

Operational resilience in a macroprudential framework

Our Financial Stability Papers are designed to develop new insights into risk management, to promote risk reduction policies, to improve financial crisis management planning or to report on aspects of our systemic financial stability work.

Published on 27 August 2024

Content

Executive summary

1: Introduction

2: Sources of operational incidents

3: Vulnerabilities

- 3.1: Micro (firm-level) vulnerabilities
 - 3.2: Macro (system-level) vulnerabilities
 - 3.3: Multiple vulnerabilities and evolving vulnerabilities over time
-

4: Transmission channels and financial stability impacts

- 4.1: Transmission channels
 - 4.2: Impact on financial stability
 - 4.3: Operational risk as an amplifier of financial risk
-

5: Resilience

- 5.1: Resilience of the financial system to operational incidents
 - 5.2: Firm-level resilience
 - 5.3: System-wide resilience
-

6: Conclusion

Box A: International approaches to building operational resilience

Box B: Literature on operational resilience

Financial Stability Paper No. 50

Rachel Adeney, Adrian Hitchins, Claudia Lane, Harsh Mehta and Alison Quashie^[1]

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 have the potential to create financial stability impacts due to the structure of the financial system, and the behaviour of institutions and other participants.

In March 2024, the Bank of England's (the Bank's) Financial Policy Committee (FPC) published a Financial Stability in Focus on its macroprudential approach to operational resilience. This paper supplements that with further staff analysis and includes supporting detail and additional examples. Its purpose is to further illustrate how financial stability can be impacted by the crystallisation of operational risk.

As previous incidents highlight, operational resilience has become more important to maintaining financial stability, particularly as the financial system has become more digitalised and interconnected. Recent operational incidents include the July 2024 worldwide IT outage caused by a flawed update distributed by CrowdStrike (a cyber-security technology firm), a July 2024 outage at Swift (a global messaging service) impacting wholesale payments in the UK and other countries, as well as cyber-attacks on ICBC Financial Services (a US broker-dealer) and ION (a third-party provider of derivatives clearing services) in November and February 2023 respectively. Looking ahead, the importance of operational resilience will continue to grow as developments in technology play a greater role in the provision of financial services and as business models continue to change.

The FPC's macroprudential approach identifies vulnerabilities and transmission channels that can amplify operational incidents in ways that could impact financial stability. These incidents can stem from a range of sources, including internally in a firm or FMI, from a third-party service provider, or from external shocks. Vulnerabilities are the weaknesses and dependencies that can be exposed in a shock, and they exist at the firm and system level. Firm-level vulnerabilities are specific to the business models or operational arrangements of individual entities. However, vulnerabilities can also exist at the system level. Firms and FMIs can have dependencies on each other, and interact with each other in markets, which means disruption in one can affect the services provided by another (ie they are interconnected). There

can also be a reliance on common technologies across the financial system which means multiple entities can be affected at the same time by a disruption. Transmission channels are the means by which operational incidents can spread across the financial system and lead to potential financial stability impacts.

An operational incident can create financial stability risks by disrupting the provision of vital services. This can either be directly because of the disruption itself, or indirectly through impacts on systemically important institutions or systemically important markets. Vital services include:

- the provision of payment and settlement services;
- intermediating between savers and borrowers (and channelling savings into investment); and
- insuring against and dispersing risk.

Operational disruptions at systemically important institutions or in systemically important financial markets – including via the disruption of material services provided by third-party service providers – can directly affect the ability of the financial system to supply vital services.^[2] 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 to access financing. Importantly, if there is disruption to vital service provision it could undermine confidence in the financial system.

In considering the macroprudential risks, it is important to first take account of the level of operational resilience at firms, FMIs and across the wider financial system. Firm-level resilience can help to reduce the risk of operational incidents occurring, and mitigate the risk of systemic impacts when there is an incident.

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. These regulators in the UK include the Bank, the Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA), and their policies 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.

The operational resilience policies set by the Bank, the PRA and the FCA help to bridge

the gap between firm-level and system-wide operational resilience. Individual firms and FMIs are required to ensure that if there is any disruption to the important business services that they provide, the impact of that does not exceed certain tolerable levels. In the March 2024 Financial Stability in Focus, the FPC set out its expectation that relevant firms^[3] and FMIs should consider the vital services that are important to financial stability when they identify their important business services. More broadly, the FPC said that 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.

But system-level vulnerabilities mean that the resilience of individual firms and FMIs alone may not be sufficient to ensure system-wide resilience. These vulnerabilities include: interconnectedness, complexity and opacity; concentration; correlation and common vulnerabilities; and system-wide dependence on data. These vulnerabilities mean that operational incidents can lead to contagion across the financial system and therefore system-wide policies and tools are needed in addition to firm-level measures.

System-wide operational resilience is supported by other system-wide policies and tools. The FPC has established an expectation for how quickly critical payments should be able to be made following an operational incident (known as the 'FPC's impact tolerance for critical payments')^[4] as well as the incoming regime to raise the resilience of material services provided by critical third parties to firms and FMIs.^[5] The FPC has acted to reduce systemic risks from operational issues through a programme of work, including stress tests, to improve the financial system's resilience to cyber-attacks. System-wide resilience is supported further by the collaborative approach between the UK financial authorities and the financial sector through collective action and wider sector engagement. And given the interconnected nature of the global financial system, the UK authorities engage internationally through a range of multilateral and bilateral channels, including through the Financial Stability Board (FSB), the international standard-setting bodies, and the G7 Cyber Expert Group.

Operational resilience of the financial system is a global challenge and other jurisdictions are also taking action to build resilience (see Box A). The interconnectedness of the financial system across borders means the impact of operational incidents in one jurisdiction can quickly spill over into another. This highlights the importance of ensuring a continued international focus and collaboration on operational resilience and financial stability.

The literature on operational resilience is still developing and has predominantly focused on cyber risks to date (see Box B). Further research considering the broader set of operational risks to financial stability and taking a macroprudential lens would be beneficial.

1: Introduction

The operational resilience of financial firms and financial market infrastructures (FMIs) is increasingly important to financial stability.

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. Firms include financial institutions such as banks, building societies, insurance companies, and investment firms. FMIs include the entities that facilitate the clearing, settlement, and recording of financial transactions, such as central counterparties, payment systems and central securities depositories.

In March 2024, the Bank's Financial Policy Committee published a [Financial Stability in Focus on its macroprudential approach to operational resilience](#). This publication set out how operational disruptions have the potential to create financial stability impacts due to the structure of the financial system, and the behaviour of institutions and other participants within it.

This paper supplements the March 2024 publication with further staff analysis. It includes supporting detail and additional examples. Its purpose is to illustrate how financial stability can be impacted by the crystallisation of operational risk, and how operational resilience at individual firms and FMIs, as well as across the system, can prevent impacts on financial stability.

Operational risk covers a wide range of non-financial risks faced by firms and FMIs. It is defined in the Basel capital framework as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.^[6] The crystallisation of operational risks can be the source of shocks to the wider financial system, or they can make episodes of financial stress worse.

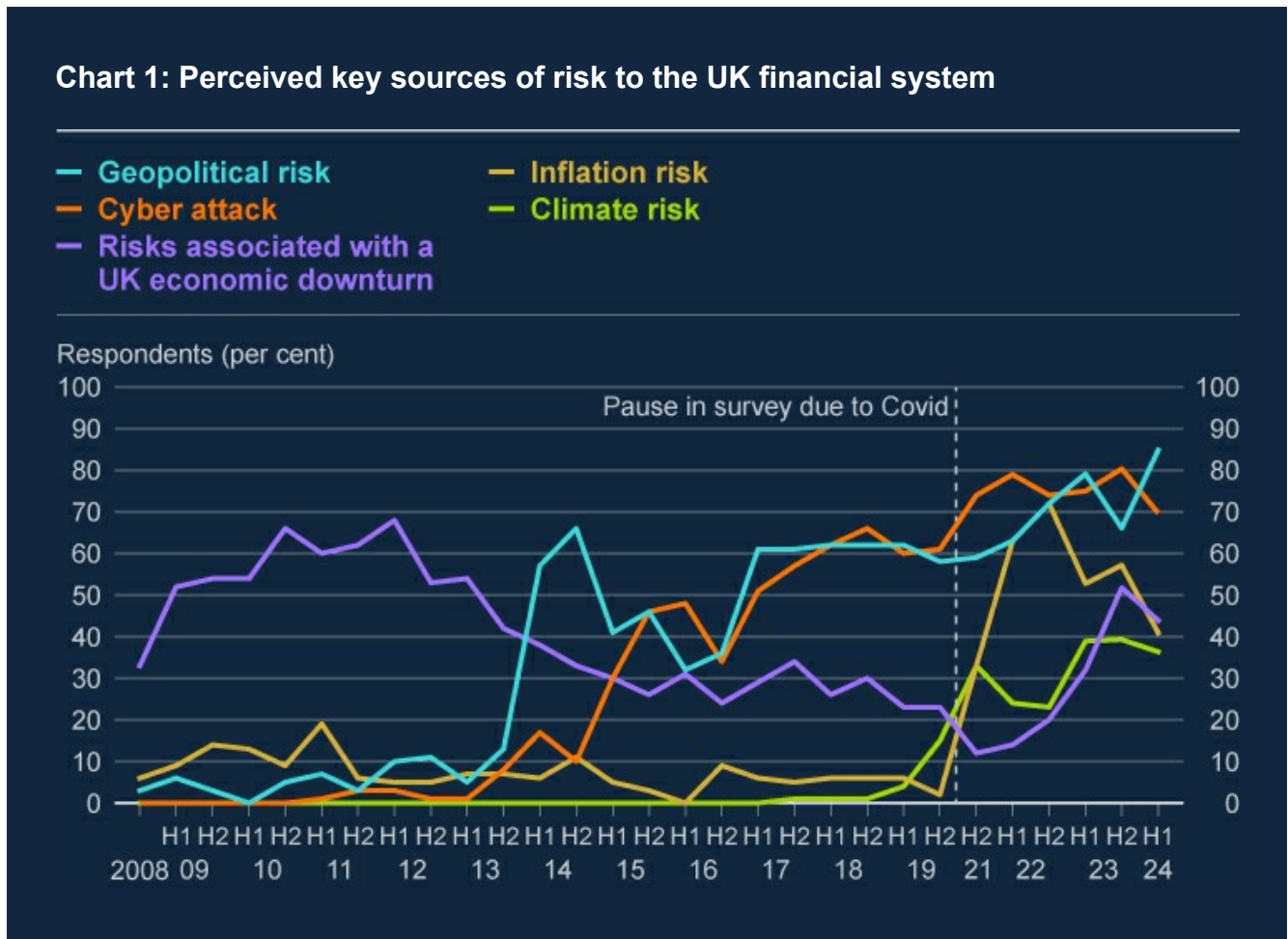
The growing importance of operational resilience reflects an increasingly digitalised and interconnected financial system.

