Bank of England

Financial Stability in Focus: The FPC's macroprudential approach to operational resilience

Financial Policy Committee
March 2024

Financial Stability in Focus

March 2024

The primary responsibility of the Financial Policy Committee (FPC), a committee of the Bank of England, is to contribute to the Bank of England's financial stability objective. It does this primarily by identifying, monitoring and taking action to remove or reduce systemic risks, with a view to protecting and enhancing the resilience of the UK financial system. Subject to that, it supports the economic policy of His Majesty's Government, including its objectives for growth and employment.

The Financial Stability in Focus sets out the FPC's view on specific topics related to financial stability. It complements the Financial Stability Report, which is published twice a year, and sets out the FPC's overall view of the outlook for UK financial stability, including its assessment of the resilience of the UK financial system and the main risks to UK financial stability, and the action it is taking to remove or reduce those risks.

The Financial Policy Committee:

Andrew Bailey, Governor
Sarah Breeden, Deputy Governor responsible for financial stability
Ben Broadbent, Deputy Governor responsible for monetary policy
Dave Ramsden, Deputy Governor responsible for markets and banking
Sam Woods, Deputy Governor responsible for prudential regulation
Nikhil Rathi, Chief Executive of the Financial Conduct Authority
Nathanaël Benjamin, Executive Director for Financial Stability Strategy and Risk
Colette Bowe
Jon Hall
Randall Kroszner
Carolyn Wilkins
Gwyneth Nurse attends as the Treasury member in a non-voting capacity.

The report was finalised on 22 March 2024. This document, unless otherwise stated, uses data available as at 12 March 2024.

For the avoidance of doubt, the Financial Stability in Focus is not intended to satisfy the requirements of Section 9W of the Bank of England Act 1998.

Contents

Executive summary

Operational resilience is the ability of individual financial firms, financial market infrastructures (FMIs) and the wider financial system to prevent, adapt and respond to, as well as recover and learn from, operational disruptions. Operational disruptions result from inadequate or failed internal processes, people and systems or from external events, such as cyber-attacks. They can be the source of shocks to the wider financial system, or they can act as amplifiers in episodes of financial stress.

One of the priorities of the Bank of England's (the Bank) Financial Policy Committee (FPC) is to continue to improve macroprudential oversight of operational resilience, by focusing on the risks that could lead to system-wide operational disruption. This is consistent with the FPC's primary objective to identify, monitor, and take action to remove or reduce systemic risks.

As previous operational incidents highlight, operational resilience has become more important to maintaining financial stability, particularly as the financial system has become more digitalised and interconnected (Section 1). Looking ahead, that importance will continue to grow as new and evolving technologies play a greater role in the provision of financial services and as business models continue to change.

The FPC is developing its approach to assessing financial stability risks from potential operational incidents and considering how and where operational resilience might need to be improved in the financial system (Section 2).

The FPC considers that firm-level operational resilience, built by individual firms and FMIs, provides the essential foundation for operational resilience across the system. The likelihood that an individual firm or FMI will experience an operational incident is determined by its vulnerabilities. These include operational weaknesses, risks associated with transformation and the need to adapt or deliver change programmes, and firm-level dependence on data to support the provision of services.

These vulnerabilities should be, and can only be, addressed by firms' and FMIs' operational risk management processes, and by implementing the operational resilience policies set by their microprudential regulators, including the Bank, the Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA), which aim to ensure that any disruption to important business services does not impact the objectives of those regulators and the Bank's financial stability objective.

But the resilience of individual firms and FMIs alone may not be sufficient to ensure system-wide resilience: some additional vulnerabilities exist at the level of the entire system. These vulnerabilities include: interconnectedness, complexity and opacity; concentration; correlation and common vulnerabilities; and system-wide dependence on data.

The operational resilience polices set by the Bank, the PRA and the FCA help to bridge the gap between firm-level and system-wide operational resilience. To build operational resilience under these policies, firms and FMIs must identify their important business services. Given the risks to financial stability from operational disruptions, the FPC expects that relevant firms[1] and FMIs, ie those that are required to take account of risks to UK financial stability under the operational resilience policies, should consider the vital services that are important to financial stability when they identify their important business services. These vital services include:

- payments, clearing and settlement, and other related activity such as custody services;
- deposit taking and the provision of credit, as well as equity capital, including activity in primary and secondary fixed income and equity markets, as well as repurchase agreements (repos) and securities lending; and
- insurance and the facilitation of transactions involving derivatives (for example, for hedging), and activities which support the functioning and supply of liquidity in markets (for example, secondary market making).

More broadly, firms and FMIs must also factor in the potential impacts on the wider financial system from weaknesses in their own operational resilience and actions they might take in response to incidents, as they take steps to build their resilience.

While there have been a number of operational incidents in the financial sector, to date they have not resulted in material impacts to financial stability. The FPC is working with other regulators and industry to ensure the operational resilience of the financial sector as a whole. The FPC will regularly review the operational resilience policy toolkit – with regard to new threats, changes in technology and changes in how the financial system provides vital services – and will explore ways to continue to build system-wide resilience to operational disruption (Section 3), including through:

- assessing potential system-wide gaps in, or risks to, operational resilience, which are not adequately covered by firm-level or microprudential policies;
- continuing to conduct cyber stress testing, and considering stress testing for other possible operational disruptions. The next cyber stress test is due to start in Spring 2024 with the findings expected to be published in the first half of 2025;
- monitoring the implementation and outcomes of the regime for critical third parties; and
- considering whether to set impact tolerances for additional vital services beyond payments.

This Financial Stability in Focus complements the work of the regulators (the Bank, the PRA and the FCA) on microprudential policies and supervisory engagement to strengthen operational resilience. It will be relevant to a range of domestic and international stakeholders, including:

- the boards and relevant executives of financial firms and FMIs, to understand better the role they play in contributing to the operational resilience of the financial system;
- third-party service providers, to understand the role they play in the financial system; and
- policymakers and academics, given increasing work on this topic globally.

1: Background and context: operational resilience

The Financial Policy Committee (FPC) is responsible for protecting and enhancing the stability of the UK financial system.

It does this by identifying, monitoring, and taking action to remove or reduce risks to financial stability. This includes operational risks, which cover a wide range of non-financial risks faced by financial firms and financial market infrastructures (FMIs).

Operational resilience is the ability of individual firms, FMIs and the wider financial system to prevent, adapt and respond to, as well as recover and learn from, operational disruptions. It is supported by firm-level and system-wide policies and tools to mitigate operational risk.

