supporting contingencies that enable parts of the sector to respond collectively to a systemic incident. **Sector Response Framework (SRF) Summary**.

Annex 2: ‘Financial instability mitigation and related barriers’, provides some examples of mitigations across financial operational, and confidence impacts, the role of those mitigations, and potential barriers to effective mitigation.

Annex 3: ‘Scenario severity amplifiers’, includes a list of factors which firms can use to plan or vary a scenario to ensure it is sufficiently severe to challenge existing planning and preparation assumptions and therefore provides useful outcomes which will improve operational resilience of the processes being tested.

Disconnection

Firms’ decisions about disconnecting from critical systems and infrastructures would determine their ability to mitigate financial stability impacts since disconnection would mean no further transactions could be processed.

It is important for firms to ensure their disconnection (and reconnection) options are understood across business functions, are aligned to their risk appetites, and that playbooks reflect the potential financial stability impacts of a loss of key connections.

Firms connect to services provided by FMIs to facilitate the provision of vital services to the economy. Firms often have several different connections with FMIs which are used for different financial products or types of business.

When a firm is affected by a malicious cyber attack they and other firms will decide to either remain connected (to continue business) or to disconnect (to prevent contagion of the cyber risk). There are many different types and levels of disconnection e.g. physical disconnection, inbound/outbound disconnection, pausing data etc. To ensure effective planning, it is important that firms ensure their technology and business leads have discussed their response strategies together, and with their customer firms.

If firms choose to disconnect, it can protect the wider sector from the attack, but it can also prevent them from mitigating the impacts of disruption e.g. where workarounds will not work if firms disconnect.

It is important for firms to explore whether a reduced or contingency level of connection could be maintained when needed, which would reduce the risk of contagion and facilitate mitigation options (E.g. manual processing). Firms can then use this understanding to make risk-based decisions on disconnection and reconnection.

It is important for FMIs to work with the sector to ensure their members understand the complexity and implications of disconnection and reconnection and can make informed, risk-based decisions which reflect the financial stability implications of these impacts.

We welcome the cross-sector work to improve firms’ understanding of their connections to FMIs and the disconnection options available to firms in relation to the test scenario. We would encourage other FMIs to work with their members and network service providers to ensure that the connection options and processes for disconnection and

reconnection are understood by their members and embedded in their planning for operational disruptions.

Reconnection

In the event of a cyber attack, firms may disconnect from financial infrastructure and from each other. Participants acknowledged that the time needed to obtain third-party assurance that it is safe to reconnect might exceed their own Impact Tolerances and the FPC's Impact Tolerance for disruption to payments and settlements.

It is therefore important that firm reconnection options are understood and are aligned to their risk appetites, and that playbooks reflect the potential financial stability impacts of a loss of key connections.

The work at the Cross Market Operational Resilience Group (CMORG) to define best practice reconnection processes, including informing firm-level reconnection decisions will be an important resource on this topic.[6]

Next Steps

It is important for all firms and FMIs to consider the findings from CST24 alongside findings from their own operational resilience testing, sector exercising, and lessons from real incidents. We acknowledge the commitment of test participants who have already started to work on the themes set out in this letter and we expect all firms to consider the implications of these findings for their own businesses, reflect on how planning and preparation for potential financial stability scenarios can be improved, and integrate those lessons into a cycle of continuous improvement.

Participant confidentiality may now be relaxed and firms that wish to do so are encouraged to share their experience of the test with their customers, sector groups and home state regulators, with a view to maximising the benefits of the test findings and continuing to improve the depth and maturity of operational resilience planning at firm and sector levels.

Yours sincerely,

Duncan Mackinnon
Executive Director
Supervisory Risk Specialists

Nathanaël Benjamin
Executive Director
Financial Stability Strategy & Risk

[6] **Welcome to CMORG | Cross Market Operational Resilience Group**

Annex 1 – Financial Stability impact planning tools

Table 1a provides illustrative examples of observable impacts that could lead to financial instability, using the impact categories outlined in the Bank's **Financial Stability in Focus**. This can help to facilitate discussion of financial stability between subject matter experts from a range of disciplines and across technology and business areas.

