



BANK OF ENGLAND



Discussion Paper

Building the UK financial sector's operational resilience

- | Bank of England DP01/18
- | Prudential Regulation Authority (PRA) DP01/18
- | Financial Conduct Authority (FCA) DP18/04

July 2018

Bank of England
Threadneedle St,
London EC2R 8AH

Financial Conduct Authority
25 The North Colonnade
Canary Wharf
London E14 5HS



BANK OF ENGLAND



Discussion Paper | Bank of England DP01/18
| PRA DP01/18
| FCA DP18/04

Building the UK financial sector's operational resilience

July 2018

By responding to this discussion paper, you provide personal data to the Bank of England and the Financial Conduct Authority (FCA) ('we' or 'us'). This may include your name, contact details (including, if provided, details of the organisation you work for), and opinions or details offered in the response itself.

The response will be assessed to inform our work as regulators, and a central bank, both in the public interest and in the exercise of our official authority. We may use your details to contact you to clarify any aspects of your response.

The discussion paper will explain if responses will be shared with other organisations. If this is the case, the other organisation will also review the responses and may also contact you to clarify aspects of your response. We will retain all responses for the period that is relevant to supporting ongoing regulatory policy developments and reviews.

Please indicate if you regard all, or some of, the information you provide as confidential.

If we receive a request for disclosure of this information, we will take your indication(s) into account, but cannot give an assurance that confidentiality can be maintained in all circumstances.

Information provided in response to this discussion paper, including personal information, may be subject to publication or release to other parties or to disclosure, in accordance with access to information regimes under the Freedom of Information Act 2000 or the General Data Protection Regulation or the Data Protection Act 2018 or otherwise as required by law or in discharge of our statutory functions.

An automatic confidentiality disclaimer generated by your IT system on emails will not, of itself, be regarded as binding on us.

To find out more about how the Bank of England deals with your personal data, your rights or to get in touch please visit www.bankofengland.co.uk/privacy. To find out more about how the FCA deals with your personal data please visit www.fca.org.uk/privacy.

Responses are requested by Friday 5 October 2018.

Please address any comments or enquiries to:

Jack Armstrong (Bank of England), Jon Newton (PRA) and Chris Walmsley (FCA)

Bank of England

Threadneedle Street

London, EC2R 8AH

Email: DP1_18@bankofengland.co.uk

Foreword

This discussion paper focuses on the operational resilience of the financial system and the individual firms and financial market infrastructures (FMIs) within it. The UK authorities' collaboration on this paper reflects the interconnectedness of the financial system and a shared interest in the opportunities and threats posed by developments in technology.

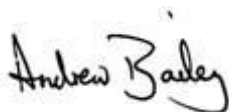
Operational disruption can impact financial stability, threaten the viability of individual firms and FMIs, or cause harm to consumers and other market participants in the financial system. Firms and FMIs need to consider all of these risks when assessing the appropriate levels of resilience within their respective businesses.

Dealing with cyber risk is one important element of operational resilience. But this paper sets out a broader approach, which addresses how the continuity of the services that firms and FMIs provide might be maintained regardless of the cause of disruption.

A resilient financial system is one that can absorb shocks rather than contribute to them. The financial sector needs an approach to operational risk management that includes preventative measures and the capabilities – in terms of people, processes and organisational culture – to adapt and recover when things go wrong. As recent high-profile disruptive events have shown, the speed and effectiveness of communications with the people most affected, including customers, is an important part of any firm's or FMI's overall response to an operational disruption.

The global and interconnected nature of financial activity makes international engagement critically important. There is not currently an international framework supporting the regulation of financial services' operational resilience, so we will share our insights with the global regulatory community.

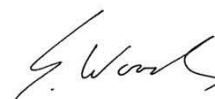
This discussion paper seeks to commence a dialogue with the financial services industry on achieving a step change in the operational resilience of firms and FMIs. We aim to generate debate about the expectations regulators and the wider public might have of the operational resilience of our financial services institutions. We hope to receive feedback from a broad range of stakeholders and look forward to receiving your responses.



Andrew Bailey
Chief Executive,
Financial Conduct Authority



Jon Cunliffe
Deputy Governor, Financial Stability
Bank of England



Sam Woods
Deputy Governor, Prudential Regulation
and Chief Executive of the Prudential
Regulation Authority

Contents

1	Introduction	5
2	Operational resilience of business services	10
3	Operational resilience and the FPC	13
4	Operational resilience of firms and FMIs	16
5	Clear outcomes for operational resilience	28
6	Supervisory assessment of operational resilience	31
7	Conclusion	34
8	Feedback and questions	36
	Annexes	37

1 Introduction

1.1 This discussion paper (DP) is issued jointly by the Prudential Regulation Authority (PRA), the Financial Conduct Authority (FCA), and the Bank of England (the Bank) in its capacity of supervising financial market infrastructures (FMIs), (collectively 'the supervisory authorities'). The purpose of this DP is to share the supervisory authorities’ thinking regarding operational resilience and obtain feedback. Feedback is welcomed from all parts of the financial sector, as well as from consumers, market participants and other stakeholders, including other regulatory organisations.

1.2 UK banks, building societies, credit unions, insurers, overseas UK deposit takers with PRA regulated activity permissions, PRA regulated investment firms, FCA authorised and recognised entities¹ (collectively ‘firms’), and the FMIs supervised by the Bank of England (recognised payment systems, specified service providers, central securities depositories and central counterparties) may be particularly interested in responding, as any future policy may be directly applicable to them.

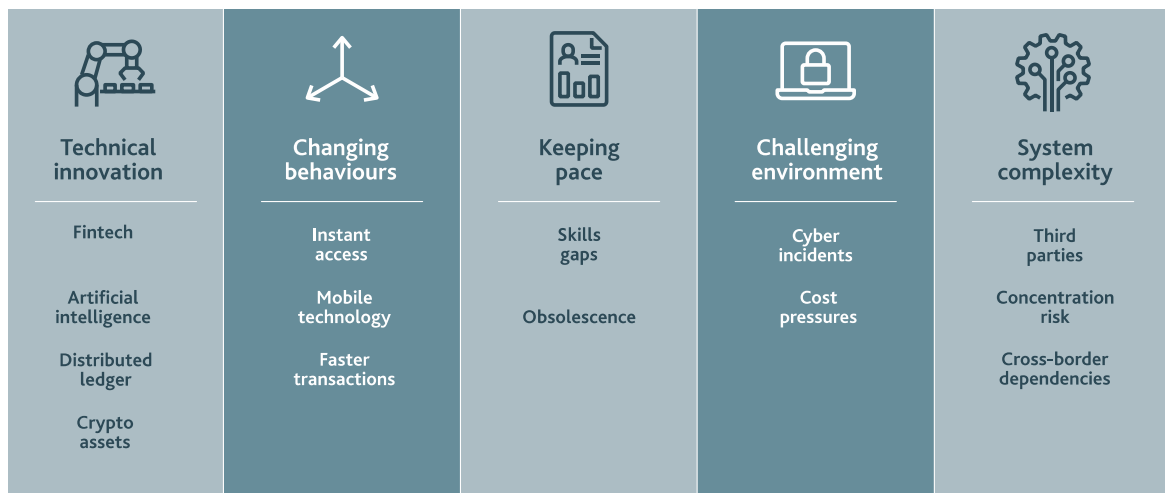
1.3 Feedback is encouraged on how firms and FMIs currently address the issues and risks discussed in this paper. The supervisory authorities would welcome responses to the questions asked throughout the DP and listed in Chapter 8. Responses are requested by Friday 5 October 2018.

The importance of operational resilience

1.4 Operational disruptions to the products and services that firms and FMIs provide have the potential to cause harm to consumers and market participants, threaten the viability of firms and FMIs, and cause instability in the financial system. This DP focuses on how the provision of these products and services can be maintained. Operational resilience refers to the ability of firms, FMIs and the sector as a whole to prevent, respond to, recover and learn from operational disruptions.

1.5 From the perspective of firms and FMIs, there are numerous challenges to making sure their businesses are resilient to operational disruption. These challenges have become more complex and intense in recent years, during a period of technological change and in an increasingly hostile cyber environment. Additional challenges occur where firms operate internationally or outsource a significant level of activities to third parties. Some of these challenges are illustrated in Figure 1.

Figure 1: Challenges to building operational resilience



¹ Entities authorised, registered or recognised under the Financial Services and Markets Act 2000 (FSMA) (eg investment or consumer credit firms or recognised investment exchanges) and authorised and/or registered under other regimes (eg, Payment Services Regulations 2017 (PSRs 2017), and Electronic Money Regulations 2011 (EMRs 2011)).

1.6 The operational resilience of firms and FMIs is a priority for the supervisory authorities and is viewed as no less important than financial resilience. A lack of resilience represents a threat to the supervisory authorities' specific objectives as well as their shared goal of maintaining financial stability (see Box A).

Box A: The supervisory authorities' objectives

The Bank has an objective to protect and enhance the stability of the financial system of the United Kingdom.¹ The Bank sets out in its Financial Stability Strategy² that financial stability is the consistent supply of the vital services that the real economy demands from the financial system. Those vital services are: providing the main mechanism for paying for goods, services and financial assets; intermediating between savers and borrowers, and channelling savings into investment, via debt and equity instruments; and insuring against and dispersing risk. The Bank as supervisor of FMIs seeks to ensure that FMIs are designed and operated in a safe way, and that they contribute to reducing systemic risks in the vital payment, settlement and clearing arrangements centred upon them. The Bank's operation of the Real Time Gross Settlement (RTGS) service and the Clearing House Automated Payment System (CHAPS) also supports the delivery of the Bank's overall mission.

The PRA's and FCA's objectives are also defined in the Financial Services and Markets Act 2000 (FSMA). The PRA seeks to promote the safety and soundness of the firms it supervises, and contribute to the securing of an appropriate degree of protection for those who are or may become insurance policyholders. The PRA also has a secondary competition objective. The FCA's strategic objective is to ensure that relevant markets work well. To advance its strategic objective, the FCA has three operational objectives: to secure an appropriate degree of protection for consumers, to protect and enhance the integrity of the UK financial system, and to promote effective competition in the interests of consumers. In achieving these objectives, both regulators seek to support financial stability.