Previous incidents highlight the growing risks to financial stability from operational issues and the importance of system-wide resilience.

A range of operational incidents have led to adverse impacts at firms and FMIs. There have been idiosyncratic incidents, including incidents related to IT upgrades at firms (for example, TSB Bank plc's 2018 IT migration) or system outages at FMIs (for example, Euroclear UK & International's 2020 settlement system outage). The entire financial sector was impacted operationally by the Covid-19 pandemic, although firms and FMIs were able to adapt quickly, illustrating the benefits that technology can bring in strengthening resilience. During the period of financial instability associated with the liability-driven investment (LDI) funds incident in September 2022, operational issues amplified the initial financial stress (see Section 2.4 for further detail). While recent ransomware attacks at several financial firms and third-party providers (for example, ION, ICBC Financial Services and EquiLend) did not impact financial stability, they showed how such incidents have the potential to amplify risks across the financial system as disruption at one firm can cause disruption at others.

Digitalisation and innovation bring benefits and opportunities in the financial system.

Financial firms are using data to improve their services and to better manage risk. And the continuing application of artificial intelligence and machine learning to financial operations is widely expected to continue these trends and bring similar benefits.

Financial services are increasingly facilitated by a wider and increasingly interconnected range of firms.

The growth in market-based finance has shifted the provision of some services away from banks to a large number of highly interconnected, non-bank financial institutions. Competition and specialisation can help drive efficiencies. But the shift in activity from systemically

important institutions to a multiplicity of interconnected firms in systemically important markets makes the management of risk, including operational risk, in these markets more important to financial stability.

At an operational level, firms and FMIs are relying more on non-financial firms to support the delivery of financial services. Cloud service providers, for instance, provide firms and FMIs with shared data storage and processing capabilities, integrated security features, and advanced approaches to big data. Using certain services provided by third parties may make some firms more resilient in certain areas, while creating new interconnections and important third-party dependencies. The resilience of third parties, and of certain services they provide to the financial sector, will continue to grow in importance to financial stability as they become increasingly integral to operations and the provision of services by firms and FMIs.

In addition, a small number of FMIs have become more central to certain operations needed for a stable financial system. Following post-global financial crisis reforms, the provision of certain functions is concentrated in FMIs, including central counterparties (CCPs), and this has made their resilience more important to financial stability.

> **Growing digitalisation, interconnectedness and third-party dependencies increase the potential for operational risks to impact financial stability.**

Operational risk covers a wide range of non-financial risks faced by firms and is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events.[2] It includes the risk of technology failures or outages, but also the potential for employee errors or negligence, including fraud and other factors related to institutional culture, such as inadequate training. The crystallisation of operational risks can be the source of shocks to the wider financial system, or they can act as amplifiers in episodes of financial stress.

> **The management of financial risk has historically been the focus for macroprudential authorities. But the effective management of operational risk is increasingly important to maintaining financial stability.**

For example, cyber-attacks are an immediate risk to firms and FMIs. The **National Cyber Security Centre** received over 2,000 reports of cyber-attacks in 2023. And cyber-attacks were cited as a risk to financial stability by more than 70% of respondents in each of the Bank of England's (the Bank) **Systemic Risk Surveys** since 2020. The risk of cyber-attacks is correlated with increased geopolitical risk, which was cited as the most significant risk to financial stability in the 2024 H1 survey.

> **A stable financial system is one which facilitates and supplies vital services to households and businesses in a manner that absorbs rather than amplifies shocks. And the continued provision of vital services is at the core of operational resilience.**

To be operationally resilient, the financial system needs to be able to continue to provide vital services to households and businesses through severe but plausible operational disruptions. Table A provides more information on the vital services set out in **The Bank's Financial Stability Strategy**, including illustrative and non-exhaustive examples of the types of activities provided by firms and FMIs that underpin the provision of vital services.

Table A: Vital services and the types of activities that underpin their provision

Vital services	Types of activities
The provision of payment and settlement services	Supports the exchange of goods and services across the financial system and the economy, and includes payments, clearing and settlement, and other related activity such as custody services.
Intermediating between savers and borrowers, and channelling savings into investment	Supports the redistribution of capital across the financial system and the economy, and includes deposit taking and the provision of credit, as well as equity capital. Includes market-based activity in primary and secondary fixed income and equity markets, as well as repurchase agreements (repos) and securities lending.
Insuring against and dispersing risk	Supports the management of risk across the financial system and the economy. Includes insurance and the facilitation of transactions involving derivatives (for example, for hedging), and activities which support the functioning and supply of liquidity in markets (for example, secondary market making).

The FPC has already taken a number of actions to support system-wide operational resilience. In recognition of the importance of vital services to financial stability, the FPC has set an impact tolerance (ie the maximum tolerable level of disruption) for critical payments whereby it expects the financial system to have the capability to complete critical payments by the end of the value date (ie the ability to make payments on the date they are due), even in severe but plausible scenarios. The Bank also uses regular cyber stress tests to explore the ability of firms and FMIs to stay within impact tolerances set by the FPC, which so far have focused on critical payments. The FPC has also previously identified the risk posed by the increasing reliance of firms and FMIs on critical third parties (CTPs). Following the creation of a statutory CTP framework, the Bank, the Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA) published a **consultation paper** in December 2023 with proposed requirements and expectations to manage risks posed by CTPs.