Digitalisation enables the automation of manual processes, which reduces costs for firms and FMIs. It can reduce risks from human error and increasingly sophisticated uses of data can help firms to enhance services and improve approaches to risk management in other ways. Customers benefit as well: new banking and payment services provide them with more information and control over their finances, and bring competition and innovation to the UK banking sector.

But an increasing reliance on digital services means that operational risks can be realised in new ways, and the financial sector's interconnectedness has the potential to spread operational disruption widely and quickly, affecting market participants, including households and businesses.

A greater reliance on digital technology also creates more opportunities for cyber-attacks to

disrupt important services. The National Cyber Security Centre received over 2,000 reports of cyber-attacks in 2023.[7] Cyber-attacks were cited as a risk to financial stability by more than 70% of respondents in each of the Bank’s Systemic Risk Surveys since 2022 (76% on average). Chart 1 shows how perceptions of risk from several sources, including from cyber-attacks, has grown since 2008.



Sources: Bank of England Systemic Risk Surveys and Bank calculations.

Financial services are increasingly facilitated by a wider range of firms as the financial sector has become more disintermediated, creating a high level of interconnectedness across the system. The growth in market-based finance, for example, has shifted the provision of some services away from banks to a multiplicity of highly interconnected, non-bank financial institutions. While in payments, transaction chains are increasingly comprised of more and more firms providing new or specialist services (eg fraud detection services). As activity shifts away from a small number of systemic institutions to a large number of interconnected firms in systemically important markets, the management of risk in these markets becomes 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. But an increasing reliance on third parties poses risks, for example, from concentrations in the provision of services, the importance of third-party services to individual firms' own levels of resilience, a lack of substitutability, and from other concentrations in the third-party provider's own supply chain. Managing such risks is a key objective for firms and FMIs as well as the Bank, PRA and FCA.

Artificial intelligence and machine learning – technology which has been used in financial services for at least a decade, but which is now being applied to more varied uses – may play an enhanced role in financial services in future. Firms and FMIs are exploring the potential of distributed ledger technology to bring efficiencies to financial processes and transactions. This technology originally underpinned the development of crypto markets, but it will likely have applications in the traditional financial system as well. Widespread adoption of distributed ledger technology, or enhanced artificial intelligence technology, by the traditional financial sector has the potential to reshape activity and the structure of the financial system. The adoption of evolving technologies will lead to greater digitalisation, potentially increasing interconnectedness in the system, and creating more third-party dependencies.

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 as a whole needs to be able to continue to provide vital services to households and businesses through severe but plausible operational disruptions, or to be able to recover from such disruption within tolerable limits such that the stability of the financial system is not impacted. 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 to access financing, and this could undermine confidence in the financial system. Through the delivery of their own services, firms, FMIs and markets all contribute to the provision of vital services and a stable financial system.

Table A provides more information on the vital services that have been set out in [The Bank's Financial Stability Strategy](#). And Table A includes 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 date they are due), even in severe stress. The FPC acknowledged 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.[8]

The Bank 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 PRA and FCA published a [consultation paper](#) in December 2023 with proposed requirements and expectations to manage risks posed by CTPs. More information on firm-level and system-wide operational resilience policies and tools is set out in Section 5.

There has also been a growing international focus on building operational resilience with the aim of preventing firm-level incidents from affecting financial stability.

Several high-profile banking failures in the mid-1990s, notably at Daiwa Bank in 1994 and Barings Bank in 1995, highlighted the potential for operational incidents to generate significant

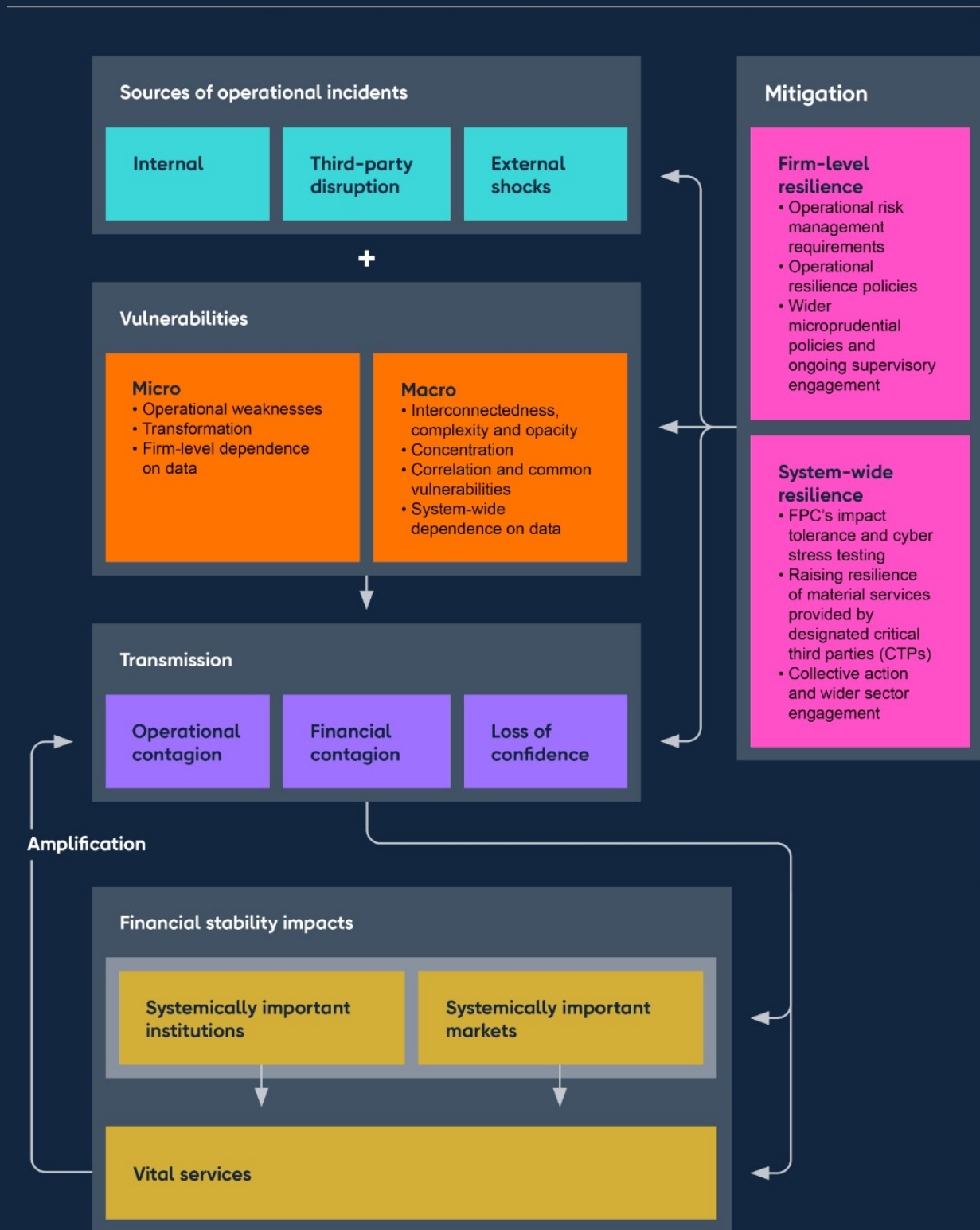
financial losses for firms. This led to the first serious consideration of operational risk as a distinct risk category through the [Basel regulatory framework and rules](#), including via minimum capital requirements. And following events seen through the 2008 global financial crisis and more recently the Covid-19 pandemic, alongside the increased risk of cyber-attacks, there has been a move towards a wider strategic focus on building operational resilience. In particular, an international focus on withstanding, adapting to and recovering from operational disruptions, which can help to prevent firm-level incidents from impacting financial stability. The Bank has led or contributed to many of the international workstreams delivering policy and analysis related to operational resilience. For example, through the [Financial Stability Board \(FSB\)](#), the international standard-setting bodies, and the [G7 Cyber Expert Group](#). A summary of recent work in other jurisdictions can be found in Box A of this paper.