1.7 The Bank and the supervisory authorities have interlinked objectives, which include promoting financial stability. The supervisory authorities consider that improvements in operational resilience would be facilitated by complementary regulatory standards and supervisory approaches.

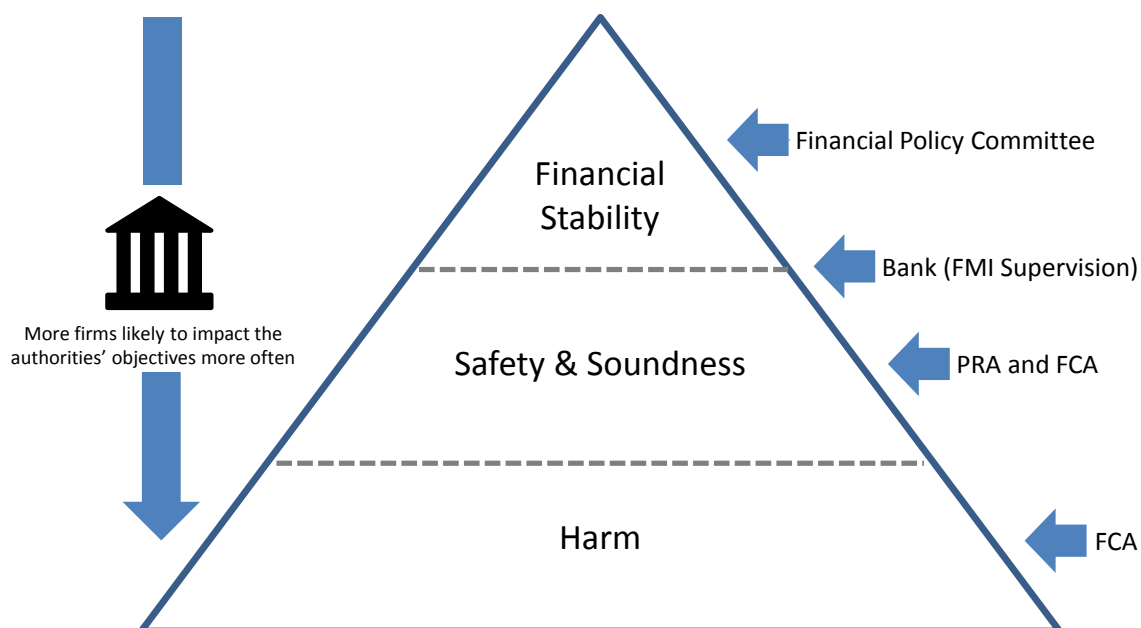
1.8 Figure 2 illustrates the objectives which are most likely to be affected by operational resilience issues. It also illustrates that the consumer protection objective is likely to be affected more often, and by more firms, than the market integrity, the safety and soundness, and financial stability objectives.

1.9 Interconnectedness occurs both within the UK and internationally. The supervisory authorities are engaged in international fora supporting the development of operational resilience principles and standards. Common standards would help ensure that operational resilience is not adversely affected by the location of firms' and FMIs' infrastructure, and will assist regulatory co-operation in the supervision of international firms.

1.10 Improving operational resilience might also be good for competition. A shared understanding of minimum standards may help new entrants establish themselves in a market.

1 Bank of England Act 1998, section 2A: <https://www.legislation.gov.uk/ukpga/1998/11/section/2A#commentary-key-8734b5fd971e45bdddb681573bfa3213>.

2 Bank of England, Financial Stability Strategy: www.bankofengland.co.uk/financial-stability.

Figure 2: Impact of operational resilience on the objectives of the authorities

Important concepts in the supervisory authorities' approach to operational resilience

1.11 This DP discusses a number of important concepts which are relevant to all firms and FMIs:

- The supervisory authorities consider that the continuity of business services is an essential component of operational resilience. Accordingly, firms and FMIs should focus on that outcome when approaching operational resilience. Avoiding disruption to a particular system supporting a business service is a contributing factor to operational resilience. But ultimately it is the business service that needs to be resilient – and needs to continue to be provided. The supervisory authorities envisage that boards and senior management should assume that individual systems and processes that support business services will be disrupted, and increase the focus on back-up plans, responses and recovery options.
- Setting impact tolerances which quantify the amount of disruption that could be tolerated in the event of an incident may be an efficient way for boards and senior management to set their own standards for operational resilience, prioritise and take investment decisions. An example would be a maximum acceptable outage time for a business service. Firms and FMIs would test their ability to stay within their impact tolerances in severe but plausible scenarios in order to identify vulnerabilities and take mitigating action. The supervisory authorities may expect some firms and FMIs to consider any FPC impact tolerance when setting their own impact tolerances.¹
- How firms and FMIs manage their response to operational disruption is critical to maintaining confidence in the business services they provide. The speed and effectiveness of communications with those affected, including customers, is an important part of their overall response and could help to manage the expectations of those affected and maintain or restore confidence in the firm's business services.

¹ This DP does not affect requirements or obligations under existing legislation or international standards such as the CPMI-IOSCO principles for Financial Market Infrastructure, PSRs 2017 or the EMRs 2011; any future changes proposed would have regard to the existing international standards and other legal requirements, including EU requirements.

- Operational resilience is already a responsibility of firms and FMIs, and an outcome supported by the existing regulatory framework. The supervisory authorities are considering the extent to which they might supplement existing policies to improve the resilience of the system as a whole, and to increase the focus on this area within individual firms and FMIs. They are reviewing existing policies, including those on risk management, outsourcing, controls and communication and business continuity plans, to ensure that these continue to be effective, in light of market and technological developments.
- The supervisory authorities are also reviewing their approach to the assessment of operational resilience matters, which may include an increased focus on firms' and FMIs' non-financial resources. Gaining assurance that appropriate impact tolerances are set, monitored and tested is likely to be a key component of future supervisory approaches.¹

Discussion paper structure

1.12 **Chapter 2** explains why the supervisory authorities consider that managing operational resilience is most effectively addressed by focusing on business services, rather than on systems and processes. The chapter also explains that firms and FMIs are more likely to be operationally resilient if they design and manage their operations on the assumption that disruptions will occur to their underlying systems and processes.

1.13 **Chapter 3** explains that financial stability rests on the operational resilience of individual firms, FMIs and the system as a whole. The FPC is establishing its tolerance for the length of any period of disruption to the delivery of vital services the financial system provides to the economy in the context of cyber (an 'FPC impact tolerance'), as set out in its June 2018 Financial Stability Report (FSR).² The supervisory authorities consider that their approach to operational resilience described in this DP is consistent with the FPC's approach, and supports its agenda.

1.14 **Chapter 4** suggests that the boards and senior management of firms and FMIs could set their own tolerances for operational disruption, on the assumption that some (or all) supporting systems and processes will fail. In setting impact tolerances, the supervisory authorities suggest that a firm's or FMI's board or senior management might prioritise those business services which, if disrupted, have the potential to: threaten the firm's or FMI's ongoing viability; cause harm to consumers and market participants; or undermine financial stability. The chapter also highlights relevant existing regulatory standards related to operational resilience that firms and FMIs are already expected to meet.

1.15 **Chapter 5** expands the idea that firms and FMIs would develop impact tolerances for important business services. These would provide clear metrics indicating when an operational disruption would represent a threat to a firm's or FMI's viability, to consumers and market participants or to financial stability. The chapter discusses what impact tolerances are and their purpose. To help inform the development of the approach, the supervisory authorities are particularly interested in metrics firms and FMIs currently use.

1.16 **Chapter 6** explains how supervisors could gain assurance that firms and FMIs ensure the continuity of their most important business services, and that boards and senior management are sufficiently engaged. The supervisory authorities are reviewing their existing approaches in light of

1 This DP has been written in the context of the current UK and EU regulatory framework. The supervisory authorities will keep the discussed approach under review to assess whether any changes would be required due to changes in the UK regulatory framework, including those arising once any new arrangements with the European Union take effect.

2 Financial Stability Report, June 2018: <https://www.bankofengland.co.uk/financial-stability-report/2018/june-2018>.

the proposed focus on business services, and are considering the role of scenario testing in this context.

1.17 **Chapter 7** summarises the key concepts set out in the DP.

1.18 **Chapter 8** is a complete list of the questions in the DP.

1.19 This DP is part of the supervisory authorities' wider engagement on this topic. Further dialogue on the financial sector's operational resilience will occur through discussions with firms, FMIs and other industry participants and through international engagement.

1.20 A glossary of terms is provided in Annex 1.

2 Operational resilience of business services

This chapter explains why the supervisory authorities consider that managing operational resilience is most effectively addressed by focusing on business services, rather than on systems and processes. The chapter also explains that firms and FMIs are more likely to be operationally resilient if they design and manage their operations on the assumption that disruptions will occur to their underlying systems and processes.

Focusing on business services

2.1 Operationally resilient business services provided by firms and FMIs directly support resilient economic functions,¹ enabling people to buy goods, borrow money and markets to transact. Resilient business services therefore support financial stability.

2.2 The UK financial system is resilient if its economic functions can continue to operate during potentially disruptive incidents at a firm, FMI or across groups of firms. Resilience of the financial system depends on both individual firms and FMIs and the interconnections between them.

2.3 Continuity of business services is also critical to the viability of individual firms and FMIs, and disruptions can cause harm to consumers and market participants.

2.4 The supervisory authorities believe that if firms' and FMIs' boards and senior management focus on the operational resilience of their most important business services, this would assist the supervisory authorities in furthering their objectives.

2.5 Priorities between firms and FMIs and the supervisory authorities may not always be aligned. It is possible that the supervisory authorities may believe that a disruption to a business service would harm their objectives, while a firm or FMI might consider the disruption to be a manageable risk.

Prioritising by business services

2.6 A business services approach is an effective way to prioritise improvements to systems and processes. Firms and FMIs may currently prioritise the upgrading of their IT systems by: age; those most prone to failure; anticipated cost of financial failure; or cost of upgrade against available budget. Such considerations may be inconsistent with an outcome focused on continuity of business services. Looking at the systems and processes on the basis of the business services they support may bring more transparency to and improve the quality of decision making, thereby improving resilience. The supervisory authorities are keen to understand which approaches to operational resilience firms and FMIs have found most useful.