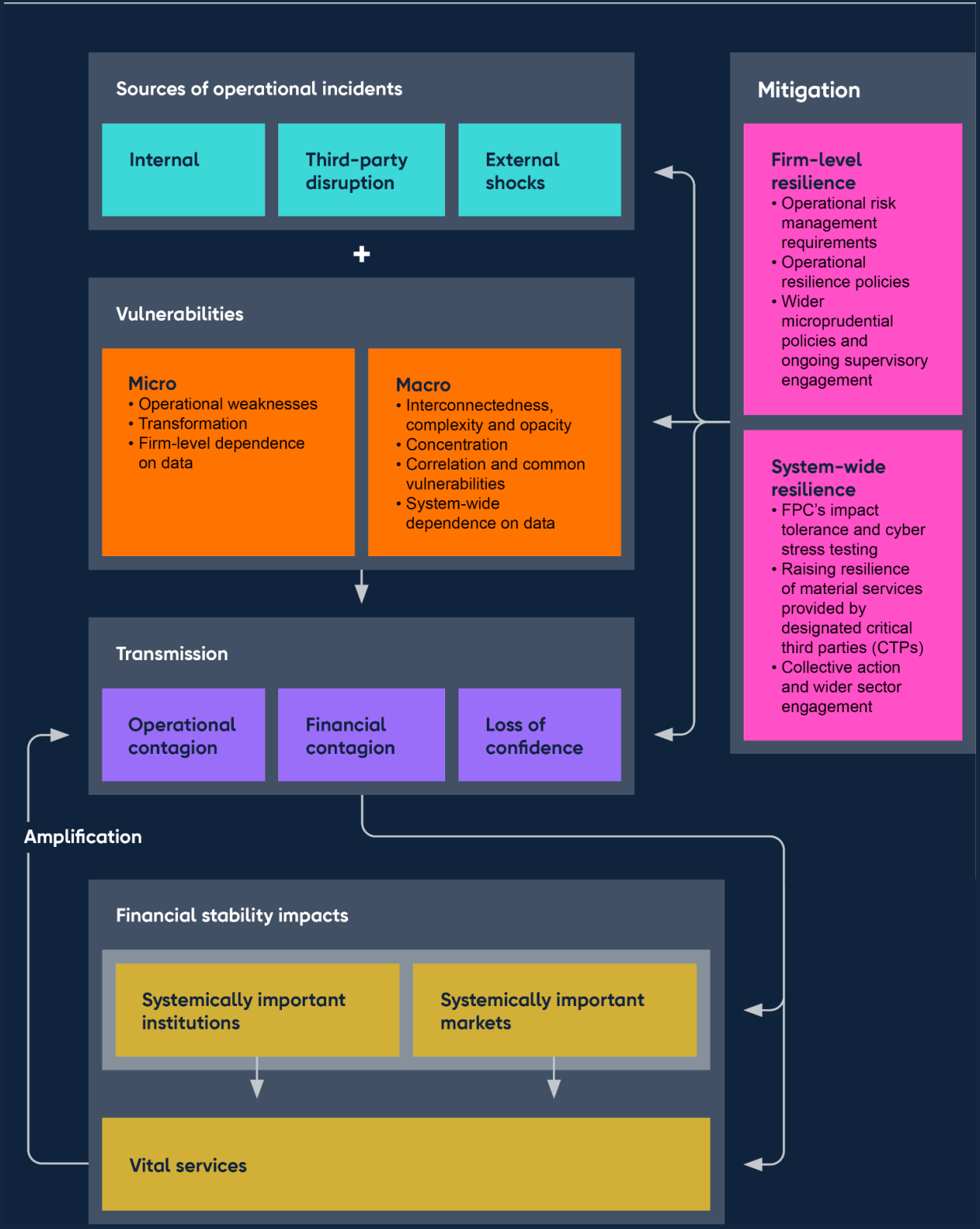
2: The FPC's approach to risk identification, assessment, and monitoring

Operational incidents can stem from a range of sources, including internally in a firm or FMI, from a firm's or FMI's third-party service provider, or from external shocks. Vulnerabilities exist at the firm and system level (micro and macro vulnerabilities, respectively), and there are various transmission channels which mean that operational incidents at a single firm can lead to potential financial stability impacts. An operational incident can create financial stability risks by disrupting the provision of vital services, either directly because of the disruption itself, or indirectly through impacts on systemically important institutions or systemically important markets.

> **The resilience of individual firms and FMIs is important but this alone may not be sufficient to ensure the resilience of the whole system.**

Figure 1 illustrates the FPC's approach to assessing financial stability risks from potential operational incidents. Macro vulnerabilities – which cover the risks that exist at the system level – can amplify operational shocks and make risks to financial stability more likely to materialise. Firm-level resilience, built by firms and FMIs and supported by microprudential policy and supervision, provides the essential foundation for system-wide operational resilience. But it may not be sufficient to ensure the resilience of the whole system. Macroprudential policy builds on firm-level policies and contributes to system-wide operational resilience by seeking to identify and address the vulnerabilities that exist at the system-wide level. The following sections outline the detail of the FPC's approach, stepping through the sources (Section 2.1), vulnerabilities (Section 2.2), then transmission channels and financial stability impacts (Section 2.3).

Figure 1: The FPC's approach to assessing financial stability risks from potential operational incidents



2.1: Sources of operational incidents

Operational incidents in firms, FMIs and markets can have a variety of sources.

The FPC's macroprudential approach considers the sources of operational incidents across the financial system in terms of three categories: 'internal', 'third-party disruption' and 'external shocks' (Table B).

Table B: Sources of operational incidents

Source	Description and examples
Internal	Disruption originating from a firm's or FMI's own processes, people and systems. For example: IT outages, implementation failure of a procedure or process, human error, conduct issues (including fraud), and poor culture.
Third-party disruption	Disruption originating from third parties supporting the provision of vital services by firms and FMIs. For example: technology failures, cyber-attacks or data integrity issues that cause disruption to a third party.
External shocks	Shocks originating from outside the financial system which impede the provision of vital services. For example: cyber-attacks, geopolitical events, severe weather events, disruption to basic infrastructure (for example, power), and pandemics.

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.

Many operational incidents can be contained and addressed by the affected firms and FMIs. This is often the case where operational incidents arise from internal sources, for example disruptions to firms' and FMIs' on-premise IT infrastructure. Operational disruptions caused by factors like poor culture and weak governance can often reflect firm-specific issues too.

Some operational incidents are more likely to have systemic impacts because of certain features of the financial system, such as interconnectedness or because the affected firm is systemically important. Operational incidents in systemically important markets could lead to widespread impacts because of interconnections between participants. Systemic impacts could also occur where internal disruptions are common across firms, such as functionality issues in commonly used software or a cyber-attack that impacts multiple firms at the same time. Disruptions at third parties that provide services widely across the financial sector, or significant external shocks that impact much of the financial sector could also have systemic impacts.

2.2: Vulnerabilities

Disruption caused by operational incidents should, in most cases, be mitigated quickly and have limited impact on the wider financial system or real economy.

However, there are vulnerabilities which, when combined with an operational incident, could lead to disruption that impacts financial stability.

Micro vulnerabilities are inherent to specific business models or operational arrangements (Figure 1).