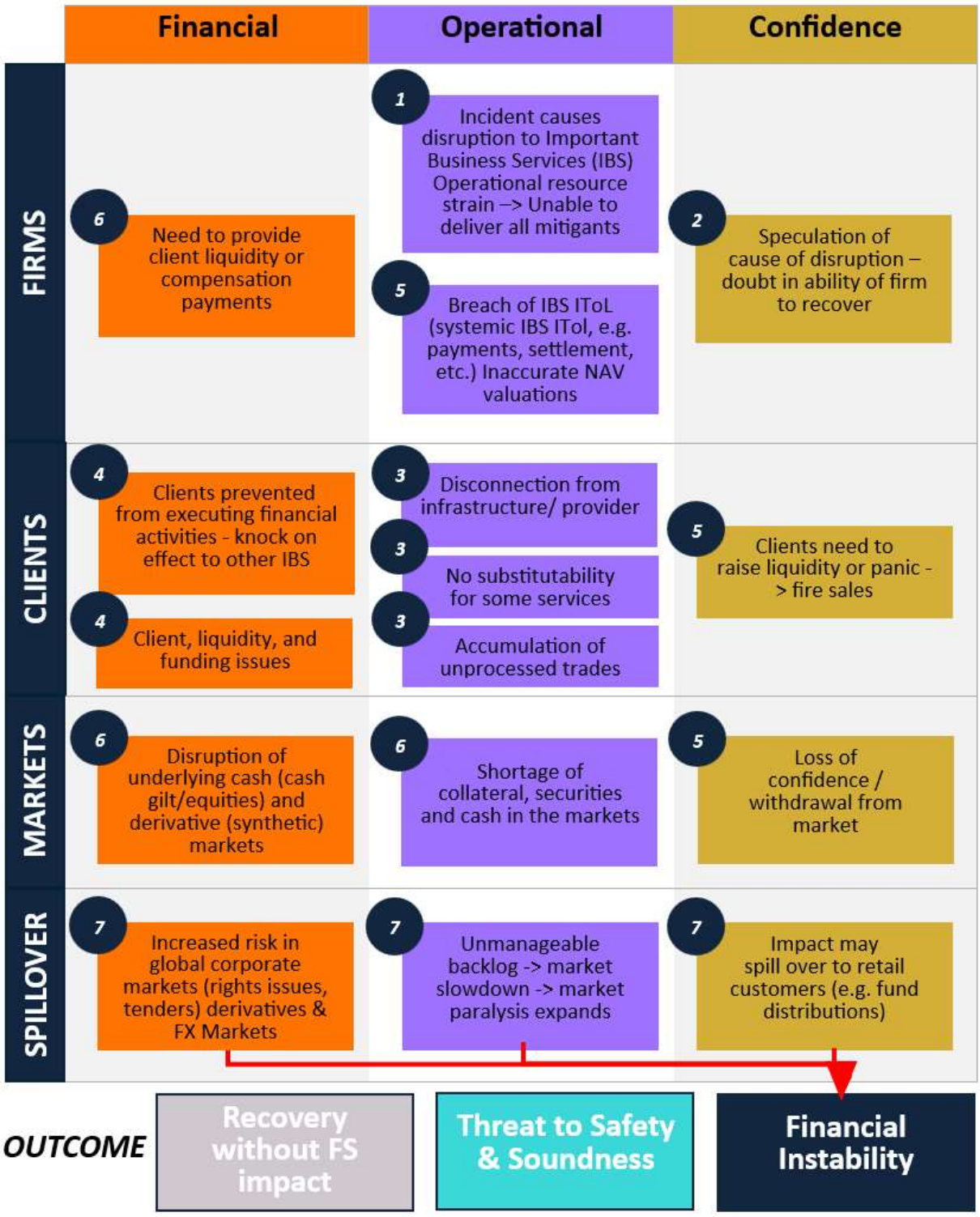
Table 1a: Examples of observable impacts that could lead to financial instability

	Impact to	Indicator of FS impact	Illustrative examples of observable indicators
Financial	Solvency & capital	Pricing	• Widening of bid-ask spreads to access liquidity or credit • Solvency Pricing Funding costs, market driven margin calls
		Volumes	• Movements outside market norms
		Metrics	• Movements in regulatory indicators e.g. CET1, LCR, NSFR[7]
Operational	Firm service delivery	Service disruption	• Firm or their counterparties unable to provide services (x duration) • Disconnection
	Central infrastructure	FMI, third party, supplier with low substitutability	• Disruption of infrastructure facilitating market operation with no or low substitutability in short term, with network or concentration impacts
Confidence	Behaviour	Demand for security	• Discretionary margin calls, change to collateral eligibility • Demand for security criteria, hoarding liquidity
		Participation in markets	• Voluntary withdrawal from market(s) • Expectation of disconnection
	Expectations	Ability to recover, sentiment	• Increased certainty that disruption was caused by a cyber-attack • Expectation that firm will be subject to a run on deposits, • Increased visibility of disruption • Impacts to retail customers

[7] Common Equity Tier 1 (CET1) is part of a bank's core capital structure, used to fund business activities. Liquidity Coverage Ratio (LCR) is the amount of liquid assets a bank must have available so that it can meet short-term obligations. Net Stable Funding Ratio (NSFR) is the amount of funding banks are required to maintain to reduce the likelihood that disruptions to regular sources of funding will erode its liquidity position and increase the risk of failure or broader systemic stress.