2.7 A focus on business services could help drive specific and measurable activities, including investment, that increase operational resilience. Firms and FMIs could set target metrics for the continuity of important business services. Firms' and FMIs' ability to meet their target metrics could then be tested, enabling them to take action as necessary.

2.8 While this DP focuses on the delivery of business services, operational disruption can also impact firms' and FMIs' ability to meet other regulatory or contractual obligations. For example, firms are expected to ensure the confidentiality of data, or may be required to provide timely and accurate financial reports. Firms and FMIs also need an appropriate degree of resilience in these and other areas.

1 A list of economic functions, defined for resolution purposes, was set out in PRA Supervisory Statement 19/13. This list is reproduced in Annex 2 of this DP to aid discussion.

Building resilient business services, assuming disruption will occur

2.9 In order to build and deliver resilient business services, firms and FMIs need the ability to: prevent disruption occurring to the extent practicable; adapt systems and processes to continue to provide services and functions in the event of an incident; return to normal running promptly when the disruption is over; and learn and evolve from both incidents and near misses. The supervisory authorities consider that firms and FMIs would pay attention to all of these aspects.

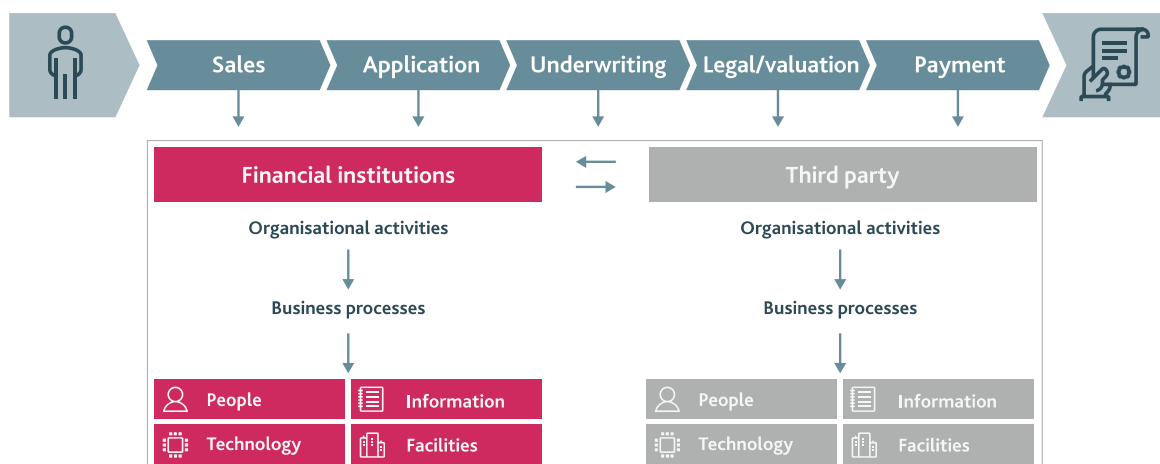
2.10 It is particularly important to plan on the basis that operational disruptions will occur. This is because it is not possible to prevent every risk materialising, and dependencies are often only identified once something has gone wrong. The assumption that operational disruptions will arise could be used to inform strategy, planning and resourcing.

2.11 The supervisory authorities believe that an operationally resilient firm or FMI would have in place:

- a clear understanding of their most important business service or services;
- a comprehensive understanding and mapping of the systems and processes that support these business services, including those over which the firm or FMI may not have direct control. This would include an understanding of the resilience of outsourced providers or entities within the same group but in another jurisdiction;
- knowledge of how the failure of an individual system or process could impact the provision of the business service;
- knowledge of which systems and processes are capable of being substituted during disruption so that business services can continue to be delivered;
- tested plans that would enable firms and FMIs to continue or resume business services when disruptions occur;
- effective internal communication plans, escalation paths and identified decision makers; and
- specific external communication plans for the most important business services, which provide timely information for customers, other market participants and the supervisory authorities.

2.12 Firms' and FMIs' implementation of these elements would be proportionate to their nature, scale and complexity, as discussed in 'What this might mean for firms and FMIs in practice' in Chapter 4.

2.13 Figure 3 illustrates the variety of systems and processes that would need to be considered. This may be contrasted with an incomplete view of resilience obtained by taking a narrow focus on particular systems or processes considered in isolation. In this example, mortgages are the important business service, and there are a number of steps necessary from origination through to customer service. Only by looking at all of these stages – and where appropriate, at how elements of this service get delivered by other parties – can a clear picture be developed of how best to support the resilience of the business service.

Figure 3: Understanding important business services**Business service: retail mortgages**

2.14 It would be neither possible nor an efficient use of resources to attempt to make every component of an organisation completely resilient to operational disruption. The supervisory authorities recognise that firms and FMIs need to prioritise and want this prioritisation to be well-considered and agreed at the appropriate level. Under the approach outlined in this DP, firms' and FMIs' prioritisation would be informed by an effective understanding of their most important business services and underlying systems and processes.

Questions

- A) What are readers' views on the proposed focus on continuity of business services? Would a service rather than systems-based approach represent a significant change for firms and FMIs compared with existing practice? What other approaches could be considered?

3 Operational resilience and the FPC

The FPC is establishing its tolerance for the length of any period of disruption to the delivery of vital services the financial system provides to the economy in the context of cyber, as set out in its June 2018 FSR.¹ The supervisory authorities consider that the approach to operational resilience set out in this DP, in particular the focus on continuity of business services and the need for firms and FMIs to have their own impact tolerances, is consistent with the FPC's approach, complementary to the FPC's activities and supports its agenda.

3.1 The FPC identifies, monitors and takes action to remove or reduce systemic risks with a view to protecting and enhancing the resilience of the UK financial system. The FPC has been considering whether testing the financial system for disruption from cyber incidents is warranted for the purpose of enhancing and maintaining UK financial stability. While the FPC has been doing this in the context of cyber, the concepts are relevant to operational resilience regardless of the specific cause of disruption.

3.2 On Wednesday 27 June 2018 the Bank published the Financial Stability Report, which set out the FPC's approach to defining its tolerance for disruption. This is reproduced in Box B.

Box B: Extract from the June 2018 Financial Stability Report

The FPC's tolerance for the disruption of financial services from cyber incidents

Financial stability is the consistent supply of the vital services that the real economy demands from the financial system. A severe operational incident, such as an IT failure or a cyber incident, can impair processes and data supporting these services, and therefore put financial stability at risk.

The FPC set out the elements of the framework of regulation to strengthen the resilience of the UK financial system to cyber risk in the June 2017 *Report*:

- i) clear baseline expectations for firms' resilience that reflect their importance for the financial system;
- ii) regular testing of resilience by firms and supervisors;
- iii) identification of firms that are outside the financial regulatory perimeter, but which may be important for regulated firms; and
- iv) clear and tested arrangements to respond to cyber attacks when they occur.

This box sets out how the FPC plans to address points (i) setting clear expectations, and (ii) testing firms.

Effective resilience requires firms to be able to: prevent material incidents from occurring; continue to provide services and functions in the event of an incident; prevent an increase in the level of fraud during an incident; return to normal operations promptly when the incident is over; and learn from incidents, in order to limit the chances of them happening again in future.

Firms have primary responsibility for their ability to resist and recover from cyber incidents. The supervisory authorities expect boards to take responsibility for the cyber resilience of their firms. For example, within the PRA's Senior Managers and Certification Regime, the Chief Operations Senior Managers Function has responsibility for the internal operations and technology of a firm,

¹ See footnote 3, page 8.

including cyber security. **To guide firms in their planning, the FPC is establishing its tolerance for the length of any period of disruption to the delivery of vital services the financial system provides to the economy. That time frame is the FPC's 'impact tolerance'.**

The services on which the FPC is focused are:

- providing the main mechanism for paying for goods, services and financial assets (hereafter, 'payments');
- intermediating between savers and borrowers, and channelling savings into investment, via debt and equity instruments; and
- insuring against and dispersing risk.

Consistent with the FPC's responsibility to mitigate systemic risk, it will set a tolerance at the point after which it judges disruption would begin to cause material economic impact.

For example, disruption to one bank's payments could have a direct impact on the real economy by impacting the ability of customers of that bank to pay for goods and services. But a severe disruption to one bank's ability to make payments may also have an impact on other firms initially unaffected by the incident which could impair interbank lending and, in turn, activities such as clearing, settlement or mortgage payments.

Likewise, disruption to derivatives trading could affect firms' ability to insure themselves against financial risk. A severe disruption could have market confidence effects if participants lost confidence in an institution or economic activity, and could also increase the risk of default of a major market participant. It could also create market uncertainty and affect market liquidity.

Working with others, especially the National Cyber Security Centre, the Bank will test that firms would be able to meet the FPC's standards for recovering services.

The FPC recognises that firms would not be able to meet its tolerances in the most extreme circumstances. Doing so would make the effective provision of financial services inefficient. The FPC intends to calibrate its stress-testing scenarios to be severe but plausible.

In stress tests of financial resilience, the FPC is able to use past macroeconomic data to calibrate a severe but plausible macroeconomic shock. No such history exists for cyber events. So the FPC will rely on the independent judgement of experts, such as the National Cyber Security Centre, to assist calibration of the stress scenarios, drawing on up-to-date intelligence.

Firms undertaking this stress testing will need to demonstrate their ability to meet the FPC's impact tolerance. In instances where that cannot be shown, remedial action plans will be agreed with supervisors.

The FPC will work with other regulators to establish which firms would be in scope of stress testing. The scope is likely to vary, depending on the vital service that is being tested, and will take into account firms' contribution to the function (measured by value, volume and/or market share), and interconnectedness.

This stress-testing approach will be developed by the Bank and the PRA, with input from the FPC. The particular incident modelled, the firms in scope, and the economic activities tested will likely vary from test to test.

The Bank plans to launch a pilot of the approach to stress testing in 2019, which will focus on payments. The Bank and the PRA will work with firms to develop the pilot approach. Further details will be published in 2018 Q4.