Operational weaknesses include inadequate or failed firm-level management of internal processes, people and systems, and a lack of preparedness to third-party disruption and external shocks. The impacts from operational incidents can be mitigated by effective control frameworks and resilience to shocks, and by having sufficient response and recovery capabilities. Operational weaknesses can arise in all parts of a firm's or FMI's operations, including processes or governance procedures that are poorly designed, employees that are inadequately trained, business areas that are insufficiently resourced, poor culture, or third-party services that are inappropriately configured or overseen by a firm or FMI. These weaknesses can result from a lack of understanding of new and evolving operational risks at various levels within firms and FMIs (from operators and managers to executives and boards) and from underinvestment in operational resilience. There can be large financial consequences for individual firms and FMIs when such weaknesses are exploited. For example, in 2012 the so-called 'London Whale' trader lost JPMorgan £4.4 billion from unauthorised trading activity.

Transformation captures the vulnerabilities that arise from adapting, or failing to adapt to, the changing technology landscape. As digitalisation and automation increase across the financial system, business models and the operational arrangements of firms and FMIs will necessarily adapt. Transformation captures the risks that arise from adopting new technologies that are less well understood, and from any large-scale change programmes. For example, in 2018, TSB Bank plc (TSB) updated its IT systems and migrated the data for its corporate and customer services on to a new IT platform. While the data itself migrated successfully, the platform immediately experienced technical failures. All of TSB's branches and a significant proportion of its 5.2 million customers were affected by the initial issues. **TSB was fined £48.65 million in December 2022** for its operational risk management and governance failures, including its management of outsourcing risks, relating to the firm's IT upgrade programme.

Firm-level dependence on data refers to the fact that available and timely data are essential to the operations of individual firms and FMIs. In the same way that the functionality of systems is important to firms' and FMIs' operations, so are the data required by those systems. Data that are both available and trustworthy are essential inputs into digitalised

systems, and any issues with access to, or integrity of, data could quickly lead to an interruption in the services provided by firms and FMIs. To realise the benefits of artificial intelligence and machine learning effectively and safely – and from digitalisation more widely – it will be important for firms and FMIs to focus on the integrity and accuracy of the data to which those tools are applied. This will be fundamental to safe innovation and operational resilience.

While these micro vulnerabilities are specific to individual firms and FMIs, disruption from firm-level incidents can be amplified and transmitted across the system, potentially resulting in financial stability impacts (as set out in Section 2.3).

> **Macro vulnerabilities are system wide and come about as a result of the structure of the financial system and the collective behaviour of individual institutions and other participants within it (Figure 1).**

While operational incidents are most likely to originate in one specific part of the financial system, structural features and the collective behaviour of firms, FMIs and other participants could amplify operational shocks in ways that can impact financial stability. These system-level vulnerabilities capture the risks in the financial system beyond those posed by adding up risks associated with individual firms and FMIs.

Markets and participants in the financial system are **highly interconnected, and often in complex and opaque ways**. Interconnections exist from counterparty relationships that arise from financial activities between firms and FMIs. Outsourcing and third-party relationships can also create interconnections, whether from the complete outsourcing of service provision (for example, banks outsourcing the provision of insurance services) or outsourcing of functions that support the delivery of services (for example, cloud storage, or key back-office functions such as administrative and support services for IT, HR or legal functions). The multitude of complex interconnections increase the likelihood that operational disruptions have knock-on impacts. This includes the risk that in the event of an operational disruption, actions taken in the interests of an individual firm or FMI could cause unanticipated disruptions in different parts of the system that lead to adverse impacts on financial stability.

Concentration arises where there is reliance on a small number of providers of a given service, which means that an incident in one provider could have a disproportionate impact on the system. FMIs are a key example: they facilitate the movement of cash and securities and the clearing of financial derivatives needed to settle transactions and intermediate exposures between market participants, helping to ensure that financial obligations are met. The services provided by FMIs reduce many risks in the financial system, but their central role means that any operational disruption they face could have systemic impacts. The Bank regulates certain FMIs to make sure they are operating safely, and to protect and enhance financial stability in the UK and internationally.

However, other critical nodes and infrastructure providers exist in the financial system. They can be critical because of their size, the criticality of the service they provide, the structure of the market in question or their position within a market. This includes messaging systems and various trading and data platforms. In 2019, the **FPC identified** that Principal Trading Firms (PTFs) had become substantial short-term liquidity providers in fast markets (including spot foreign exchange, equities and some derivatives markets), and that there was a concentration of 'nodes' of clearing services to PTFs. The FPC highlighted that this concentration increases the risk of short-term disruption to market liquidity in the event of failure or paralysis (for example, from operational disruption) of one of these nodes. Indeed, in November 2023, ICBC Financial Services – the US broker-dealer and a key clearing member in US Treasuries for PTFs – experienced a ransomware attack. The attack impacted its client clearing business and there was some disruption in the US Treasury market. Wider impact was limited, however, by the availability of several alternative ways to trade in the broader structure of the US Treasury market, which demonstrated the resilience of the market as a whole.

Systemic risk may also be driven by operational resilience failings from outside the finance sector, in particular where financial firms are dependent on a small number of third-party service providers, or from reliance on key upstream infrastructure (including, for example, electricity and communications). The vulnerabilities in the financial system from concentration are further amplified when there is a lack of substitutability. Critical nodes can become single points of failure where there is a lack of viable alternative providers for services, or where there are potential difficulties for firms and FMIs in migrating services in a timely manner and without undue risk.

Correlation and common vulnerabilities exist where it is possible for one source of disruption to have widespread impacts across the financial sector. Operational similarities across the financial system could mean that multiple firms or FMIs may be impacted simultaneously by the same operational incident, leading to widespread and potentially systemic disruption. This could occur if many firms or FMIs use the same software and a weakness in that software is exploited, which was the case in the SolarWinds hack in 2020. It could also occur if multiple firms have similar processes that fail in the same way at the same time, for example, widespread mis-selling of Payment Protection Insurance (PPI) by UK banks between 1990 and 2010. Reliance on common technologies could also cause multiple firms or FMIs to respond in the same way during an incident, whether operational or financial in nature, and such herding behaviour could amplify the impacts. There is a risk that this could be exacerbated if there is widespread adoption of common artificial intelligence models, for example. Correlated risk can also arise when multiple firms or FMIs rely on the same contingency resources during a disruption, which may not have the capacity to service all those firms or FMIs simultaneously. An operational incident that affects confidence could also have systemic impacts if the loss of confidence impacts a wide number of firms or FMIs.