Table 1b is an example of how a firm may use the impacts identified in table 1a to define a 'route to financial instability'. This can be used to explore impacts and facilitate discussion on the knock-on implications from disruptions.[8]

Table 1b: Route to financial instability



[8] The numbers in the circles in Table 1b show the sequence of the impacts we might expect to see in the scenario.

Firms can use tables 1a and 1b to facilitate discussion of the impacts of an operational disruption and to think about how they would manifest in a scenario. For example, identifying the impacts at each level and determining how the original event (1) could develop (2-7) to result in financial instability. Combining knowledge and understanding from different perspectives (business and technical areas) helps build a more holistic understanding of how services are delivered, facilitates constructive challenge to planning assumptions, and may identify gaps in understanding.

Annex 2– Financial instability mitigation and related barriers

Table 2 provides illustrative examples of mitigations firms can action, how those mitigations might reduce financial stability impacts, and some potential barriers for each. The examples will not be relevant for every scenario, but firms will be able to add their own examples. Where mitigations have been included in testing and exercising, firms and their customer firms can have greater confidence they will be effective during a disruption.

Table 2: Illustrative examples of mitigations, the roles, and barriers

	Role in reducing financial stability impacts	Barrier (examples)
Mitigation		
Manual processing	Ability to continue delivering services, potentially at reduced volumes	• Disconnection • Contingency processes not integrated with firm technology • Untested processes
Prioritised processing (or semi-automated)	Ability to process transactions that may be relatively more important for financial stability	• Client communications process • Granular data
Communication and coordination	Ability to avoid unpredictable behaviour by managing stakeholder expectations and maintaining confidence	• Granular data • Alignment across firm boundaries • Disinformation
Provision of liquidity for clients	Ability to reduce dependency on settlement of trapped' instruments by providing alternative sources of liquidity or credit	• Firm liquidity resources • Appetite for extending credit • Tested processes or trained staff for delivering mitigation
Managing build-up of transactions	Ability to reduce the build-up of transactions that subsequently need to be reconciled and processed	• Client appetite • Uncertainty over effectiveness or ability to reconcile data
Managing certainty over transactional integrity	Ability to provide clarity and certainty through a managed pause in processing	• Flexibility in playbook strategy • Ability to determine point at which pause in service delivery becomes threat to financial stability
Back up data (quality and availability)	Ability to maximise the speed and certainty that transactional integrity can be restored	• Lack of confidence in tested processes or trained staff to deliver mitigation
Portability	Ability to process new transactions on an alternate platform	• High cost of setting up redundant systems • Sharing back up arrangements may require cooperation across firm or divisional boundaries
Substitution	Ability to provide an alternative means of delivering services through alternative processes	

Annex 3 – Scenario severity amplifiers

Table 3 identifies a range of amplifiers, which can be used to design a scenario (and to make it more, or less severe), or to create variations which challenge firms' response and recovery plans. Scenario variations can be a useful to explore how responses change as assumptions change, without the need to re-run a complete test.

Table 3: Severity amplifiers which can be used in scenario design

Amplifier	Impact on scenario severity (not intended to be comprehensive)
Duration	• The longer the period of disruption, the more likely it is for this to cause impacts which could result in financial instability • Depending on the trading cycle of the disrupted service, there may be a period beyond which mitigation becomes less feasible or effective
Timing	• For some processes the time of day may be critical in making a response difficult to respond to e.g. proximity to market close or processing windows
Scale	• The larger the number and range of data sets, firms or FMIs affected by the disruption, the more complex the response and recovery can be expected to be. Uncertainty as to the scale may also add complexity • It may be necessary to assume failure of some controls (e.g. availability of first back up) to ensure a test provides valuable results
Stakeholders	• The number, variety and visibility to retail customers are all likely to be factors that could increase the demands of staff communicating and coordinating the firm and sector response • Impacts on retail customers are likely to attach a higher level of media interest and scrutiny of the incident response (e.g. IPO) • A specific client segment with a majority concentration with a single custodian being adversely impacted
Nature	• The cause of the disruption may change stakeholders' reaction to it. A confirmed cyber-attack could increase the probability that some services would be disconnected from other firms (or FMI's) making reconnection of services a more complex and lengthy process • A data integrity incident is likely to also affect the availability of a service and imply an added degree of complexity in resuming services
News	• Even unrelated events may change stakeholder perception or reaction to a service disruption and make a response more complex
Market	• Market volatility or trading volumes could lead to market asset shortages, price dislocation and potentially market dysfunction which could affect a firm's planned response and the effectiveness of its mitigation actions
Media	• The media framing of the incident may play a significant role in public response to the disruption and the accuracy and reliability of key messages could enhance or hinder an incident response
Poor mitigation	• A failed or partially ineffective attempt at incident response or impact mitigation may reduce confidence in the affected firm's future ability to effectively respond and recover from a disruption