Figure 1 illustrates the FPC’s approach to assessing financial stability risks from potential operational incidents.

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 are the weaknesses and dependencies that can be exposed in a shock, and they exist at the firm and system level. Micro (firm-level) vulnerabilities are inherent to specific business models or operational arrangements. Macro (system-level) vulnerabilities come about because of the underlying structure of the financial system and the collective behaviour, or dependencies, of individual institutions and other participants within it. For example, firms and FMIs can have dependencies on each other, and interact with each other in markets, which means disruption in one can affect the services provided by another. There can also be a reliance on common technologies in the financial system which means multiple entities can be affected at the same time by a single disruption. Transmission channels are the means by which operational incidents can spread across the financial system and lead to potential financial stability impacts. An operational incident can create financial stability risks by disrupting the provision of vital services, either directly, or indirectly through impacts on systemically important institutions or systemically important markets.

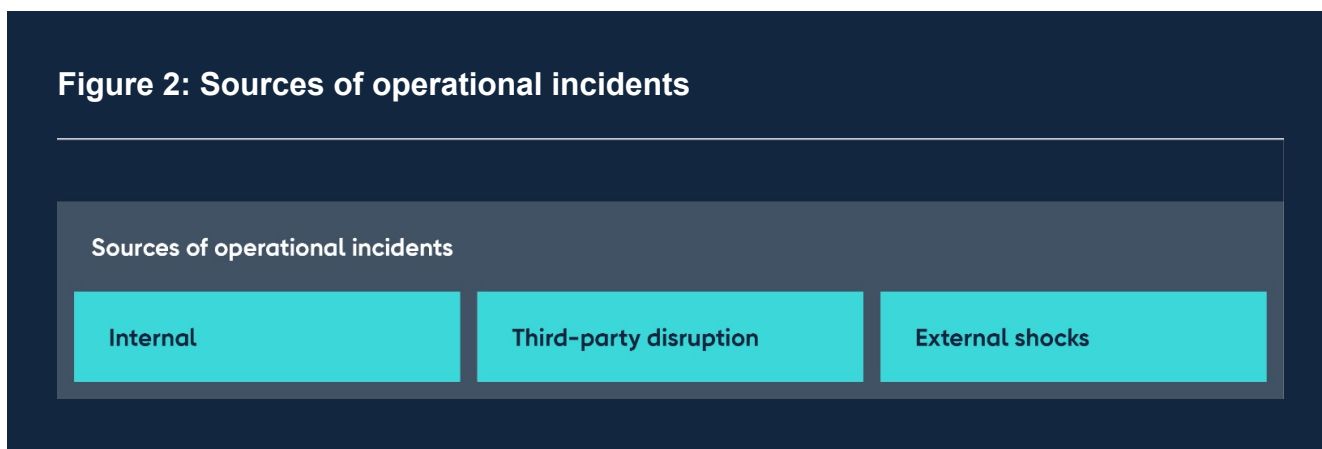
The following sections outline the detail of the FPC’s approach, stepping through the sources (Section 2), vulnerabilities (Section 3), transmission channels and financial stability impacts (Section 4), and resilience policies and tools at firm and system-wide level (Section 5).

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



2: Sources of operational incidents

Figure 2: Sources of operational incidents



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

The sources of operational incidents across the financial system can be split across three categories: 'internal', 'third-party disruption' and 'external shocks' (Table B). Firm-level causes of operational risk have been explored in more detail in taxonomies developed by several organisations and regulatory bodies[9]. It could also be the case that multiple sources trigger an incident, for example if an external shock such as a severe weather event caused disruption at a third party.

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 that are of most relevance from a macroprudential perspective are those with the greatest potential to have system-wide impacts. For

example, incidents that could affect multiple participants in the financial system, like cyber-attacks.

Many operational incidents can be contained and addressed at source 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. Other firm-specific factors that can lead to operational incidents, such as poor culture and weak governance, can also be addressed at the source.

Some operational incidents are more likely to have systemic impacts because of certain features of the financial system, such as its interconnectedness or because the affected firm or market is systemically important. For example, the London Stock Exchange experienced an outage due to a software glitch in 2023 which impacted the trading of many smaller listed companies. While this did not impact financial stability, if the incident was not resolved as promptly as it was, it could have affected the ability of these companies to raise equity finance and had wider effects on market confidence. There have also been operational 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.

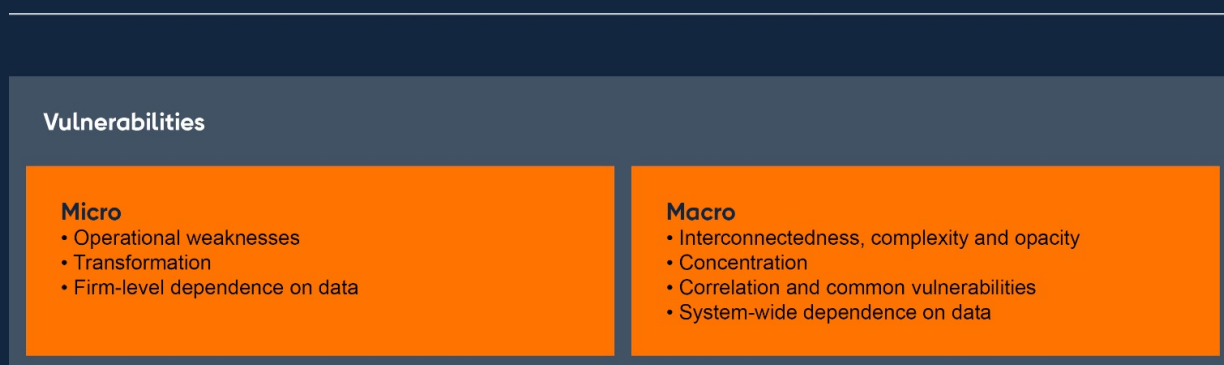
Systemic impacts could also occur where internal disruptions are common across firms, such as functionality issues in commonly used software that impacts multiple firms at the same time. In July 2024, a worldwide IT outage resulted from a flawed software update distributed by CrowdStrike, a cyber security technology firm, which affected computers running Microsoft Windows. While the quick resolution meant it did not risk affecting financial stability and there was no evidence of malicious intent, around 8.5 million devices were affected globally, impacting businesses and institutions in a range of sectors, including UK high street banks and other financial firms.

Cyber-attacks are another source of disruption which can impact multiple firms at the same time. Cyber-attacks are also unique because they can be conducted with malicious intent and be designed and timed for maximum disruption ([Kashyap and Wetherilt \(2019\)](#) ). As a result, macroprudential authorities have tended to prioritise promoting system-wide resilience to cyber-attacks.

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.

3: Vulnerabilities

Figure 3: 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.

Operational incidents can often be idiosyncratic, given that incidents arising from internal sources tend to be related to firm-specific business models and operational arrangements. For this reason, from a regulatory perspective the management of operational risk and resilience has traditionally been considered a firm-specific issue. Individual firms should 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.

However, some threats or shocks, when combined with existing vulnerabilities in the financial system could impact the system more broadly.

An operational incident occurs when a threat, whether intentional or unintentional, from one of the potential sources described above (eg a cyber-attack) interacts with a vulnerability (eg a weakness in a firm's IT system). In the absence of any vulnerabilities to exploit, a threat may not lead to an operational incident. Effective risk management frameworks at firms and FMIs are important because they can help prevent operational incidents from occurring.

Micro vulnerabilities exist at the firm level (Section 3.1) and macro vulnerabilities exist at the system level (Section 3.2). These vulnerabilities can transmit across firms and markets meaning an operational incident at even a single firm can be amplified and impact vital services leading to potential financial stability impacts (Section 4).

3.1: Micro (firm-level) vulnerabilities

Micro vulnerabilities are inherent to specific business models or operational arrangements (Figure 3).

Micro vulnerabilities lead to firm-level disruption, but could lead to system-wide impacts if the incident occurs at a systemically important firm or FMI or in a systemically important financial market (Section 4.2).

‘Operational weaknesses’ include inadequate or failed management of internal processes, people and systems, and a lack of preparedness to third-party disruption and external shocks.

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. These weaknesses can result from a lack of understanding of new and evolving operational risks within firms and FMIs (at various levels 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. The impacts from operational incidents can be mitigated by effective control frameworks and by having sufficient response and recovery capabilities. It is important that firms and FMIs are able to identify the weaknesses in, and threats to, their services.

Systems are vulnerable when they exhibit functionality, performance, or capacity issues, or when there is a lack of maintenance or inadequate testing. While the root causes of system disruption may be small (eg a routine software update), such incidents can lead to outsized impacts. In 2012, an IT incident at RBS, NatWest and Ulster Bank directly affected at least 6.5 million customers, impacting their ability to access their accounts or make payments and impeded the ability of the banks to fully participate in settlement activities.

Several different operational weaknesses may play a part in the occurrence of an operational incident. In the context of cyber risk, successful phishing attacks can reflect poor systems for detecting such emails (a process or system failure) as well as weaknesses in the ability of employees to identify the emails as malicious.

‘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. As outlined in Section 1, digitalisation and automation can reduce vulnerabilities because of reduced manual processing and risks from human error. However, they can also introduce new and potentially unknown risks that come from the increased complexity of financial service delivery.

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.