System-wide dependence on data arises because timely access to accurate data is critical to the functioning of the financial system. Concerns about the loss of access to data, or uncertainty about the integrity of data – for example in the event of a cyber-attack – could spread quickly across the financial system because of an inability to transact, which could disrupt payment flows or impede price discovery. Disruption to data availability or integrity could lead quickly to a widespread loss of confidence and trigger behavioural choices not to transact in the financial system. Difficulty restoring data access and gaining reassurance about the accuracy of data could lengthen recovery time following an operational disruption and further amplify impacts.

In practice, several vulnerabilities are likely to be present and could interact during an operational disruption. For example, in January 2023, ION – a third-party provider of derivatives clearing services that operates in a concentrated market – experienced a ransomware attack which impacted the processing of trades, and there were knock-on impacts caused by loss of data availability. The relative importance of vulnerabilities can also evolve over time, and steps to reduce some vulnerabilities may increase others.

2.3: Transmission channels and financial stability impacts

> **Transmission of an operational incident across the financial system can occur through operational contagion, financial contagion, and a loss of confidence (Figure 1).**

- **Operational contagion** occurs when an initial operational disruption causes further operational disruption elsewhere in the financial system or the real economy. An operational outage affecting the services of a firm or FMI could leave them unable to transact with other firms or participate in financial markets. This will have knock-on impacts to the ability of the disrupted firm's or FMI's counterparties to undertake their own activities. For example, in January 2024, EquiLend – a global securities trading platform – experienced a ransomware attack which led to an outage in its trading services, impacting its clients' ability to meet regulatory reporting requirements and manage their own risks. A disruption like this could cause widespread market disruption if vital services delivered by multiple firms are impacted at the same time. Operational contagion could also spread beyond the financial sector and lead to disruption in the real economy if households and businesses are prevented from transacting.
- **Financial contagion** occurs when operational disruption leads to financial impacts. This could happen if an operational disruption impacts liquidity flows. For example, as part of intraday liquidity management, banks use incoming payments to provide funds for outgoing payments. If one firm in the system is unable to send payments, this may create liquidity shortages at other firms (**Eisenbach et al (2021)**). **Kotidis and Schreft (2022)** used confidential data to study the effects of a cyber-attack at a technology service provider in

the US that impacted the ability of several banks to send payments over Fedwire. This caused other banks to receive fewer payments, and these other banks had to take mitigating actions such as drawing on their reserves or borrowing from the discount window or federal funds market to prevent the financial impacts from spreading further. Financial contagion could also occur if an operational disruption impacts access to funding sources, price discovery in certain markets or for particular assets, or a firm's ability to make margin payments to a CCP, triggering default proceedings (**Ros (2020)**, and **Brando et al (2022)**). If a financial loss from an operational issue threatened the solvency of a firm it could lead to systemic impacts if the losses occurred at a systemically important institution, or if financial losses were widespread across a large number of firms.

- **Loss of confidence** can be a key point of transmission across the financial system. Operational disruption can lead to a loss of confidence if the incident causes a firm's or FMI's counterparties or customers to revise their view of the riskiness of the institution, or the institution's ability to manage its risks and the risks to its business model (**Healey et al (2021)**). The possibility that an unaffected firm or FMI could be vulnerable to the same operational disruption, or cyber-attack, that impacted another firm or FMI could trigger a loss of confidence across the financial system. This could lead to run behaviour at otherwise healthy firms or mean that firms reduce their risk appetite and become reluctant to extend liquidity or credit. Even if an individual institution is not considered systemic, if a risk is perceived to be common among similar institutions, the collective impact could pose a systemic risk. While operational and financial contagion can be mitigated with a number of workaround solutions (such as manual processing where automated systems are impaired, or alternative sources of funding), confidence can be difficult to restore once lost. For this reason, loss of confidence is the transmission channel by which an operational disruption may most likely lead to financial instability, though there is yet to be an instance where an operational incident in the UK financial sector has resulted in financial instability.

In addition to an operational disruption at one firm leading to operational, financial and confidence impacts at other firms, there may also be interaction between those three channels, further amplifying the negative effects. For example, financial impacts could lead to a loss of confidence if liquidity was impacted at multiple firms following an operational disruption at one firm and that led to wider concerns about the management of liquidity risk across the system.

> **Vital services can be disrupted when there is disruption to systemically important institutions or markets.**

The provision of vital services by the financial system matters because if it is disrupted, it could impact the ability of financial sector participants, households and businesses to transact or access financing. Importantly, if there is disruption to vital service provision it could

undermine confidence in the financial system. In providing their own services, firms and FMIs collectively contribute to the provision of vital services and a stable financial system.

Systemically important institutions are those that, if disrupted, could impair parts of the financial system and have serious negative consequences for the real economy. This is due to their size, level of substitutability, interconnectedness and/or complexity. The services provided by these firms and FMIs are a crucial part of the overall provision of vital services, so operational resilience in the provision of such services is important to maintaining a stable financial system.

Payment and settlement services are necessary for facilitating transactions within the financial system and between households and businesses, enabling activity in the real economy. The impacts from disruptions to payment and settlement services are often quickly felt and, as such, there is limited tolerance for disruption. For example, Visa Europe – a recognised payment system in the UK – experienced a partial service disruption in June 2018 in which 5.2 million Visa transactions in the UK and elsewhere failed to process correctly. The impacts on customers' ability to transact and the potential to affect confidence in the financial system led the **Bank to use its statutory powers** to direct Visa Europe to fully implement the recommendations of an independent review.

Systemically important financial markets are those that are essential for financing or providing other important services to the real economy, and which cannot be easily substituted. Disruption to systemically important markets, for example due to disruption in the ability of market participants to conduct trades, can impact the provision of vital services in a number of ways. This includes by disrupting intermediation between savers and borrowers (for example, in equity and bond markets) and risk sharing (for example, in derivatives markets). For example, the London Stock Exchange Group experienced an outage due to a software glitch in 2023, and while there were no impacts to financial stability, the trading of many smaller listed companies was impacted. There have also been incidents at exchanges in other jurisdictions, including at Deutsche Börse and the Australian Securities Exchange in 2020, and at the New York Stock Exchange in 2023.