Cyber risks are one example of operational incidents that could have a significant impact on firms' ability to provide vital services. The FPC focuses on these risks, as cyber incidents are most likely to be part of a system-wide threat. In the Bank's latest *Systemic Risk Survey*, published alongside the *Financial Stability Report*, 62% of respondents cited it as a key source of risk, up from 51% a year ago.

While they did not have systemic consequences, recent episodes of disruption to customers using the Visa payment system and of TSB bank highlighted the importance of operational risk beyond cyber incidents for individual firms and consumer protection. They will therefore inform further work of firm-level supervisors in this area. The authorities' broader approach to operational resilience, including cyber risk, will be discussed in an upcoming joint FCA, Bank and PRA Discussion Paper.

3.3 The supervisory authorities consider that the approach to operational resilience set out in this DP would be consistent with the FPC's approach. Both focus on continuity, whether it is the continuity of vital services at the system level for the FPC, or the continuity of business services for the supervisory authorities. There is also a common emphasis on severe but plausible scenarios to establish the level of resilience of the system as a whole, or of individual firms and FMIs.

Questions

- B) Would encouraging firms and FMIs to consider their contribution to the vital services that the real economy demands change the way they manage operational resilience, and if so how? What additional costs would this incur?

4 Operational resilience of firms and FMIs

This chapter suggests that the boards and senior management of firms and FMIs would set impact tolerances for the operational disruption of business services, on the assumption that some or all supporting systems and processes will fail. In setting impact tolerances, the supervisory authorities suggest that a firm's or FMI's board or senior management might prioritise those business services which, if disrupted, have the potential to: threaten the firm's or FMI's ongoing viability; cause harm to consumers and market participants; or undermine financial stability. The chapter also highlights relevant existing regulatory standards related to operational resilience that firms and FMIs are already expected to meet.

4.1 In view of the potentially severe consequences of poor operational resilience, the supervisory authorities believe operational resilience is a key issue on which boards and senior management should focus. A firm's or FMI's resilience is the result of its activities and choices, and will depend on its governance, culture, corporate structure, controls and regulatory framework.

4.2 To be effective, boards and senior management must agree clear standards that they expect the executive of a firm or FMI to meet. Chapter 2 suggests that the supervisory authorities consider that they might best do this by focusing on business services. The supervisory authorities consider that boards and senior management could go further by setting impact tolerances for disruption to the most important business services.

4.3 An impact tolerance describes a firm's or FMI's tolerance for disruption to a particular business service, under the assumption that disruption to the systems and processes supporting that service will occur. Impact tolerance is expressed by reference to specific outcomes and metrics. Such metrics could include the maximum tolerable duration or volume of disruption, a measure of data integrity or the number of customers affected.

4.4 Having impact tolerances may help ensure that boards and senior management consider what the firm or FMI would do when a disruptive event occurs, rather than only trying to minimise the probability of disruption. This might include how to handle the situation to minimise the consequences of disruption as well as ensuring that the relevant business services continue to be delivered within tolerance.

4.5 While an assumption that disruption will occur enables greater clarity around the outcome being sought, firms and FMIs may also need to think about the instances in which it would, or would not, be acceptable to meet a tolerance. This DP describes such instances as scenarios.

4.6 The supervisory authorities may also consider setting their own impact tolerances for firms or FMIs to meet within the context of severe, but plausible, scenarios.

4.7 In arriving at an impact tolerance, boards or senior management would consider the commercial interests of the firm or FMI and the objectives, rules, principles, expectations and guidance of the relevant supervisory authorities. This chapter therefore discusses:

- factors relating to the supervisory authorities' objectives that are likely to be key components in determining appropriate impact tolerances: when the viability of the firm or FMI is threatened; the impact on consumers and market participants; and the impact on financial stability;
- existing rules, principles, expectations and guidance relating to operational resilience that firms and FMIs are already required to meet; and

- what this might mean for different types of firms and FMIs in practice.

4.8 For the purposes of this DP, the supervisory authorities envisage that how impact tolerances are derived and justified might be set out by firms and FMIs in a single document – an impact tolerance statement.

4.9 Firms and FMIs could use their impact tolerances in running their businesses: to take decisions on investments, risk management, business continuity planning and corporate structure. Chapter 5 discusses how impact tolerances might be set and considered alongside existing risk appetite statements. The supervisory authorities are aware that some firms and FMIs may already be taking this approach, for example CPMI-IOSCO principles for financial market infrastructure (PFMI)¹ indicate that an FMI should design and test its systems and processes to aim for the safe resumption of critical operations within two hours of a disruption,² but it will be a new idea for others. It is also recognised that individual approaches to impact tolerances would be determined by the nature, scale and complexity of a firm's or FMI's activities. Readers are encouraged to provide feedback on practices that are already being employed, along with potential difficulties in implementing the approach.

4.10 Once impact tolerances are set, they will be relevant to the systems and processes supporting business services wherever they are located. This includes the systems and processes of outsourced service providers. This might require consideration of the extent to which standards differ between jurisdictions. In general, the impact tolerance for a particular business service would still need to be met, regardless of the location of supporting systems and processes.

Factors relating to the supervisory authorities' objectives

Impact on the viability of firms and FMIs

4.11 The supervisory authorities require firms' and FMIs' operations to be run in a sustainable manner. The PRA and the FCA, which prudentially supervises approximately 46,000 firms, expect the firms they supervise to run their businesses in a safe and sound manner.³ The Bank seeks to ensure that FMIs operate in a safe way, in support of its financial stability objective.⁴ Prudently-run firms and FMIs should try to maintain and increase their operational resilience, particularly in response to evolving threats such as cyber attacks.

4.12 The supervisory authorities consider firms and FMIs might assess their operational resilience in the context of how disruptions to important business services might threaten their ongoing viability. To identify business services that support a firm's or FMI's viability, boards and senior management might consider which services, if disrupted, could lead to significant loss of customers, major financial loss or reputational damage. Examples might include: disruptions to the services that allow customers to transfer funds between accounts; a bank not being able to extend commercial finance; an FMI not being able to collect margin payments; or an insurance company not being able to fund and hedge its balance sheet.

4.13 Under requirements such as Internal Capital Adequacy Assessment⁵ and Risk Control,¹ boards and senior management should already be able to articulate those circumstances which may lead to

1 A joint publication of the Committee on Payments Systems and Market Infrastructures (CPMI) and the Technical Committee of the International Organization of Securities Commissions (IOSCO): www.bis.org/cpmi/publ/d101a.pdf.

2 Principle 17.

3 The FCA is the prudential supervisor for approximately 46,000 firms; for 18,000 firms, a regime of minimum standards beyond both the principle of business of financial prudence and the threshold condition of appropriate resources exists.

4 Box A on page 7 sets out the supervisory authorities' specific objectives.

5 Internal Capital Adequacy Assessment Part of the PRA Rulebook: www.prarulebook.co.uk/rulebook/Content/Part/211179/05-07-2018.

the firm's or FMI's failure, develop their own risk appetites and oversee delivery of risk mitigation. This should include:

- an assessment of the adequacy of a firm's or FMI's operational resources to maintain resilience, relevant to a firm's or FMI's ability to remain viable; and
- effective risk management of their organisation, people, processes and technology assets,² all of which support the continuity of business service delivery during operational disruptions.

Impact on consumers and market participants

4.14 The supervisory authorities are also concerned by the potential harm that operational disruptions could cause to users of a firm's or FMI's business service, including both consumers and market participants.

4.15 Harm to consumers (such as an inability to access cash deposits, savings, credit or other financial services) and harm to market participants (such as an inability to price trades or to complete post-sale activities) arising from operational disruptions is likely to manifest before risks to the viability of a firm or FMI start to crystallise. As the FCA's Mission³ requires it to consider harm to consumers, the FCA may engage with authorised firms in relation to their management of an operational disruption more frequently and at an earlier stage than the PRA, to understand how they would seek to minimise the amount of harm caused by operational disruption.

What is meant by 'harm' in this context?

4.16 Harm to consumers may arise, for example, from disruption to the:

- ongoing availability of existing business services, for example when claiming on an insurance contract, making loan repayments, checking balances, or accessing deposits and savings; and
- supply of new business services, for example renewing a general insurance contract, obtaining life insurance, receiving a mortgage advance or personal loan, or making a money transfer.

4.17 Harm to market participants is concerned with the risks that operational disruptions pose to the smooth operating of financial markets and the potential threat to market confidence that can result from a substantial disruption. Harm to market participants and market integrity may arise from, for example, the failure of a shared facility or market infrastructure on which the functioning of a market depends, uncontrolled access to and misuse of market sensitive data, the inability to access market data to price trades, or the inability to complete post-sale activity.

4.18 The supervisory authorities invite discussion about how firms and FMIs could be more active in assessing harm caused by the disruption to business services. Identifying harm caused by the disruption to business services could inform the setting of impact tolerances explained in Chapter 5.

1 Risk Control Part of the PRA Rulebook: PRA www.prarulebook.co.uk/rulebook/Content/Part/214146/05-07-2018.

2 For example, BCBS Principles for the Sound Management of Operational Risk (BCBS 2011), PRA rulebook, Solvency II firms, Conditions Governing Business 3. Risk Management.

3 FCA, Our Mission, April 2017: www.fca.org.uk/publication/corporate/our-mission-2017.pdf.

Box C: Examples of harm

Harm arising from operational resilience failures is illustrated in the following examples. Some relate to the continuity of business services, while others relate to the integrity of data.

Supply of new business services:

- A retail bank's mortgage application system fails to present all relevant questions for customers or brokers to answer, with the result that underwriting decisions start to be based on incomplete disclosure. Harm materialises in several ways: some mortgage applications are rejected and, once the error is detected, all the affected customers experience delays while the additional information is obtained from them.

Availability and integrity of existing business services:

- A software error results in duplicate Bacs Direct Debit payments being taken from customers' accounts. Some payees' bank accounts incur unauthorised overdraft charges. Some customers are unable to access cash when they need it because their balances are incorrect.
- A system error at a consumer credit firm leads to inaccurate (higher) debt repayment demands and consequential effect on the customers' credit files.