Despite the risks surrounding transformation, digitalisation and automation play an important role in improving the technological resilience of firms and FMIs. Technological changes can reduce firms' and FMIs' reliance on old infrastructure, manual processes, and legacy expertise, all of which can act as amplifiers during periods of stress. For example, delays caused by manual processing at some custody banks acted as an amplifier during the liability-driven investment (LDI) episode in September 2022 (see Section 4.3).

'Firm-level dependence on data' refers to the fact that available, accurate 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. For example, doubt over information relating to deposit accounts could impact the ability of customers to access their funds. Where firms or FMIs have data that is stored with, or rely on data provided by, third-party suppliers, it is important for firms and FMIs to ensure such data are adequately protected and processes are resilient to disruption given the risk from incidents arising at weaker parts of the supply chain. In January 2024, EquiLend – a global securities trading platform – experienced a ransomware attack which led to an outage in its trading services. This impacted the ability of financial firms that were clients of EquiLend to meet regulatory reporting obligations, and to manage their own risks.

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.

3.2: Macro (system-level) vulnerabilities

Macro vulnerabilities come about because of underlying externalities in the financial system, such as the structure of the financial system and the collective behaviour, or dependencies of, individual institutions and other participants within it (Figure 3).

While operational incidents are most likely to originate in one specific part of the financial system, structural features and the collective behaviour or dependencies 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.

‘Interconnectedness’ of markets and participants in the financial system means operational disruptions in one firm or FMI can have knock-on impacts on others.

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). Interconnections can also arise between firms and FMIs where common third-party technology providers are used, or where firms and FMIs use the same software packages. Such interconnections can be difficult to observe ex ante given the complexity of the financial system.

Business model developments such as Banking-as-a-Service (BaaS) are another form of interconnectedness. BaaS refers to arrangements where banks provide banking services to non-bank intermediaries (such as financial technology companies) that then deliver products and services to end users. While non-banks have distributed certain financial products for some time, new technologies are creating opportunities to increase the scale and complexity of these arrangements.

In the event of an operational disruption, firms will enact their response and recovery plans. This is an important part of ensuring an individual firm’s operational resilience. However, actions taken in the interests of an individual firm could create adverse impacts for the wider financial system. For example, if a firm believes that a third party, or FMI it is connected to, has experienced a cyber-attack, it may take action to disconnect from the system to protect its own systems and data. This disconnection could have potential knock-on impacts to its own customers, other firms and the wider financial system, which could pose a risk to financial stability. Under the operational resilience policies set by the Bank, the PRA and the FCA, relevant firms^[10] should be considering the system-wide implications of their own actions during an operational disruption.

‘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 and settlement of financial instruments 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 importance 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 become single points of failure where there is a lack of viable alternative providers for services, or where there are potential difficulties that firms and FMIs may face when migrating services in a timely manner and without undue risk. For a substitute to be effective, services should be able to be migrated to alternative providers with ease and speed. Impacts from operational incidents may be amplified if a single point of failure leads to an extended outage. The operational resilience policies highlight how substitutability can be important in allowing firms and FMIs to resume their services following disruption.

Substitutability will be an important consideration for the relevant firms required to consider financial stability outcomes.

Real-Time Gross Settlement (RTGS) is the infrastructure that lies at the heart of every payment in the UK and settles over £700 billion on an average day. On 14 August 2023, there was a six-hour disruption to RTGS and CHAPS (the UK's high-value payment system) settlement due to a technical issue. RTGS and CHAPS settlement resumed at lunchtime, following technical recovery, with the backlog of payments cleared by mid-afternoon. On 18 July 2024, there was a four-hour CHAPS settlement outage as a result of a known dependency on the third-party provided Swift Y-


Copy messaging service, which itself was disrupted. In both cases, operational resilience of the system enabled all payments to be settled by the end of the day which was within the impact tolerance set by the FPC for critical payments (see Section 5 for detail on the FPC's impact tolerance). The Bank is continuing to evolve its RTGS/CHAPS Operational Resilience Framework. The Bank is also considering additional ways to connect to RTGS under its [Future Roadmap for RTGS](#), mitigating the reliance on the Swift messaging network.

Measures to address concentration and lack of substitutability in the financial system increase systemic resilience by adding alternative channels for the delivery of financial services that support the provision of vital services. However, there can be costs involved with developing and maintaining substitutes that improve system-wide operational resilience, both financial and in terms of lost efficiency. The balance between efficiency and resilience in the provision of vital services should be considered on a case-by-case basis, including with consideration to financial stability outcomes.

'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. Widespread disruption 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. If there is an operational disruption that is widespread across the financial system, an inability to use planned contingency measures (or use them at expected speeds or capacities) may further amplify the impacts. The [Bank's 2022 cyber stress test](#)  highlighted the importance of firms considering the capacity of fall-back systems in their intended contingency options.

An operational incident that affects confidence could also have systemic impacts if the loss of confidence impacts a wide number of firms or FMIs, or other market participants. The spreading of misinformation or disinformation could further amplify the loss of confidence. A widespread loss of confidence could also be triggered by a series of low-level operational incidents at firms –

whether systemic or non-systemic – or at an FMI.

‘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. There could be widespread impacts if there was disruption to third-party data providers that feed time-sensitive data into systemically important markets. This could lead quickly to a widespread loss of confidence and trigger behavioural choices not to transact in the financial system or other atypical behaviour such as runs or disruptive flights to safety. Difficulty restoring data access and gaining reassurance about the accuracy of data could lengthen recovery time following an operational disruption and further amplify impacts.

Loss of data integrity can be particularly difficult to remedy. The [2022 cyber stress test](#) found that where data were corrupted, making critical payments by the end of value date might not always be possible and might lead to adverse impacts on financial stability. In such instances, alternative mitigating actions might be appropriate (for example providing emergency cash or extending overdrafts in the case of retail payments). The availability of clean data and suitable tools for data reconciliation are important elements of the recovery process where an operational incident involves loss of data integrity. In the event of any kind of operational incident, key services should be resumed safely without loss of data, impairment of data integrity, or causing contagion to the wider financial system.

Data confidentiality and security is also important to the functioning of the financial system. If a data breach – whether accidental or malicious – revealed confidential information about transactions or market positions, it could lead to sharp market moves or a broader loss of confidence. This could be destabilising to the financial system. The development of quantum computing could increase these risks. Quantum computing poses a risk to encryption methods that have been considered secure and could be used to decrypt confidential financial data.

3.3: Multiple vulnerabilities and evolving vulnerabilities over time

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 change over time, and steps to reduce some vulnerabilities may increase others.

The Covid-19 pandemic was an external shock that impacted the ability of the entire financial sector to provide vital services. Firms and FMIs adapted quickly to ensure continuity in their service provision. In some ways this episode has reduced vulnerabilities in the financial sector to operational risk. Firms accelerated their technological rollouts and advanced plans to digitalise their services, including migrating functions to the cloud. These measures have likely lessened operational weaknesses at individual firms. For example, migrating functions to the cloud can provide additional security for data storage. However, a larger number of such change programs could increase opportunities for disruption due to vulnerabilities in firm-level transformation, and as cloud outsourcing has increased across the whole sector, it has created additional concentration in third-party service providers.

Vulnerabilities to operational risks can also build up over time if there is insufficient investment in operational resilience by firms and FMIs. The [thematic findings of the 2022 Cyber Stress Test](#) [↗](#) highlighted the importance of firms and FMIs investing in areas which would enhance their capability to respond and recover from incidents. Investment in suitable mitigants may also be necessary to better manage risks to financial stability during an incident, in particular where it is not possible to restore services before recovery of a third-party (eg where an FMI was disrupted) or where restoring services would be harmful for financial stability.

Operational risk-taking can also build over time, increasing the vulnerability of firms and FMIs to cyclical downturns.

Firms and FMIs can be incentivised to take excessive operational risks during periods of heightened competition or due to moral hazard. Doing so can leave them exposed to potentially large financial losses or causing wider impacts when market conditions change. The mis-selling of PPI in the UK is an example of misconduct that could have occurred in pursuit of higher profits or due to competitive pressure. The combination of regulatory fines and customer compensation claims resulting from these operational failures have led to significant financial costs for many firms.

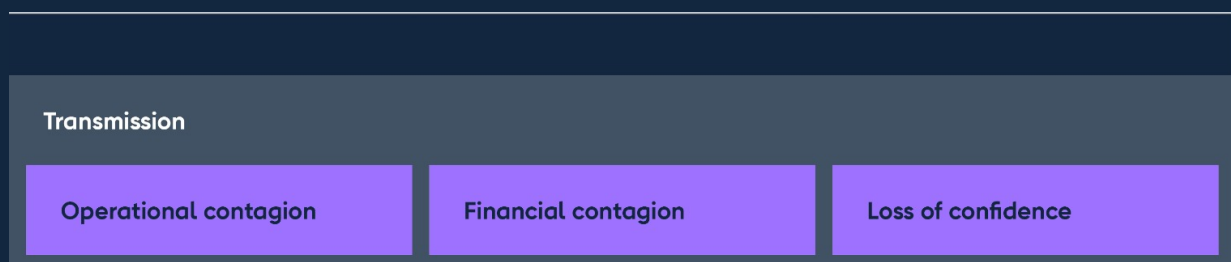
4: Transmission channels and financial stability impacts

An operational incident can have a wider impact across the financial system through operational contagion, financial contagion, or a loss of confidence.