There can be an interdependence between systemically important institutions and markets. Systemically important institutions rely on well-functioning markets to provide services for their customers, as well as for their own financing and liquidity needs. Similarly, systemically important markets rely on the participation of firms and FMIs to function well. For example, operational disruption in firms, FMIs and trading platforms operating in sovereign bond markets could impact government financing, the provision of high-quality and liquid collateral, the cost of borrowing and the pricing of other financial instruments, as well as impact related repo and futures markets.

Firms and FMIs must factor in the potential impacts on the wider financial system from weaknesses in their own operational resilience and actions they might take in response to incidents, as they take steps to build their resilience.

> **Disruption to non-systemically important firms can also impact the provision of vital services.**

Systemically important activities can be carried out by a number of smaller, non-systemic firms collectively. If only one or a few non-systemic firms are disrupted operationally, it is unlikely that the impact would lead to serious negative consequences for the real economy. But if a disruption was common – or perceived to be common – among similar institutions, the collective impact to the provision of vital services could pose a systemic risk. This could be due to correlated risks caused, or faced by, a large number of smaller firms, or through a widespread loss of confidence.

A series of low-level operational incidents at a firm – whether systemic or non-systemic – or at an FMI could also pose a risk to financial stability and the provision of vital services if the accumulated impact grew large enough, or if it led to a loss of confidence in the financial system. It is important that individual firms and FMIs have the ability to withstand a wide range of operational risks through their risk management approach and put in place effective response and recovery plans.

The scale of impact from an operational disruption depends to an extent on the duration of the incident. Uncertainty about the potential duration or form of an incident could also act as an amplifier.

2.4: Operational risk as an amplifier of financial risk

> **Operational barriers can also arise during periods of financial stress and have the potential to act as amplifiers of system-wide impacts.**

The **LDI stress in September 2022** is a key example of a period of financial instability during which operational issues amplified the initial financial stress.

During this episode of market volatility, the replenishment of LDI funds' liquidity buffers was hindered by firms' operational arrangements, and in some cases by the governance processes at pension schemes, exacerbating liquidity issues and the need to sell assets in stressed conditions. In addition, some custody banks which provide services to these funds struggled to keep pace with the volume and complexity of requests. The operational complexities of making and receiving large volumes of collateral calls during periods of significant market volatility amplified the market stress. This was particularly a problem for pooled LDI funds due to operational lags and the large number of smaller investors.

The incident also highlighted the importance of good operational processes; custody banks with automated processes and usable crisis playbooks were able to manage the incident relatively well compared to those with manual processing and inadequate scenario testing.

Alongside its March 2023 **Recommendation** to the Pensions Regulator on steady-state minimum levels of resilience for LDI funds, the FPC judged that pension schemes might need to improve their operational processes to provide collateral to their LDI funds more swiftly when needed.

2.5: Monitoring and identifying emerging risks

> **The FPC monitors a range of potential sources of system-wide operational disruption, including national security, geopolitical and climate risks. The FPC regularly considers changes in the financial system, including through the emergence of new and evolving technologies, which are leading to operational changes that may require further attention.**

The FPC has considered the financial stability implications of a number of emerging technologies and applications, including distributed ledger technology, tokenisation and new forms of digital money. It has also considered risks posed by the financial sector's increasing reliance on certain technology firms such as cloud service providers. **In December 2023 the FPC was given an update** on work undertaken by the Bank, the PRA and the FCA to assess the continued application of evolving technologies, such as artificial intelligence and machine learning. Wider adoption could conceivably amplify herding or broader procyclical behaviours, or increase cyber risk (such as through more sophisticated fraud or scams) and risks arising from interconnectedness.