Availability of a vital link in a value chain:

- A custody bank is unable to confirm ownership of assets in a timely way, which delays asset valuations, and sales cannot be completed on the intended value dates.
- A disruptive event at a specialist trading venue prevents trading of derivatives for a number of hours.

Unauthorised access to market sensitive data:

- A corporate liability insurer's file management system is upgraded. After the upgrade, all employees have access to folders containing market sensitive data disclosed by listed companies, and the folder permissions error is not identified for several months.

Impact on financial stability

4.19 The financial system comprises many participants who interact to provide services to each other and the real UK economy. There are significant dependencies between participants. The resilience of individual participants can thus depend on the resilience of others, including the Bank (see Box D). The resilience of the financial system as a whole depends on the resilience of individual participants and the interconnections that exist between them.

4.20 Changing business models and increased outsourcing has increased the dependence of participants on others, including, in some cases, a limited number of technology providers, giving rise to concentration risk. This illustrates how, while technological innovation creates opportunities, including increasing efficiency and enabling better risk management, changing technologies are also creating new risks. Cyber threats have increased and have a greater propensity to be transmitted between participants.

4.21 Supporting financial stability is reflected in each of the supervisory authorities' objectives and their respective approaches to supervision. The supervisory authorities do not seek to ensure that no firm or FMI fails, but they do seek to ensure that, in the event of failure, it is orderly and avoids significant disruption to the UK economy.

4.22 Firms and FMIs should consider the impact of disruption within their own businesses on consumers and market participants which rely upon them, and take this into account when considering their approach to operational resilience.

Box D: Building operational resilience; the Bank as a provider of payment and settlement systems

The Bank recognises that it has its own part to play in building the operational resilience of the UK financial sector as operator of the CHAPS and RTGS services. RTGS processes an average of over £600 billion worth of transactions every working day, of which approximately half is CHAPS settlement. Firms and FMIs rely on the Bank's provision of these services to move sterling around the financial market and the real economy.

The CHAPS payment system is used for high-value wholesale payments as well as time-critical retail payments. The Bank's RTGS settlement infrastructure holds accounts for banks, building societies and other institutions. The Bank's operational function holds itself to high standards and is committed to a very low tolerance for any disruption to the RTGS and CHAPS services. As the operator of CHAPS, the Bank is the 'systemic risk manager' for the CHAPS system, a role that includes understanding and managing risks across the end-to-end CHAPS system. The Bank's operation of CHAPS is independently supervised by the Bank's FMI Directorate on a non-statutory basis against the same standards as other payment systems.¹ The Bank's Banking, Payments and Financial Resilience Directorate also self-assesses RTGS and CHAPS against the CPMI-IOSCO Principles for Financial Market Infrastructures annually. For RTGS, the Bank commissions an ISAE3402 external control audit and holds an ISO 27001 certificate.

The Bank sets access criteria for firms that want direct access to CHAPS, as well as operational and technical requirements for RTGS and CHAPS. Assurance is sought from CHAPS Direct Participants that they meet the rule book's requirements, complemented by a rigorous testing regime. Requirements cover areas such as day-to-day operations; resilience and contingency; technical maintenance; network connectivity; and physical, environmental and information security.

Strengthening the resilience of RTGS and its flexibility to respond to emerging threats is a key focus of the programme to renew the RTGS service and supporting infrastructure.

Existing regulatory requirements and expectations for firms and FMIs

4.23 The supervisory authorities consider that setting impact tolerances could play an important part in increasing the operational resilience of firms and FMIs. These would support existing regulatory expectations and obligations. The supervisory authorities are reviewing the existing regulatory framework in the light of the overall approach set out in this DP, and with regard to existing international, European Union and domestic requirements and regulatory frameworks.

4.24 Each supervisory authority is responsible for a spectrum of firms or FMIs and each has its own rules, principles, expectations, or guidance. Nevertheless, common regulatory themes apply across regulated entities including individual and collective accountability for matters that support operational resilience. This is generally achieved by rules, principles, expectations, or guidance on: management and governance; risk management; internal controls for systems and processes; contingency planning; and oversight of outsourcing arrangements.

4.25 Some of the existing rules and standards are summarised below. Those listed here cover key policy areas only and may not necessarily be applicable to all firms and FMIs; more detail is provided

¹ See Box 2 of the 'Bank of England's supervision of financial market infrastructures – annual report' for further explanation: www.bankofengland.co.uk/news/2018/february/supervision-of-financial-market-infrastructures-annual-report-2018.

in Annex 3. Box E provides an example of how some existing regimes interact to support operational resilience.

Box E: Interaction of regimes

The regulatory framework already features many requirements that help build the operational resilience of firms and FMIs. A brief explanation of how the supervisory authorities see the relationship between operational resilience and policies on operational continuity in resolution and capital requirements for operational risk is set out below.

Operational resilience, operational continuity in resolution and operational risk

This DP on operational resilience is focused on the continuity of business services and economic functions. The approach set out in this DP includes an assumption that disruptions to systems and processes will occur and focuses on firms' and FMIs' responses to these disruptions. Time-to-recover is often a key metric. Operational resilience is an outcome which emerges from a wide array of practices and disciplines undertaken by firms and FMIs.

Some of the UK's largest banks and building societies are subject to the PRA's operational continuity in resolution (OCIR) policy.¹ OCIR policy aims to ensure the continuity of critical functions, from an operational perspective, through severe stress and resolution. It is similar to operational resilience in its focus on the continuity of services, but is narrower as it focuses specifically on stress and resolution, and events that might occur in those circumstances. OCIR policy includes requirements to have resolution-proof contracts with third parties and for firms to be able to map critical services supporting critical functions.

Operational risk refers to the risk associated with inadequate or failed processes, people or systems or from external events including legal risk. It includes consideration of both the severity of impact and the likelihood of loss occurring, in the broader context of the requirement on firms to manage their businesses prudently, or for those firms to whom the Capital Requirements Regulation (CRR) applies, requiring capital to be held against operational risks.² In the latter case, the policy aim is to minimise the impact and likelihood of such losses. Loss can include financial loss and loss of availability or confidence. Regulation relating to operational risk has tended to focus on minimising the probability of risk events occurring and ensuring firms can absorb financial losses when they do occur. Good operational risk management and the holding of capital against potential operational losses will help build operational resilience, but the ability to withstand financial loss is not sufficient in itself to ensure continuity of business services.

Existing regulatory requirements relating to the viability of firms and FMIs

Management and governance

4.26 An effective board is critical to ensuring a sound and well-run business. The supervisory authorities set expectations of the boards and senior management of regulated firms and FMIs to run their businesses prudently and in support of their objectives, including the continuing stability of the financial system.

4.27 Boards should ensure there is sufficient challenge to the executive and that they have access to people within the business with appropriate technical skills. They should also ensure the recruitment and training of suitable people for relevant executive roles, drawing on additional skills where relevant.

¹ PRA Policy Statement 21/16 'Ensuring operational continuity in resolution', July 2016: www.bankofengland.co.uk/prudential-regulation/publication/2014/ensuring-operational-continuity-in-resolution.

² Capital Requirements Regulation (575/2013) (CRR), Article 4.1(52): <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0036&from=EN>.

4.28 The PRA's Senior Managers and Certification Regime (SM&CR) requires relevant firms to have a Senior Management Function (SMF) responsible for the internal operations and technology of a firm, SMF 24.¹ This includes operational resilience, cybersecurity and operational continuity. The PRA and FCA have consulted on the creation of an equivalent SMF as part of the extension of the SM&CR to insurers, to be effective on 10 December 2018,² and FCA solo-regulated firms (FCA CP17/40). In respect of FCA solo-regulated firms, this SMF would apply in 'enhanced firms', which are generally those that are larger and more complex.

4.29 Similarly for FMIs, the PFMI³ recommend that FMI boards should explicitly define the roles and responsibilities for addressing operational risk and the FMI's operational risk-management framework.

Risk management

4.30 Risk management should cover all types of risk, including operational, and firms and FMIs are expected to identify, monitor and manage the risks they are or might be exposed to.

4.31 FMIs in particular are encouraged to consider threats such as natural disasters, terrorism, pandemics and cyber attacks. FMIs are also expected to assess the evolving nature of the operational risks they face on an ongoing basis so they can analyse potential vulnerabilities and implement appropriate defence mechanisms.

Internal controls

4.32 To deliver a firm or FMI's board-led strategy and direction, boards and senior management must be able to exercise appropriate oversight and be confident their direction is being carried out. This requires an effective internal control framework for prioritisation, undertaking specific activities, internal reporting and escalation.

4.33 The supervisory authorities' existing rules, principles, expectations and guidance already require firms and FMIs to manage their affairs in a responsible manner, which includes having adequate control systems in place. Effective internal controls should ensure firms' and FMIs' core businesses are managed appropriately, and that risks are dealt with.

Business continuity and contingency planning

4.34 The supervisory authorities have requirements of firms and FMIs to undertake appropriate contingency planning. Effective prior planning for when something goes wrong enables firms and FMIs to deal more efficiently with issues when disruptions occur, potentially reducing their impact.

4.35 The supervisory authorities also require firms and FMIs to maintain continuity plans explaining how they will respond and recover following disruption. The approach in this DP could require alignment of these plans with firms' and FMIs' most important business services and explanation of how they would continue to operate.

Outsourcing and critical service providers

4.36 Boards' and senior managements' oversight also needs to cover any activities outsourced to third-party providers, for example cloud service providers. While outsourcing can enable firms and

1 PRA Supervisory Statement 28/15, 'Strengthening individual accountability in banking', May 2017: www.bankofengland.co.uk/prudential-regulation/publication/2015/strengthening-individual-accountability-in-banking-ss.
2 Final policy published July 2018: www.bankofengland.co.uk/prudential-regulation/publication/2018/strengthening-individual-accountability-in-insurance-extension-of-the-smcr-to-insurers.
3 Principle 17 (Operational risk), consideration 2, of the CPMI-IOSCO PFMI: www.bis.org/cpmi/publ/d101a.pdf.

FMI's to manage risks more effectively and at a reduced cost, it can also give rise to new risks for which they remain responsible.