Interdependencies across the financial sector mean that operational disruptions can spread between firms and FMIs. Parts of the financial sector not exposed to the initial disruption can be affected where there are knock-on operational and financial impacts on other firms, FMIs or markets, or where the disruption causes loss of confidence to spread.

4.1: Transmission channels

Figure 4: Transmission channels



Operational contagion occurs when an initial operational disruption causes further operational disruption elsewhere in the financial system or real economy.





Operational contagion can occur because of interdependencies that arise from financial and non-financial activities between firms, and between firms and FMIs. 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 on the ability of the disrupted firm's counterparties to undertake their own activities. This in aggregate could cause wider market disruption if vital services delivered by multiple firms are impacted at the same time. For example, an operational disruption to one firm's ability to make payments will affect the operations of the firms expecting to receive those payments due to corresponding settlement issues. IT and network connections have also created new channels by which operational disruption can spread across the financial system, especially cyber-attacks.

There can also be operational contagion because of deliberate actions taken by firms during a disruption. For example, in the event of a cyber-attack, firms may choose to disconnect

themselves from affected entities to prevent their own systems from becoming corrupted. However, disconnecting could create operational disruption elsewhere in the financial system. For example, in the November 2023 ransomware attack on ICBC Financial Services, the firm disconnected from BNY Mellon. The attack did not spread to other firms, but the disconnection meant that ICBC Financial Services had no access to the electronic settlement platform for US Treasury securities. While the impacts were not widespread, there was some contagion to the clients of ICBC Financial Services as they had to reroute their trades, and there was some backlog of settlements.

Operational contagion could spread beyond the financial sector and lead to disruption in the real economy if households and business are prevented from transacting. This could disrupt the ability of households and businesses to pay for essential goods and services. Further, regulators' ability to monitor risks in markets can be impacted because of operational disruption in the financial system, as was the case in January 2024 when EquiLend experienced a ransomware attack which impacted the ability of market participants to report the lending and borrowing of their securities.

| Financial contagion occurs when operational disruption leads to financial impacts.

Financial contagion across the financial system could happen if an operational disruption impacted 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 which 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, impacts price discovery in certain markets or for particular assets, or if it affects a firm's ability to make margin payments to a central counterparty (CCP), triggering default proceedings ([Ros \(2020\)](#) , and [Brando et al \(2022\)](#) )

The financial impacts associated with operational disruptions include the cost of responding to an incident (such as contracting experts to resolve the issue, or paying compensation), losses (which could arise from a financially motivated cyber-attack, fraud, lost business, or an inability to conduct hedging and trading activities), and financial market impacts (including to funding costs). In the case of banks, the capital framework requires that they have sufficient capital to reflect the risks posed by operational disruptions and to help mitigate the associated losses. 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 firm, or financial losses were widespread across a large number of firms.

Operational disruptions can lead to a loss of confidence in firms or FMIs that has the potential to spread across the system.

Trust is critical to the functioning of the financial system. The [FPC has previously discussed](#) the risk that incidents involving individual banks or firms could be amplified if they lead to a broader shock to confidence among customers, or through interconnections in the financial system. If depositors – whether retail or wholesale – lose confidence, it can trigger run behaviour and potentially lead to firm failure.

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 firm, or the firm's ability to manage its risks and the risks to its business model ([Healey et al \(2021\)](#) [↗](#)). Loss of confidence is particularly relevant to cyber-attacks compared to other operational disruptions, where there can be high levels of uncertainty over the cause of the attack, including the possibility of malicious intent, whether the attack is contained, and what the impacts may ultimately be ([Ros \(2020\)](#) [↗](#)). Indeed, recovery can be complicated by uncertainty over the integrity of data, and this can also contribute to a loss of confidence.

Loss of confidence can be a key transmission channel across the financial system. 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 (as highlighted by the macro vulnerability 'correlation and common vulnerabilities' in Section 3).

Operational and financial contagion can be mitigated with a number of workaround solutions (such as manual processing where automated systems are impaired, or using alternative sources of funding). However, confidence can be difficult to restore once lost. As highlighted in the [thematic findings of the 2022 cyber stress test](#) [↗](#), consistent, effective, and timely communications are important throughout an incident, and can help maintain public confidence. Furthermore, it is important that firms invest in technologies and processes which would enhance their capability to respond to and recover from incidents. Suitable mitigating actions could help to maintain public confidence in the financial system and therefore limit the risk of an incident causing financial instability.

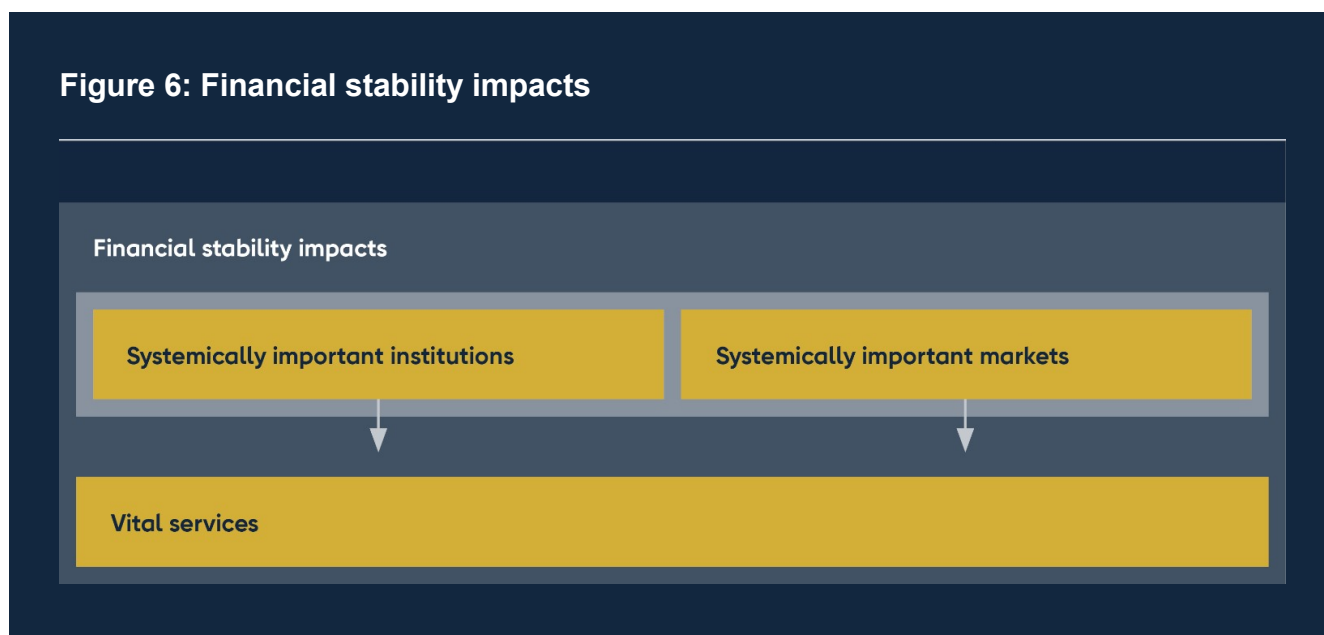
Interaction between the three transmission channels can further amplify impacts.

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, which further amplifies the impacts. For example, financial contagion could have further knock-on impacts to operations or confidence across the financial system. And loss of confidence could

trigger knock-on financial or operational impacts.

4.2: Impact on financial stability

Figure 6: Financial stability impacts



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

As set out in Section 1, the vital services provided by the financial system are: the provision of payment and settlement services; intermediating between savers and borrowers (channelling savings into investment); and insuring against and dispersing risk. 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 to access financing. Through the delivery of their own services, firms, FMIs and markets all contribute to the provision of vital services and a stable financial system.

Systemically important firms and FMIs are those that, if disrupted, could impair parts of the financial system and have potential serious negative consequences for the real economy. This is due to their size, level of substitutability, interconnectedness and 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 business, enabling activity in the real economy. The impacts from disruptions to payment and settlement services are often quickly felt and, as such, there is sensitivity to 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 failed to process correctly, around half of which were transactions initiated on UK-issued cards.

The impacts on customers' ability to transact – particularly given the timing of the disruption over a Friday afternoon and evening when transactions may be higher – 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 of the disruption.

Disruption to systemically important markets can impact the provision of vital services in a number of ways.

Systemically important financial markets are those that provide financing or other important services to the real economy, and which cannot be easily substituted. Disruption in systemically important markets could affect the provision of vital services, for example, by disrupting intermediation between savers and borrowers (for example, in equity and bond markets) and risk sharing (for example, in derivatives markets).

There can be an interdependence between systemically important firms and markets which is important to the provision of vital services. Systemically important firms 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 to function well. Such interdependence means the operational resilience of each participant in a systemically important market contributes to the operational resilience of the whole market.

For example, government bond markets across jurisdictions (eg the US Treasury market, the Japanese Government Bond market, or the gilt market in the UK) play key roles in supporting government financing and the provision of high-quality and liquid collateral. Market pricing of government bonds also serve as a benchmark for the cost of borrowing and the pricing of other financial instruments. Government bond markets typically have strong interconnections with related repo and futures markets.