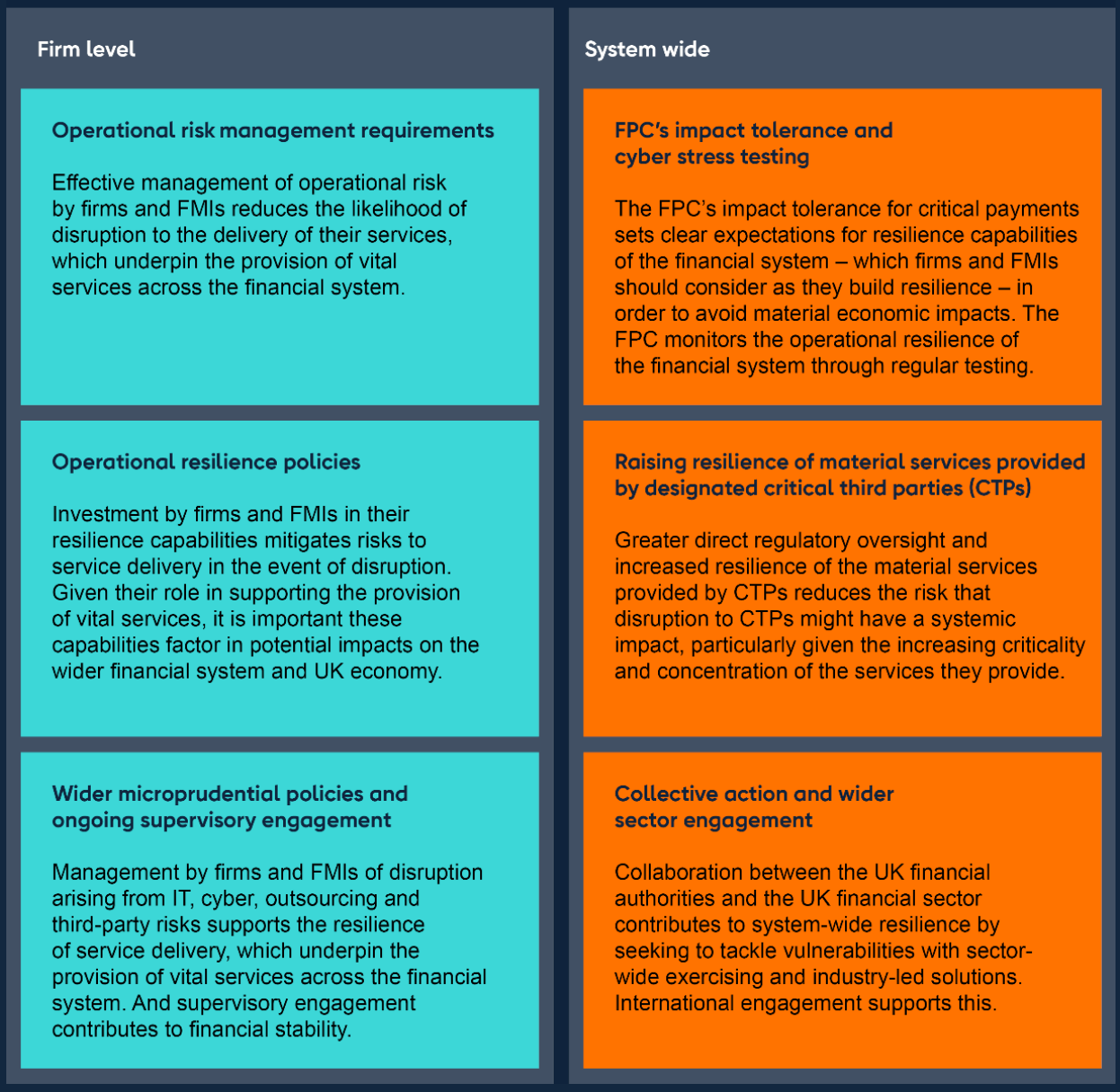
3: Building resilience

When individual firms, FMIs, and the wider financial system are resilient, the risk of threats from a range of potential sources to vital services can be reduced. Firms and FMIs will also be able to respond to and absorb shocks, limiting their transmission across the financial system and to the real economy.

> **The operational resilience policy toolkit seeks to strengthen operational resilience across the financial system.**

There are a range of firm-level and system-wide policies and tools that are focused on strengthening operational resilience across the UK financial system. Firms and FMIs, along with third-party service providers, contribute to the operational resilience of the wider financial system through measures they implement within their own organisations, as well as through system-wide resilience policies, as set out in Figure 2.

Figure 2: Both firm-level and system-wide policies contribute to the operational resilience of the financial system



These measures collectively support system-wide operational resilience and help to reduce financial stability risks posed by the macro vulnerabilities set out in Section 2.2. Greater resilience at individual firms and FMIs can reduce the likelihood of operational incidents occurring, and this can, for example, improve the system's resilience to simultaneous cyber-attacks on multiple firms, as fewer individual firms or FMIs may be adversely affected. High-quality response and recovery capabilities at individual firms and FMIs can also limit contagion across the system when operational incidents occur, maintaining confidence in the financial system.

3.1: Building firm-level operational resilience

Effective management of operational risk promotes operational resilience.

Firms and FMIs are required to manage operational risk in a way that:

- includes an effective risk management framework, enabling them to reduce the likelihood of operational incidents occurring;
- limits losses and the impact of risks in the event of disruption; and
- promotes the ability to absorb losses by holding sufficient capital and having robust business continuity plans for when risks crystallise.

The operational resilience policies set by the Bank, the PRA and the FCA came into force on 31 March 2022 and firms and FMIs will need to demonstrate their ability to meet the policies by 31 March 2025.[3] The policies require and expect regulated firms to deliver important business services within impact tolerances, even under severe but plausible disruption, while regulated FMIs are expected to do so while withstanding extreme but plausible disruption.[4] This entails firms and FMIs identifying their important business services, undertaking scenario testing and addressing weaknesses that might stop them from remaining within impact tolerances. Doing so may involve making investment decisions to build appropriate capabilities and resilience. And the boards of firms and FMIs have to play an active role in approving and regularly reviewing the important business services and impact tolerances that have been set.

Relevant firms and FMIs should also consider system-wide operational resilience.

Relevant firms[5] and FMIs are expected to identify important business services and set impact tolerances with consideration to financial stability in terms of the impact on the wider financial sector and UK economy. For relevant firms, this includes considering the potential to cause knock-on effects for counterparties or markets, the potential to inhibit the functioning of the wider economy, and whether the service is covered by an impact tolerance set by the FPC. And FMIs should consider whether a prolonged disruption of a business service would significantly disrupt the orderly functioning of a market in which an FMI provides services, thereby impacting financial stability.

The operational resilience polices set by the Bank, the PRA and the FCA help to bridge the gap between firm-level and system-wide operational resilience.

As highlighted in Table A, firms and FMIs play a key role in the provision of vital services to households and businesses. And Section 2.3 describes the potential financial stability impacts arising from disruption to vital services. Given the risks to financial stability from operational disruptions, the FPC expects that relevant firms and FMIs should consider the vital services that are important to financial stability when they identify their important business services under the operational resilience policies.

Wider microprudential policies and tools also contribute to firm-level operational resilience.

There are expectations on **firms'** and **FMIs'** ability to manage IT, cyber, outsourcing and third-party risks, as well as ensuring capabilities on incident management and business continuity.

To maintain the cyber resilience of the UK financial sector and to support supervisory oversight, regulators have developed **cyber assessment tools**. The CBEST Threat Intelligence-Led Assessment programme and STAR-FS (Simulated Targeted Attack & Response assessments for Financial Services) enable firms to explore how an attack on the people, processes and technology of a firm's cyber security controls may be disrupted, and how they can plan to strengthen their resilience through remediation. CQUEST, a cyber resilience questionnaire, forms part of the Bank, the PRA and the FCA's supervisory toolkit to gauge the cyber risk and resilience capabilities of the financial sector.

3.2: Enhancing system-wide operational resilience

The presence of macro vulnerabilities means operational incidents can lead to significant contagion across the financial system.

Alongside the need for firms and FMIs to consider system-wide resilience when implementing operational policies, the FPC is taking forward a range of approaches to strengthen operational resilience.

Assurance from firms and FMIs that they will be able to remain within the FPC's impact tolerance for critical payments will support system-wide operational resilience.

Building on its previous work on cyber risks, and to support its role on establishing clear baseline expectations, the FPC can set 'impact tolerances' for how quickly financial companies must be able to restore vital services following a severe but plausible cyber or operational incident.

The FPC has set an impact tolerance for critical payments and expects the financial system to have the capability to complete critical payments by the end of the value date, even in severe but plausible scenarios.[6] The **FPC has judged** that firms and FMIs that are required to take account of risks to UK financial stability under the operational resilience policies should consider the FPC's impact tolerance for critical payments when formulating their own payment impact tolerances, alongside other applicable requirements.

The Bank uses regular cyber stress tests to explore the ability of firms and FMIs to meet impact tolerances set by the FPC, with a focus on how firms and FMIs respond and recover in severe but plausible scenarios. To date, the tests have focused on the FPC's impact tolerance for critical payments. Cyber stress testing considers potential financial stability impacts, helps

to build an understanding of the financial system's operational capacity to absorb a significant operational incident, and the ability of firms and FMIs to restore functioning of services after such an incident.