4.37 Boards' and senior managements' oversight also needs to include identification and understanding of the firm's or FMI's reliance on critical service providers. These are third party services critical to the continuous and adequate functioning of the firm's or FMI's operations, for example information technology, telecommunications and messaging services.

4.38 Indeed, existing rules require dual-regulated firms to avoid reducing the level of control or introducing additional risk through outsourced arrangements. Similarly, FMI's are expected to deal with outsourcing in a prudent way and ensure that outsourced and critical service providers meet the same requirements as internally provided services.

Existing regulatory requirements relating to harm

4.39 Existing requirements relevant to harm caused by operational resilience come from different legal sources. These include: domestic legislation, such as provisions in FSMA; sector-specific legislation, such as the Payment Services Regulations 2017; supervisory authorities' rules and guidance; and directly applicable European legislation. Examples are set out in Annex 3C.

4.40 Existing requirements include obligations on firms and FMI's to put in place risk management systems and business contingency or continuity arrangements. The supervisory authorities invite discussion about whether the way that firms approach existing requirements is compatible with identifying and preventing harm caused by disruption to business services.

Communications plans

4.41 The supervisory authorities have been considering the role of communications plans used at times of operational disruption. These can be important in mitigating consumer harm. It is important that business continuity policies include prompt and meaningful communication arrangements for internal and external parties, including supervisory authorities, consumers, other clients and the press. The supervisory authorities are considering whether there should be specific rules or further guidance on the content of communications plans. For example, the plans could address how to get hold of key people, how to contact operational staff, and how to contact consumers, suppliers, and the supervisory authorities.

4.42 The supervisory authorities recognise that harm may also arise from the loss of, or unauthorised access to, personal, financial and other sensitive data relating to consumers and market participants. The obligations on firms under, for example, the General Data Protection Regulation (GDPR)¹ will be relevant to operational resilience.

Existing regulatory requirements relating to financial stability

4.43 FMI's are typically unique in the services they provide to other market participants and are an integral part of almost all financial transactions. The financial system has a significant dependency upon them. Given their role and the obligations this creates, FMI's have an important role to play in promoting financial stability.

1 Regulation (EU) 2016/679 Of The European Parliament And Of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation): <https://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en>.

4.44 The Bank expects FMIs to comply with the PFMI.¹ The PFMI were designed to enhance the safety and efficiency of FMIs, but more broadly, to limit systemic risk and foster transparency and financial stability. In this regard they include a principle that an FMI's governance arrangements should support financial stability.

4.45 Specifically to manage systemic risk, an FMI should review the risks that it bears from others as a result of interdependencies, and develop appropriate risk management tools. To this end, FMIs impose and monitor standards and disciplines at their members to improve the robustness and resilience of the service provided. These typically include satisfying the FMI that adequate security and resiliency arrangements are in place, including technical requirements (eg around messaging) to access the FMI's infrastructure. FMIs should then have procedures to ensure their members continue to meet the standards for membership.

4.46 FMIs should also work with their members to enhance standards and minimise the adverse effects of disruption when it occurs. The standards need to be complementary to any regulatory standards, but it is also the case that these standards might need to be more rigorous or be more granular to enable the FMI to meet fully its obligations to its members and regulators. Box F provides an example of how an FMI could work together with its participants and other stakeholders to mitigate risk to financial stability.

Box F: Managing risks in the end-to-end processing of payments

A payments network connects a number of participants: the end users that want to make or receive payments; the banks that hold the end-users' accounts and initiate the payment process following their customers' instruction; and the payments system operator (FMI) that connects the banks to enable the payments to be processed, transferred and settled.

The resilience and robustness of the network depends on both the processes and systems of each participant and the nature of the connection between each participant. Threats to the network could be introduced by any participant and communicated to others via the network's connections.

If participants have concerns about the resilience of the payments network, their own resilience or the resilience of other participants, each of them may implement additional controls before releasing payments or may limit or halt processing payment instructions. When confidence in the integrity of the entire system has been lost, such individual precautionary controls could, in aggregate: create significant gridlock in processing payments; reduce overall liquidity in the financial markets; and potentially cause a build-up of unsettled positions and bilateral credit exposures among financial institutions. In extreme circumstances these actions could ultimately impede economic activity and disrupt financial stability. The existence or fear of fraud and weaknesses in security arrangements could also be reasons for concern by participants.

Individual firms and FMIs are responsible for their own robustness and security. However, it is important that participants work together to deliver the resilience of the end-to-end processing of payments within the network. This is a good example of how an FMI can work together with its participants and other stakeholders to mitigate risks to financial stability.

¹ The PFMI are formally applied to Central Counterparties and Central Securities Depositories through the European regulatory regimes (EMIR and CSDR). There is, however, no equivalent legislative framework applying the PFMI to payment systems.

What this might mean for firms and FMIs in practice

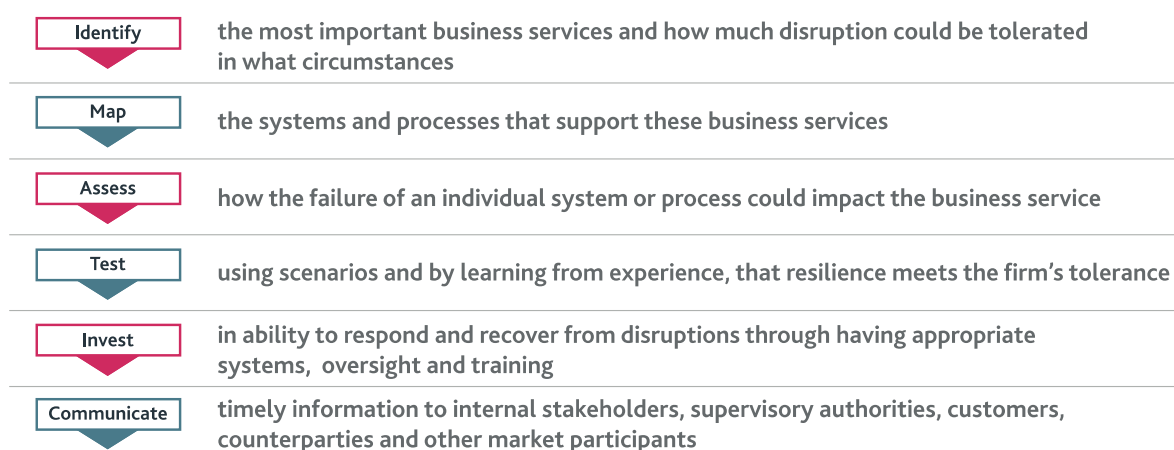
4.47 The supervisory authorities consider the ideas in this DP to be applicable to all types of firms and FMIs. The application of these ideas will, however, differ depending upon the nature and complexity of the relevant firm or FMI, including its size, activities and level of interconnectedness (and hence its impact on others and the financial system). Generally, all firms and FMIs would be considering two aspects in determining whether significant change is required by any future policy:

- Have they identified their business services in a way that permits the firm or FMI to link their activities to their business objectives and the objectives of the supervisory authorities?
- Have they appropriately prioritised between business services to ensure the most important ones are resilient to operational disruption?

4.48 Figure 4 illustrates the steps firms and FMIs could go through if policy were to be developed along the lines set out in this DP.

Figure 4: Improving operational resilience

Firms and FMIs could consider the following issues. To be effective, the process would need to be repeated routinely, with lessons learned incorporated into each iteration.



Large firms and FMIs

4.49 Large firms are likely to have many business services, while FMIs typically have a single business service which is likely to be significant to financial stability. There are numerous ways disruptions to business services could impact the supervisory authorities' objectives.

4.50 Such firms and FMIs could be expected to consider their impact tolerances for their most important business services. In doing so, the supervisory authorities could also expect them to take into account the work of the FPC, consider their contribution to economic functions, and use any FPC impact tolerances to inform their own impact tolerances. They could test themselves regularly against their own severe but plausible operational scenarios. They could also ensure that they have co-ordinated communications plans for internal functions, the supervisory authorities, consumers and other market participants should tolerances be breached. As set out in the June 2018 FSR, some firms and FMIs may also be the subject of stress testing developed by the Bank and the PRA, with input from the FPC.

4.51 The supervisory authorities could review the work these firms and FMIs undertake in relation to operational resilience on a regular basis, and provide feedback as appropriate. If the supervisory

authorities identify concerns, they could take further targeted action, with specific assessments of certain areas and, if necessary, request remedial action.

4.52 In many instances, the ideas discussed in this DP are a natural extension of what large firms and FMI and the supervisory authorities already do.

Small or mid-sized firms

4.53 Smaller firms are likely to only have a few business services, not all of which will be important to the firms' viability, have the potential to cause harm to consumers, or impact on financial stability. Nevertheless, some business services may be pivotal to the firm or even to the wider economy. There is likely to be a wide range of different business services across the sector.

4.54 A small bank or building society might identify operating customer savings accounts and the provision of mortgages as its most important business services. Identifying these two services, and assuming disruptions to them will occur, could support a smaller firm's own risk management and the setting of appropriate impact tolerances.

4.55 Such firms could undertake some limited testing of their operational resilience, based on their own scenarios. A pre-designed scenario provided by the supervisory authorities may also be of use. Testing could be designed to reveal, for example, what impact an incident would have on a firm's customers for a specific business service and other connected business services, as well as how the continuity planning arrangements seek to mitigate or prevent harm to consumers.

4.56 Firms could then address any deficiencies identified. This could include: ensuring joined up communications between all relevant functions within the firm (such as the business area that owns the data, customer services, operations, technology, and any third party providers); providing customers with information and advice; and prioritising assistance to customers exposed to the greatest harm.

4.57 The supervisory authorities could review the work such firms undertake on a periodic basis. But it is less likely such firms would be required to undertake further supervisory authority led review work, unless the supervisory authorities have particular cause for concern.

Very small firms

4.58 The smallest firms, such as financial advisors with few employees, are likely to only have few – perhaps only one – important business services. Such firms are also likely to have limited resources to increase their operational resilience.