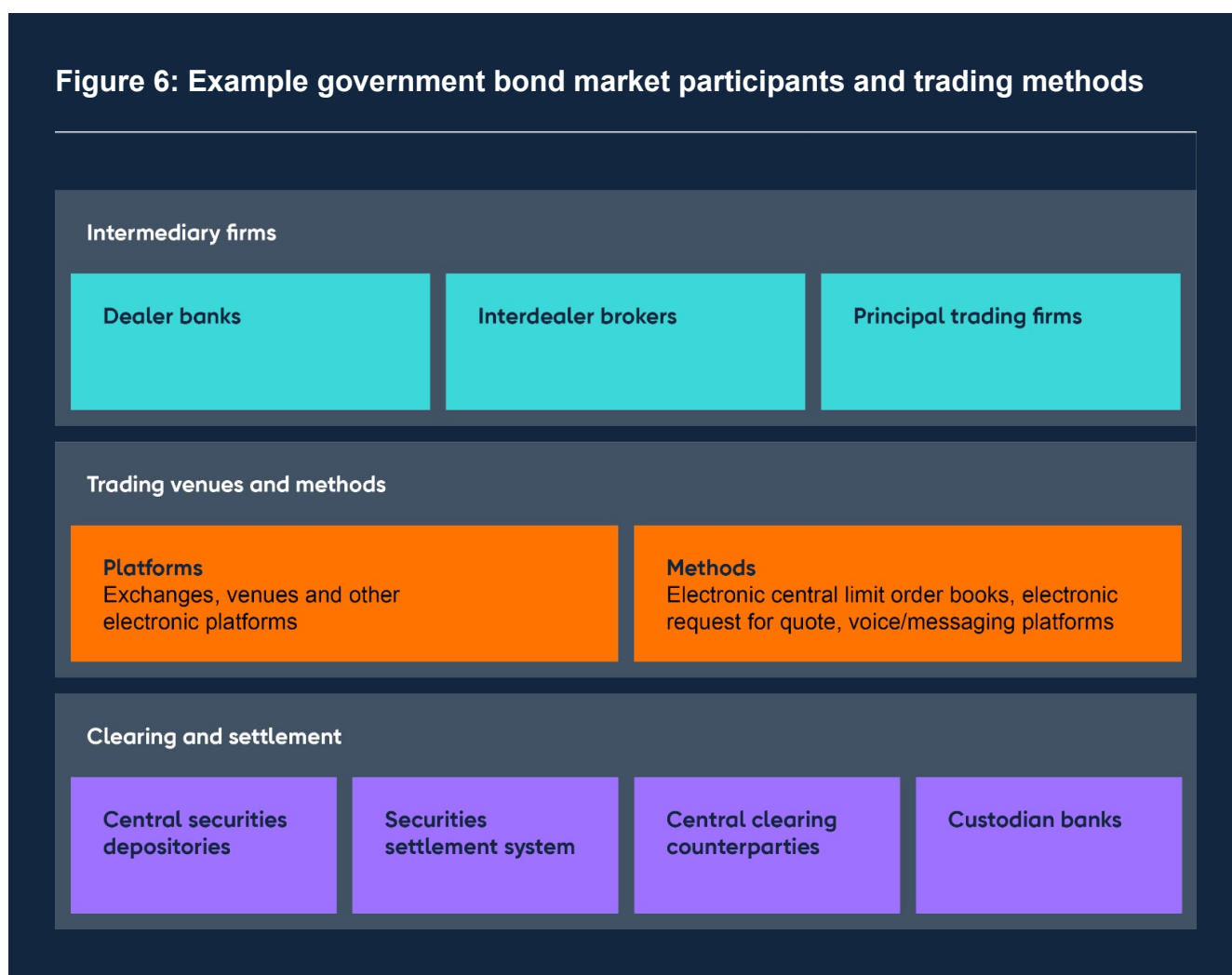
Within these markets, firms and FMIs operate to provide a range of services to market participants, including market intermediation, trade execution, clearing and settlement. In aggregate, their services are essential for the efficient functioning of these systemically important markets and they contribute to the provision of vital services to the real economy. Market structures vary significantly from jurisdiction to jurisdiction but examples of important firms, FMIs and trading platforms operating in these markets are set out below (and in Figure 6):

- Intermediary firms: including dealer banks, interdealer brokers, principal trading firms and other liquidity providers. Dealer banks, which are usually systemically important firms, are active across cash, repo, and futures markets. Along with other firms (depending on jurisdiction), they play a crucial role in providing liquidity via secondary market making activities, including in government bonds.
- Trading platforms: including exchanges, trading venues, and other platforms which can operate via electronic central limit order books, electronic request for quote and other trading protocols, as well as voice and messaging platforms. There are a range of trading venues and

platforms used across jurisdictions to facilitate trading in different market segments with varying levels of market share.

- Clearing and settlement firms and FMIs: including central securities depositories, securities settlement systems, custodian banks and central clearing counterparties. Clearing arrangements in government bond cash and repo markets vary across jurisdictions and levels of central clearing are idiosyncratic to jurisdiction. In futures markets, trades are centrally cleared across jurisdictions. In some jurisdictions dealer banks facilitate client access to CCPs.

Figure 6: Example government bond market participants and trading methods



In addition to interconnectedness, complexity and opacity, the presence of other macro vulnerabilities could lead to operational incidents affecting firms and FMIs to have wider impacts on the provision of vital services and financial stability. For instance, in some jurisdictions there is concentration in services provided by systemically important firms which intermediate between buyers and sellers. And trading and data platforms can be critical nodes in the execution of these activities.

While it is important to note that the role of FMIs can (through their design, rules, procedures, and

operations) reduce risk in financial markets, in many cases market participants have few, if any, practicable alternatives to using these infrastructures. Operational failure could therefore lead to systemic disruption and financial stability risk, highlighting the importance of operational resilience. In addition to efforts in the UK, there is ongoing international action to address vulnerabilities and improve operational resilience (see Box A).

Vital services can also be disrupted if there is disruption to non-systemic firms that is widespread or collectively undermines confidence in the broader system.

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 impairment 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.

In general, the faster an operational incident is resolved, the smaller the impacts are likely to be. For example, the consequences of being unable to make payments – such as firms' access to liquidity or the payment of salaries – are likely to compound and spread further through the financial system and real economy the longer an outage persists.

In addition, confidence is more likely to be lost if an operational disruption is prolonged or if service restoration takes longer than expected. This could occur if rumours have more time to spread, or due to a general loss of confidence in the ability of firms to manage their operational risks. Uncertainty – including about the cause of an incident (especially if it could plausibly be a cyber-attack), how widespread the impacts might be, and how long it will take to resolve the incident – may in itself trigger a loss of confidence.

4.3: Operational risk as an amplifier of financial risk

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

The **LDI incident in September 2022** is a key example of a period of financial instability where operational issues amplified the initial financial stress. UK government bond yields increased significantly over a short period: 30-year gilt yields rose by over 120 basis points in three days. This episode demonstrated that levels of resilience across LDI funds to the speed and scale of moves in gilt yields were insufficient.

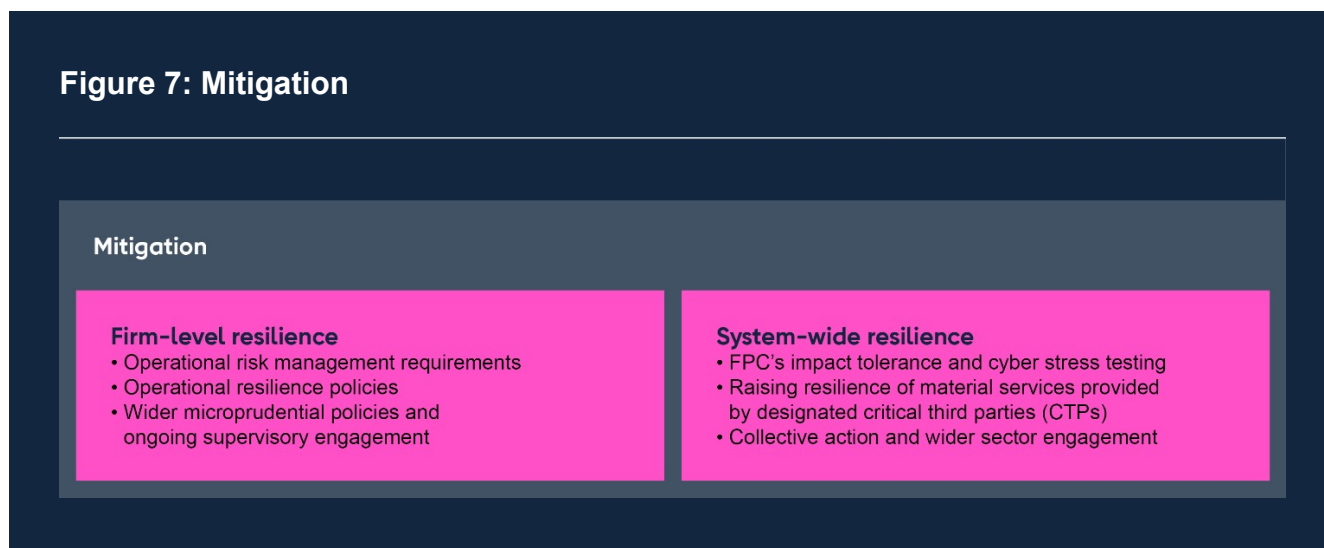
During this episode of market volatility, the replenishment of LDI funds' liquidity buffers was hindered by firms' operational arrangements, and in some cases by the governance processes at pension schemes, exacerbating their liquidity issues and need to sell assets in stressed conditions. In addition, 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 small 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. The **FPC recommended** in March 2023 that the Pensions Regulator take action as soon as possible to mitigate financial stability risks by specifying the minimum levels of resilience for the LDI funds in which pension scheme trustees may invest. As part of an appropriate steady-state minimum level of resilience, the FPC judged that pension schemes might need to improve their operational processes to provide collateral to their LDI funds more swiftly when needed, among other things. **The FCA has also published guidance on enhancing resilience in the LDI sector** [↗](#), including giving special consideration to operational arrangements.