The 2022 exercise explored a hypothetical data integrity scenario in retail payments covering FMIs and several firms, and following this **the FPC reviewed its impact tolerance for critical payments**. While the FPC still expected the financial system to have the capability to meet its impact tolerance, it recognised that there might be instances where the disruption caused by an incident was such that, despite prior planning, attempting to recover by the end of the value date could have a more adverse impact on financial stability than failing to make the value date. An instance in which data were corrupted might be one such example.

> **Improving the resilience of material services provided by designated CTPs through the setting of resilience standards will help to reduce systemic risks.**

The FPC has previously highlighted that the increasing reliance of firms and FMIs on CTPs has the potential to threaten financial stability in the absence of greater direct regulatory oversight of the resilience of material services that CTPs provide. The **Financial Services and Markets Act 2023** gave HM Treasury the power to designate CTPs – which will generally follow a recommendation from the regulators (the PRA, the FCA and the Bank) – and allows the regulators to make rules to raise the resilience of material services that designated CTPs provide to firms and FMIs.

The CTP regime will help to reduce the risks of systemic disruption to the financial sector and enhance system-wide operational resilience. UK regulators published a **consultation paper** in December 2023, which includes proposed fundamental rules, operational risk and resilience requirements, information-gathering and testing requirements, and incident notification requirements for CTPs.

> **The collaborative approach between the UK financial authorities and the UK financial sector, through collective action and wider sector engagement, promotes an important and timely emphasis on system-wide operational resilience.**

This collaboration contributes to enhancing system-wide operational resilience, including by seeking to tackle some of the macro vulnerabilities identified, which helps to ensure the industry works together effectively to respond to an operational incident.

In support of this, **the Bank, the PRA and the FCA engage in collective action and wider sector engagement** to develop a view on sector-wide risks, to support firm and sector-level resilience building, and to enhance the sector's ability to respond to system-wide disruption through exercising. This includes working closely with the Government, including the National Cyber Security Centre, to respond to cyber threats.

The financial sector's collaborative work to build resilience, known as collective action, is co-ordinated through the **Cross Market Operational Resilience Group (CMORG)**, which seeks to identify risks, develop solutions and share knowledge for the benefit of the sector as a whole, supporting system-wide resilience.

The financial authorities regularly work with the financial sector to run a range of exercises to assess and test the UK financial sector's resilience to major operational disruption, which helps to develop an understanding of risks to the sector. A sector-wide operational resilience exercise (known as SIMEX) takes place every two years. A two-day market-wide simulation exercise took place in 2022, which simulated how the financial sector could respond to an operationally-paralysed global systemically important bank (**SIMEX 22**). The next exercise is due later this year.

In the event of a disruption, the authorities maintain a sector-wide incident response capability, which is facilitated by the Sector Response Framework. And where disruptions have the potential to impact the sector as a whole, the UK's financial authorities act together through the **Authorities' Response Framework**.

Given the interconnected nature of the global financial system, the impact of operational incidents in one jurisdiction can quickly spill over into another. The FPC supports the UK financial authorities' continued engagement internationally through a range of multilateral and bilateral channels. There is frequent engagement and co-ordination with international authorities on operational resilience issues that transcend borders and benefit from a global approach. For example, through the **Financial Stability Board**, the international standard-setting bodies and the **G7 Cyber Expert Group**. UK authorities have led or contributed to many of the international workstreams delivering policy and analysis related to operational resilience.

3.3: Developing the FPC's approach to assessing operational resilience

> **The operational risk landscape is changing rapidly as a result of the emergence of new threats, technological change, and changes in how the financial system provides vital services.**

The FPC will continue to develop its approach to assessing operational resilience and will regularly review the operational resilience policy toolkit, including with consideration to future operational changes and innovation in the financial system. Consistent with its forward-looking macroprudential approach, the FPC will do this through:

- **assessing potential system-wide gaps in or risks to operational resilience**, which are not adequately covered by firm-level or microprudential policies. This includes considering

implementation by firms and FMIs of the Bank's, the PRA's and the FCA's operational resilience policies, which play an important role in supporting the continued provision of vital services. It also includes monitoring new system-wide gaps or risks that could arise as the financial system continues to evolve;

- **continuing to conduct cyber stress testing** to assess the financial system's ability to absorb and restore functioning following a significant operational incident, and considering stress testing for other possible operational disruptions. Cyber stress testing supports the FPC's work to further its analysis of sources of system-wide disruption and macro vulnerabilities. The next cyber stress test is due to start in Spring 2024 with the findings expected to be published in the first half of 2025;
- **monitoring the implementation and outcomes of the CTP regime**, including the framework underpinning designation decisions taken by HM Treasury, the regulators' new powers to oversee CTPs (such as technology service providers), and actions taken to raise the resilience of the services they provide to firms and FMIs. The FPC's particular focus is on the impact this has on reducing the systemic risks posed by CTPs, including as the financial system continues to evolve; and
- **exploring ways to continue to build system-wide resilience** to operational disruption, including considering whether to set impact tolerances for additional vital services beyond payments.

---

1. As set out in **PS6/21 – Operational resilience: Impact tolerances for important business services**, this includes firms identified by the PRA as other systemically important institutions (O-SIIs) and insurers with gross written premiums exceeding £15 billion or technical provisions exceeding £75 billion, both on a three-year rolling average.
2. This definition includes legal risk but excludes strategic and reputation risk. Bank for International Settlements (2021), **Revisions to the Principles for the Sound Management of Operational Risk**.
3. This includes the **PRA's Supervisory Statement SS1/21**, the **FCA's Policy Statement PS21/3**, the **Bank's policy on operational resilience of FMIs** and relevant PRA rules (for CRR firms, **the Operational Resilience Part of the Rulebook**, and for Solvency II firms, the **Insurance – Operational Resilience Part**).
4. For FMIs the terminology 'extreme but plausible disruption' is used. In practice, this is equivalent to the 'severe but plausible disruption' terminology used for firms.
5. As set out in **PS6/21 – Operational resilience: Impact tolerances for important business services** this includes firms identified by the PRA as other systemically important institutions (O-SIIs) and insurers with gross written premiums exceeding £15 billion or technical provisions exceeding £75 billion, both on a three-year rolling average.
6. Value date refers to the day on which the payment, transfer instruction or other obligation is due, and the associated funds and securities are typically available to the receiving participant.