4.59 Nevertheless, the supervisory authorities consider the proposed framework could still be relevant and beneficial. They envisage such a firm could:

- identify 'financial advice' as its important business service;
- identify how long it could operate as a business without providing that service;
- consider the systems and processes it relies on – for instance access to financial products and communication to clients; and
- consider how these processes could be duplicated in the event of some type of disruption, the length of time it might take to set up alternative arrangements, and whether prior-planning would be useful.

4.60 Such firms are likely to have limited supervisory engagement in this area. Nevertheless, thinking about the issue of operational resilience and what alternative arrangements could be made may still be beneficial.

Questions

- C) How do boards and senior management currently prioritise their work on operational resilience?
- D) What changes are firms and FMIs planning to make to strengthen operational resilience over the next few years? How involved are board members in the planning, implementation and embedding of any changes? What are the likely benefits and costs involved?

5 Clear outcomes for operational resilience

This chapter expands the idea that firms and FMIs would develop impact tolerances for important business services. These would provide clear metrics indicating when an operational disruption would represent a threat to a firm's or FMI's viability, to consumers and market participants or to financial stability. The chapter discusses what impact tolerances are and their purpose. The supervisory authorities are particularly interested in metrics firms and FMIs currently use.

5.1 As discussed in Chapter 2, the supervisory authorities consider that there is a benefit in boards and senior management having a clear understanding of the level of resilience required for their most important business services. To achieve this, they would need to be able to identify the relative importance of business services and be able to articulate the clear outcomes required.

5.2 The supervisory authorities envisage that the relative importance of business services can be derived by boards and senior management considering a firm's or FMI's business interests alongside the supervisory authorities' objectives. A business service that, if disrupted, represents a threat to a firm's or FMI's viability is clearly important – likewise, a business service that, if disrupted, could cause consumer harm, or impact financial stability.

5.3 The supervisory authorities are considering whether firms and FMIs should be required to set metrics that describe an intolerable level of disruption to their most important business services, in a severe but plausible stress scenario – impact tolerances. As discussed in Chapter 4, it is important to note that the impact tolerance would apply to the provision of the business service as opposed to the systems and process that support it.

5.4 The supervisory authorities envisage that firms and FMIs would determine their own impact tolerances. A firm or FMI would need to be able to explain how the particular impact tolerance has been arrived at for an important business service, how it relates to the supervisory authorities' objectives, and in which scenarios a breach of impact tolerances could be acceptable. These are likely to be limited to the most severe, but plausible, scenarios.

5.5 Scenarios are important because they introduce proportionality. They indicate how severe a disruption the firm or FMI anticipates being able to withstand, while remaining within its impact tolerance. This is illustrated in Figure 5 in Case 1, where Scenario 4 is so severe that it would be disproportionate for a firm or FMI to stay within their impact tolerance. Case 2 shows where a firm or FMI might need to improve the systems and processes supporting the business service, as less severe scenarios would breach their impact tolerance.

5.6 Impact tolerances would need to be expressed clearly and would be separate from any risk appetites or recovery time objectives (RTO). Impact tolerances express an upper limit where a breach is to be avoided in all but the most extreme scenarios. Risk appetites and RTOs, on the other hand, tend to express a desired outcome that is achieved with high probability. The supervisory authorities anticipate that firms and FMIs would be able to explain the relationships between the impact tolerances, risk appetites and RTOs they have set and that the approaches are complementary.

5.7 As an example of an impact tolerance in practice, the Bank sets a time and volume-based impact tolerance as operator of CHAPS.¹ The Bank states that all payments (volume) should be settled by

1 See also the PFMI. Principle 17 (Operational risk) indicates that an FMI should aim to resume operations within two hours following a disruptive event and complete settlement by the end of the day, even in extreme circumstances.

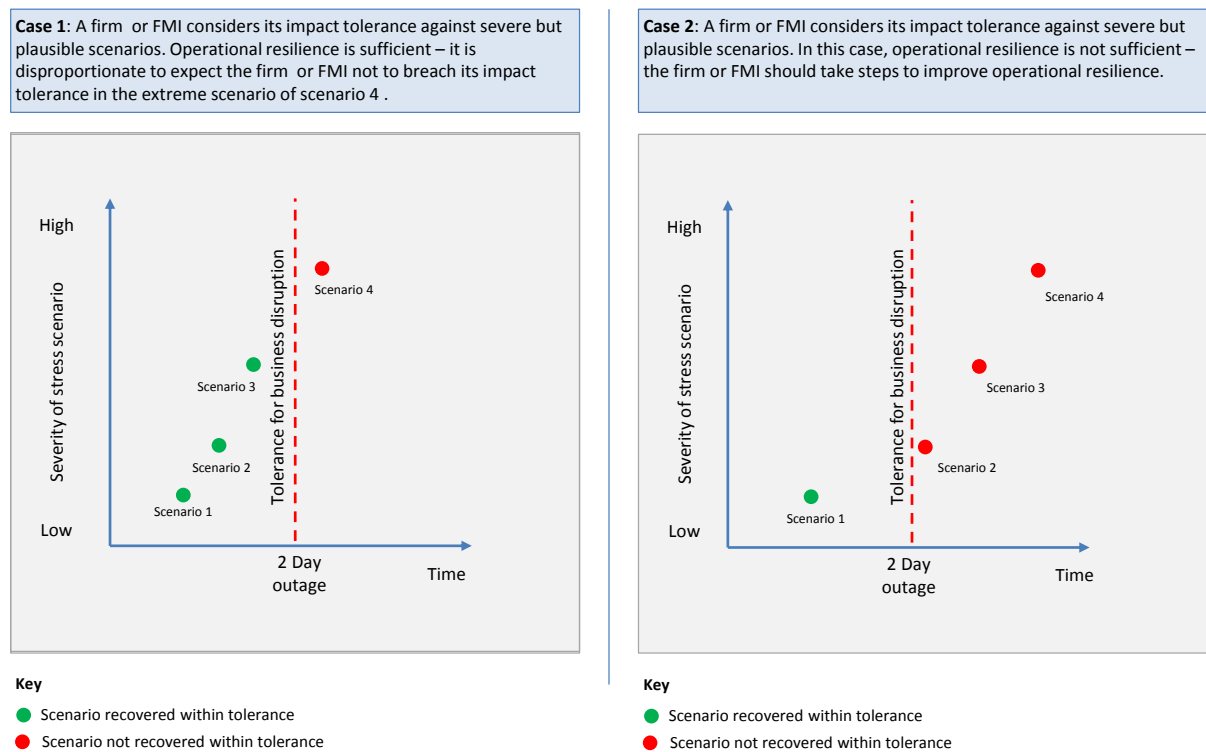
the end of the operating day (time) in all, even extreme, circumstances.¹ The supervisory authorities envisage that firms and FMIs may need to establish time-based impact tolerances for services such as transferring funds between accounts, the processing of mortgages, and the ability to perform collateral management.

Current approaches

5.8 Many firms and FMIs will already be setting their own risk appetites.² In suggesting the introduction of impact tolerances for the most important business services, the supervisory authorities seek to provide a focus for some of the existing work many firms and FMIs will already be doing. For instance, firms and FMIs would still set board-agreed risk appetites, but the supervisory authorities consider these could be better informed by detailed impact tolerance statements focused on the most important business services. Similarly, there is still likely to be a need for setting performance metrics on individual systems and processes which support delivery of these services.

5.9 The supervisory authorities are interested in understanding how the approach outlined above differs from firms’ or FMIs’ current activities. In particular, the supervisory authorities are keen to understand what types of metrics firms and FMIs use and which have proved most useful – whether these metrics relate to service downtime, volume of transactions, or anything else.

Figure 5: Combining impact tolerances and scenario testing to establish a proportionate level of operational resilience



1 The Bank’s tolerance is in line with Principle 17 of the PFMI, that requires an FMI to aim to resume operations within two hours following disruptive events, and to complete settlement by the end of the day, even in extreme circumstances.

2 In line with the Basel Committee on Banking Standards’ Principles for the Sound Management of Operational Risk (Principle 4 www.bis.org/publ/bcbs195.pdf), the Basel Committee and International Organization of Securities Commissions’ joint Principles for Financial Market Infrastructures (Principle 2, www.bis.org/cpmi/publ/d101a.pdf), and EIOPA Guidelines on System of Governance (Guideline 19 (Operational Risk Management Policy): https://eiopa.europa.eu/Publications/Guidelines/Final_EN_SoG_Clean.pdf). For PRA-regulated firms, see PRA Supervisory Statement 5/16 ‘Corporate governance: Board responsibilities’, May 2016, www.bankofengland.co.uk/prudential-regulation/publication/2016/corporate-governance-board-responsibilities-ss.

Potential benefits of setting impact tolerances

5.10 The supervisory authorities consider that setting impact tolerances for the most important business services could:

- (a) support firms and FMIs in prioritising investment and resource allocation;
- (b) provide a clear scope when firms and FMIs want to test their own resilience; and
- (c) provide a focus for supervisory engagement.

5.11 By setting and articulating a clear impact tolerance at the business service level, it is possible to define alternative processing procedures that can be deployed in case of disruption to systems and processes in order to remain within impact tolerance. An additional benefit is that it is possible for firms to also consider substitute options more broadly. For example, payments could be routed via other payment schemes in order to remain within impact tolerance, although this may not be economically feasible or straight forward at present for many firms.

5.12 An impact tolerance approach could also address other factors. For instance, firms and FMIs may need to maintain policies for prioritising the provision of a certain level of service in the event of a disruption. This will depend on the type and severity of the operational disruption, and the particular impact the disruption would have. For example, if a bank sets an impact tolerance of delivering a percentage of total payment transactions during a disruption, it would also need a protocol for prioritising payments. Banks could process payments in order of arrival, or prioritise time-critical payments such as house purchases or payments to vulnerable people.

5.13 While an impact tolerance is likely to focus on performance during a single operational disruption, firms and FMIs could also analyse business service delivery over a longer time period to inform their wider risk management. Analysis could include the number of outages in a year, the total length of time that a business service was impaired and the volume of transactions disrupted.