The LDI incident illustrated how, when hit by a shock, vulnerabilities can combine to create financial stability risks. Micro vulnerabilities were present in operational weaknesses (delays from manual processing and governance) and macro vulnerabilities acted as an amplifier in the form of interconnectedness and common vulnerabilities across many pooled funds.

5: Resilience

Figure 7: Mitigation

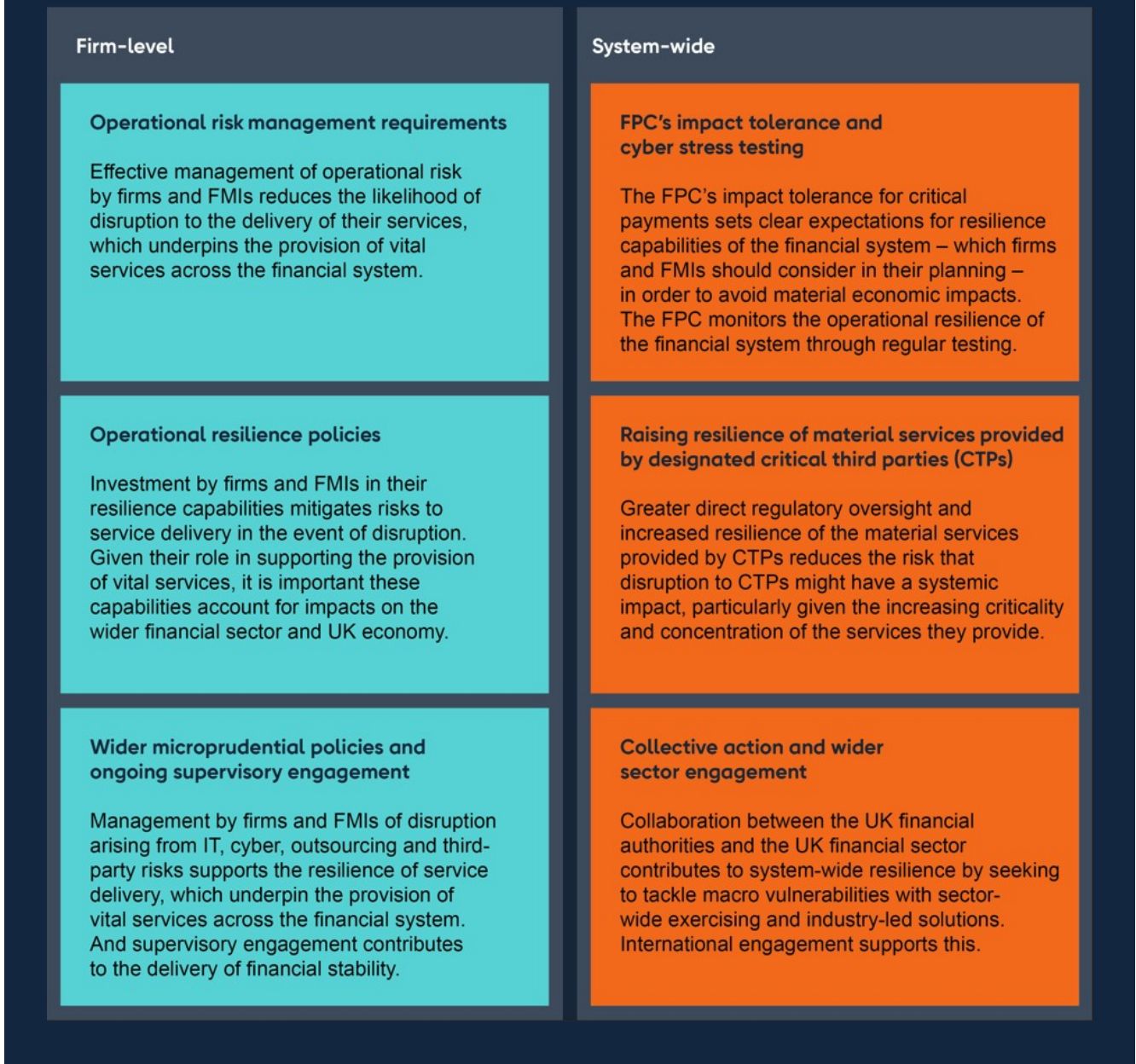


5.1: Resilience of the financial system to operational incidents

When individual firms, FMIs, and the wider financial system are resilient, the risk of threats to the provision of 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.

As set out in Figure 8, 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.^[11] 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.

Figure 8: Firm-level and system-wide policies both contribute to the operational resilience of the financial system



5.2: Firm-level resilience

Firm-level operational resilience provides the foundation for operational resilience across the system.

Operational resilience is essential to the ability of firms and FMIs to function, and to their ability to mitigate risks to their own viability. Firms and FMIs will seek to ensure continuity of service provision, including by responding effectively to operational incidents, making adjustments to processes and systems to mitigate operational weaknesses, and by responding to changes in the wider financial system.

As shown in Figure 8, firms and FMIs are building operational resilience through the application of operational risk management requirements, the implementation of operational resilience policies and wider microprudential policies, and through ongoing supervisory engagement. Specifically, 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 crystallising 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.

Building firm-level operational resilience in such ways helps to address the micro vulnerabilities that are specific to individual firms and FMIs. For example, good operational risk management can prevent the occurrence of incidents due to operational weaknesses, and robust planning can reduce the risk of disruption from large-scale transformation projects.

The operational resilience policies set by the Bank, the PRA and the FCA outlined clear expectations for firms and FMIs to demonstrate resilience capabilities in the event of a severe/extreme but plausible disruption scenario. 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.^[12]

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.^[13] 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.

Disruption from firm-level incidents can be amplified and transmitted across the system, potentially resulting in financial stability impacts. For this reason, firm-level resilience supports system-wide operational resilience. 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

FMI can also limit contagion across the system when operational incidents occur, maintaining confidence in the financial system.

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

Under the operational resilience policies set by the Bank, the PRA and the FCA, relevant firms^[14] 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 FPC published its [macroprudential approach to operational resilience](#) in March 2024. In that publication, the FPC set out its expectation that relevant firms 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. More broadly, the FPC said that 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.

5.3: System-wide resilience

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

These vulnerabilities arise from externalities like the structure of the financial system and the collective behaviour of individual institutions and other participants. Macro vulnerabilities can amplify operational shocks in ways that can impact financial stability. Given this, there is a need for system-wide policies and tools, in addition to firm-level measures (see Figure 8).

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, unless doing so could have a more adverse impact on financial stability than failing to make the value date. 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 in both wholesale and retail scenarios. Cyber stress testing considers potential financial stability impacts, helps to build an understanding of individual firms' and the financial system's operational capacity to absorb the impact of a significant operational incident, such as a cyber-attack, and the ability of firms and FMIs to restore functioning of services after such an incident. The tests also explore how the operational, financial and confidence impacts of a disruption could impact financial stability.

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

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.

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, and 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.

6: Conclusion

Operational incidents can impact the stability of the financial system because system-level vulnerabilities and transmission channels have the potential to amplify the impacts of initial disruption.

These system-level vulnerabilities – interconnectedness, complexity and opacity; concentration; correlation and common vulnerabilities; and system-wide dependence on data – encompass risks in the financial system that go beyond the sum of the risks posed by individual firms and FMI. System-level vulnerabilities and the three transmission channels identified – operational contagion, financial contagion, and loss of confidence – can amplify the effects of operational incidents across the financial system and disrupt the provision of vital services.

The financial stability risks from operational incidents can be reduced by mitigating system-level vulnerabilities and transmission channels. Nevertheless, it is important that operational resilience is strong across each part of the financial system as firm-level resilience is an essential foundation to resilience across the system.

As set out in the March 2024 Financial Stability in Focus, 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, which aims to mitigate system-level vulnerabilities and identify potential transmission channels, the FPC will do this through:

- Assessing potential system-level gaps in, or risks to, operational resilience, which are not adequately covered by firm-level or microprudential policies.
- Continuing cyber stress testing, and considering stress testing for other possible operational disruptions. The next cyber stress test began 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.
- Considering whether to set impact tolerances for additional vital services beyond payments.

Operational resilience in the financial system is a global issue and other jurisdictions are also taking action to build resilience (see Box A). The interconnectedness of the financial system across borders means the impact of operational incidents in one jurisdiction can quickly spill over into another. This highlights the importance of ensuring a continued international focus and collaboration on operational resilience and financial stability. With this in mind, further analysis of gaps between policy frameworks across jurisdictions would help identify risks of cross-border spillover effects.

Operational resilience is a relatively new field in financial stability research, particularly when compared to research into financial resilience. Further research that considers a broad set of operational risks to financial stability through a macroprudential lens would be beneficial.

Box B outlines some of the literature on operational resilience, which is still developing. There has been a lot of recent attention on cyber risk and how disruption from cyber-attacks could spread across the financial system. Research into potential system-wide impacts from a wider range of potential sources of operational disruption would be valuable.

Research is also crucial for understanding potential operational risks that arise from the application of new or evolving technologies across the financial system, including artificial intelligence, distributed ledger technology and quantum computing. These technologies have the potential to increase efficiencies and improve decision-making, but they also pose risks if innovation is not fostered safely. Further research into operational risks to financial stability posed by new and developing technologies would support efforts taking place globally by financial authorities to identify, mitigate and manage risks from such technologies, in order to support the resilience and stability of the financial system as it continues to evolve.

Box A: International approaches to building operational resilience

Operational resilience in the financial system is a global issue and other jurisdictions are also taking action to build resilience.

A number of overseas financial authorities are also taking action on operational resilience in their jurisdictions, as highlighted by [Prenio and Restoy \(2022\)](#).^[14] In line with the UK's focus on microprudential policies aimed at building operational resilience, the US and the European Union (EU) have put in place policies to ensure operational resilience at the firm level.

- In the US, [the Sound Practices to Strengthen Operational Resilience](#)^[15] outlines practices drawn from existing regulations and guidance to increase operational resilience for large banks. A cybersecurity focus supplements this through the [Computer-Security Incident Notification Requirements](#)^[16] for banking organisations and their third-party service providers. And work has progressed to assess the benefits and challenges associated with cloud service adoption in the financial sector.^[15]
- In the EU, the [Digital Operational Resilience Act \(DORA\)](#)^[17] sets out the requirements on financial institutions and critical third parties to withstand, respond to and recover from all types of information communication technologies (ICT)-related disruptions and threats. DORA will apply from January 2025.

A common feature across these jurisdictions is the intention of the firm-level policies to also support and provide a foundation to system-wide operational resilience, including through mitigating the risks posed by the services provided by third-party service providers. Cyber security has also been a key area of focus in these jurisdictions and is increasing in importance given heightened geopolitical risks and the rise in ransomware attacks on financial firms. The European Systemic Risk Board (ESRB), for example, published several reports on systemic risks from cyber-attacks and most recently a report setting out policy tools for cyber resilience. At a system-wide level, building on the UK's approach to stress testing, other jurisdictions are also progressing operational disruption-focused stress tests, for example the European Central Bank's (ECB's) 2024 cyber resilience stress test.^[16]

In recent years, enhancing operational resilience has risen up the global policy agenda across a range of international fora.

Amid digital transformation, increased dependencies on third-party service providers and geopolitical tensions, a range of multilateral organisations and standard-setting bodies are focusing on issues relating to operational resilience. These international efforts seek to strengthen the operational resilience of firms, FMI, and the financial system as a whole, reduce fragmentation and promote interoperability in regulatory and supervisory approaches across jurisdictions and sectors. They are also intended to facilitate international co-ordination and co-operation.

The Bank actively participates in these international fora, in particular as Chair of the FSB's Standing Committee for Supervisory and Regulatory Cooperation, co-Chair of the G7 Cyber Expert Group, and as leads and contributors to a range of workstreams related to operational resilience in the FSB, standard-setting bodies and beyond. As highlighted in the FPC's macroprudential approach to operational resilience, the FPC supports the UK financial authorities' continued engagement in international discussions and workstreams, as well as bilateral engagement with international financial authorities.

Enhancing cyber and operational resilience has been a key focus in the FSB's work programme. This includes the publication of [recommendations to promote convergence in cyber incident reporting](#) in April 2023, the publication of a [toolkit to enhance third-party risk management and oversight](#) in December 2023, as well as ongoing work to design a common format for incident reporting exchange (FIRE) planned for consultation in 2024.^[17]

The Basel Committee on Banking Supervision (BCBS) published [Principles for Operational Resilience](#) in 2021 to promote a principles-based approach to improving operational resilience. This aims to strengthen banks' ability to withstand operational risk events capable of causing large-scale disruption. The BCBS is also developing updated supervisory principles on banks' outsourcing practices and reliance on third and fourth-party service providers.^[18] The International Organization of Securities (IOSCO) published a set of updated [Principles on Outsourcing](#) in 2021 for regulated firms in the securities markets. The Committee on Payments and Market Infrastructures (CPMI) and the IOSCO also issued [guidance to FMIs on cyber resilience](#) in 2016. Moreover, the G7 Cyber Expert Group considers cyber security issues in the financial sector, and since 2016 it has issued a series of 'Fundamental Elements' on key issues relating to cyber resilience, such as, ransomware resilience and third party cyber risk management.^[19]

Given the interconnectedness of the financial system across borders, the impact of operational incidents in one jurisdiction can quickly spill over into another, which highlights the importance of ensuring a continued international focus and collaboration on operational resilience and financial stability.

Box B: Literature on operational resilience

The literature on operational resilience is still developing and has predominantly focused on cyber risks. Further research considering the broader set of operational risks to financial stability and taking a macroprudential lens would be beneficial.

The literature on operational resilience is new and still developing, particularly when compared to the work that exists on financial risks and resilience at a system level. The work to date has tended to focus mainly on the implications of operational risks from a micro perspective. For instance, [Berger et al \(2022\)](#) ^[20] note the absence of studies in the academic literature directly testing the link between operational and systemic risk. A key challenge facing researchers is the limited scope to draw on good-quality data needed for the analysis.^[20]




There has been recent attention towards considering the system-wide angle to operational issues, although the focus has primarily been on cyber risks.^[21] Several papers have developed frameworks that consider the amplification of cyber shocks across the financial system. [Ros \(2020\)](#) ^[21] highlighted several characteristics unique to cyber incidents – intent, scale and speed – that can amplify impacts across the system. While [Healey et al \(2021\)](#) ^[22] emphasise the role of different cyber and financial risks and vulnerabilities that can amplify or dampen transmission channels. [Brando et al \(2022\)](#) ^[23] note the role of firm-level and system-level vulnerabilities that lead to a cyber event affecting financial stability, while the ECB publication on [framework for assessing systemic cyber risk](#) ^[24] highlights the role that systemic entities and interconnections between several non-systemic entities can play, as well as heightened uncertainty. The ESRB proposes mitigants, including effective incident coordination and appropriate macroprudential tools in its [paper on systemic cyber risk](#) ^[25].


Several papers explore the impacts of operational risks and cyber-attacks. [Berger et al \(2022\)](#) ^[26] find evidence corroborating that operational risk can threaten financial stability; [Bouveret \(2018\)](#) ^[27] find average losses from cyber-attacks to be 9% to 26% of banks' net income, with contagion effects increasing these by a fifth; while [Kotidis and Schreft \(2022\)](#) ^[28] explore the effects of a multi-day cyber-attack on a technology service provider used by banks.

1. The authors would like to thank Yuliya Baranova, Nathanaël Benjamin, Sarah Breeden, Roisin Brennan, Omer Bugarinovic, Dan Clements, Orlando Fernandez Ruiz, Lee Foulger, Bernat Gual-Ricart, Carl Gunvaldsen, Andrew Huddart, Andrew John, Wai Keong Lock, Amy Lee, Sam Leighton, Matt Lloyd, Owen Lock, Joanna Lourenco, James Manchester, Maighread McCloskey, John Mears, Natan Misak, Jus Naylor-Smith, Rachele Negro, Gianandrea Padovani, Matt Roberts-Sklar, Greg Ros, Oscar Spencer, Helen Stone, Julia Tennant, Tryfonas Theophilou, Sarah Venables, Sharon Wallis, Andrew Walters, and Ben Westwood for their helpful input and comments to this paper and the Financial Stability in Focus.
2. The FPC has published its approach to assessing risks in market-based finance in its October 2023 [Financial Stability in Focus](#), which identifies weaknesses in operational processes and risk management as a vulnerability.
3. 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.
4. The FPC has set 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 in severe but plausible scenarios. See Section 5.3 and [Record of the Financial Policy Committee meeting – 23 March 2023](#).
5. [CP26/23 – Operational resilience: Critical third parties to the UK financial sector](#).
6. 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](#).
7. [NCSC Annual Review 2023](#).
8. [Record of the Financial Policy Committee meeting – 23 March 2023](#).
9. Some examples include: [ORX Operational Risk Reference Taxonomy](#); [FSB Cyber Lexicon](#), [FSB Format for Incident Reporting Exchange \(FIRE\)](#); and [Improving Data for Managing Cyber Risk and Building Resilience](#).
10. 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.
11. For an overview of how the Bank works with the financial sector to improve operational resilience, including official guidance, see: [Operational resilience of the financial sector](#).
12. 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.
13. In December 2023, the Bank published thematic findings from the latest cycle of CBEST assessments on participating banks, insurers, asset and investment managers, and FMIs: [2023 CBEST thematic](#).
14. 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.
15. [US Treasury Report on the Opportunities and Challenges Facing Financial Sector Cloud-Based Technology Adoption](#).
16. [ECB to stress test banks’ ability to recover from cyberattack](#).
17. [FSB Work Programme for 2024](#).
18. [Basel Committee work programme and strategic priorities for 2023/24](#). In July 2024, the BCBS published a consultative document proposing principles for the sound management of third-party risk in the banking sector:

[Principles for the sound management of third-party risk](#) .

19. [G7 Cyber Expert Group: Fundamental Elements series](#) .

20. [Improving Data for Managing Cyber Risk and Building Resilience](#) ; [Cyber Risk and Financial Stability: It's a Small World After All](#) ; [Towards a framework for assessing systemic cyber risk.](#) .

21. [Could a cyber-attack cause a systemic impact in the financial sector?; IMF GFSR April 2024 Chapter 3: Cyber Risk: A Growing Concern for Macrofinancial Stability](#) .