Questions

- E) What are readers' views on the possibility of firms and FMIs being asked to set impact tolerances for their most important business services?
- F) What approach and metrics do firms and FMIs currently use?
- G) If these proposals would require some firms and FMIs to update part of their existing risk management framework, what would this involve?
- H) What are readers' views on producing an impact tolerance statement as described? What relevant operational resilience risk management documentation do firms and FMIs already produce, and how does this differ from impact tolerance statements?

6 Supervisory assessment of operational resilience

This chapter explains how supervisors could gain assurance that firms and FMIs ensure the continuity of their most important business services, and that boards and senior management are sufficiently engaged. The supervisory authorities are reviewing their existing approaches in light of the proposed focus on business services, and are considering the role of scenario testing in this context.

6.1 The supervisory authorities anticipate that a focus on the operational resilience of firms' and FMIs' most important business services will offer the opportunity to review and consolidate existing supervisory tools and assessment practices.

6.2 A future supervisory approach could cover four broad areas, taking into account the specificities of the relevant regulatory regimes for firms and FMIs:

- sector-wide work, including any potential stress testing developed by the Bank and the PRA with input from the FPC;
- supervisory assessment of how firms and FMIs set and use impact tolerances;
- analysis of systems and processes that support business services; and
- assurance that firms and FMIs have the capabilities to deliver operational resilience and are in compliance with existing rules, principles, expectations and guidance.

6.3 The supervisory authorities can deploy a range of existing tools to deliver the above, including questionnaires. The supervisory authorities are seeking to develop their existing supervisory approach in a targeted and proportionate manner.

6.4 Such an approach could provide the supervisory authorities with a layered understanding of both the resilience of individual firms and FMIs, and the financial resilience of the UK economy.

Sector-wide work

6.5 As discussed in the June 2018 FSR (see Box B), a stress-testing approach will be developed by the Bank and the PRA, with input from the FPC.

6.6 In addition, the supervisory authorities already help to coordinate the sector exercising programme sponsored by the Cross Market Operational Resilience Group (CMORG), which is chaired by the Bank and industry. These voluntary exercises rehearse collective response mechanisms, including testing of communication lines, co-ordination arrangements and decision-making processes. Participants are the supervisory authorities, Government, and firms and FMIs at the core of the financial system. The aim is that in a real event the participants are familiar with the actions they need to take, and that the mitigating actions are implemented efficiently to achieve the desired outcomes.

6.7 These exercises also identify ways in which collective response arrangements might be strengthened. Several sector-wide exercises have been organised in the past to rehearse the sector's response to bomb threats, flu pandemic, severe weather and travel disruption. More recently the supervisory authorities simulated and tested the industry's response to an extended outage of the Bank's RTGS system.

6.8 The supervisory authorities also participate in technical desktop exercises organised by the sector. These aim to assess the potential impact from market disruption and consider how it may be mitigated in a major event. Some of these exercises have led to the development of industry-owned resilience playbooks, which set out coordinated approaches to dealing with particular scenarios.

Reviewing how impact tolerances are set and used

6.9 The supervisory authorities are considering how to review the setting of impact tolerances, whether there is clear governance and accountability, and how the impact tolerances are tested. The translation of impact tolerances into actual investment decisions and contingency planning is of particular interest.

6.10 The supervisory authorities envisage impact tolerance statements being the responsibility of individual firms and FMIs, and would look to them to explain how their impact tolerances link to their ongoing viability, the potential harm to consumers and market participants, and any potential impact on financial stability. The supervisory authorities might not agree with a firm's or FMI's impact tolerance statement. This might be because the supervisory authorities have more information than the firm or FMI, or because the relevant authority makes a different judgement. In such cases, the appropriate supervisory authority would ask the firm or FMI to revise its impact tolerance.

6.11 The supervisory authorities may also consider setting their own impact tolerances for firms or FMIs to meet within the context of severe, but plausible, scenarios.

Analysis of systems, people and processes that support business services

6.12 The supervisory authorities would seek to gain further assurance that firms and FMIs have taken appropriate tangible steps to increase their operational resilience. At a minimum, firms and FMIs would be able to map the systems, people and processes that support their business services. This would include dependencies outside of their firm and not be restricted by geography. They would also ensure that they have appropriate communications plans in place, for when disruption to a business service occurs.

6.13 As explained earlier in this DP, the assumption of failure is likely to be fundamental to the supervisory authorities' approach. The supervisory authorities might focus on the back-up systems, redundancies, substitutability arrangements and other measures firms and FMIs have put in place and the extent to which a firm or FMI has self-assessed its resilience using scenarios. Supervisors might also conduct targeted assessments of firms' and FMIs' operational infrastructure, activities, decision-making and their supporting data.

Gaining assurance that firms and FMIs have the capabilities to deliver operational resilience

6.14 The overall resilience of firms and FMIs is the result of how all their practices, processes and culture – collectively 'capabilities' – combine to allow them to adapt and respond to operational disruption. As part of this approach, the supervisory authorities would consider how effective the board is in providing governance and leadership to their organisation's resilience work, and in developing the necessary capabilities.

6.15 The supervisory authorities would be likely to use firms' and FMIs' own risk management as a starting point for operational resilience supervision. They are also considering setting scenarios for firms to test (not dissimilar to some of the current elements of the PRA's capital framework). An objective of using scenarios would be to help determine which firms or FMIs need to develop their operational resilience.

6.16 Where development is required, firms' and FMIs' actions could include the identification and rehearsal of alternative processing procedures; system design offering greater substitutability at the service level; outsourcing; or third party substitutability arrangements.

Supervisory tools

6.17 Regular supervisory engagement and review of firms' and FMIs' own risk management is already complemented by a range of specific tools which the supervisory authorities currently apply on a proportionate basis. Such review work typically targets specific risks and can be undertaken in a variety of ways including questionnaires, simulations, skilled persons' or experts' reports and wider thematic reviews. Firms' recovery and resolution plans and OCIR arrangements, where applicable, can also be useful sources of information for the supervisory authorities.

6.18 The supervisory authorities could make an increased use of questionnaires to assess operational resilience in future, potentially drawing on existing frameworks which support assessment of firms' and FMIs' capabilities. Existing frameworks include the CPMI-IOSCO guidelines, the G7 Fundamental Elements of Cybersecurity, the National Institute of Standards & Technology (NIST) Cybersecurity Framework, and the National Cyber Security Centre (NCSC) Cyber Assessment Framework.

6.19 A capabilities assessment questionnaire could be derived from the existing NIST principles, which set out that companies should: identify potential vulnerabilities and sources of risk, seek to protect themselves from threats, detect incidents, respond to, and recover from disruptions.

Questions

- I) What operational resilience tests or scenarios do firms and FMIs already consider and undertake for their own risk management purposes? What factors do firms and FMIs take into account when devising operational resilience tests or scenarios?
- J) How do boards and senior management currently gain assurance over the operational resilience of their firm or FMI?
- K) What are readers' views on the proposed developments to the supervisory authorities' approach to operational resilience?

7 Conclusion

7.1 This DP aims to promote an open and constructive dialogue with stakeholders, and share the supervisory authorities' current thinking on how the operational resilience of the financial services sector could be enhanced.

7.2 The supervisory authorities are exploring a business services approach because it could be of value to organisations of all sizes as they manage their resilience in a dynamic environment. A focus on business services could help increase the transparency of firms' and FMIs' resilience work. It could drive better decision-making, as it would enable prioritisation of resilience work and the associated investment. It would provide a basis for firms and FMIs to set impact tolerances, set with reference to the supervisory authorities' objectives. The supervisory authorities themselves might also see the need to set impact tolerances for some business services.

7.3 The concept of impact tolerance is core to the supervisory authorities' thinking and may challenge firms and FMIs to think differently. It encourages them to assume operational disruptions will occur. This means that attention can be directed towards minimising the impact of disruption on important business services. Impact tolerance focuses firms, FMIs and the supervisory authorities on the potential vulnerabilities in business and operating models. The work they do to increase the resilience of these need not be tied to specific threats, rather an important business service should be made resilient to a wide variety of threats.

7.4 Firms' and FMIs' processes, practices and culture need to work effectively to achieve the increased level of operational resilience that they and the supervisory authorities seek. This DP suggests an approach for potential supervisory expectations and assessment:

- Preparation: firms and FMIs identify and focus on the continuity of their most important business services as a means of prioritising their own analysis, work and investment in operational resilience. They set impact tolerances for their important business services and are able to demonstrate substitutability or the capability to adapt processes during disruption.
- Recovery: firms and FMIs assume disruptions will occur, and develop the means by which they can adapt their business processes and practices in the event of shocks in order to preserve continuity of service.
- Communications: firms and FMIs have strategies for communicating with their internal and external stakeholders, including the supervisory authorities and consumers. This should include how to handle the situation to minimise the consequences of disruption.
- Governance: firms' and FMIs' boards and senior management are crucial in setting the business and operational strategies and overseeing their execution in order to ensure operational resilience.

Responses and next steps

7.5 The supervisory authorities welcome feedback on this DP, including any specific suggestions, issues, or potential alternatives.

7.6 The supervisory authorities will work together to reflect on the feedback as they: develop potential proposals for consultation; develop their respective supervisory approaches; and work with the FPC as it develops its own impact tolerances. The supervisory authorities will also be

drawing together existing policy material related to operational resilience in order to support firms and FMIs to build their resilience.

7.7 The supervisory authorities have found that collaboration with firms, FMIs, security and other public and private sector organisations provides a constructive approach to promoting operational resilience. They intend to continue this strategy, working with other organisations in both authority-led and industry fora. The supervisory authorities believe that cooperation in this area is vital to achieving good operational resilience outcomes and financial stability.

8 Feedback and questions

8.1 The supervisory authorities encourage responses to the questions posed and any other observations that readers may have in response to this DP by Friday 5 October 2018. Responses and input from a wide range of stakeholders including regulated firms, FMIs, consumers, industry bodies, auditors, specialist third-party providers, professional advisors and other regulators are welcomed. Contact details are provided on page 3 of this document.

8.2 The supervisory authorities will use these responses to inform current supervisory activity and future policy-making. The supervisory authorities will share relevant information with the FPC to inform its approach to building cyber resilience in the UK financial system. They may publish extracts or summaries of views from respondents.¹

- A) What are readers' views on the proposed focus on continuity of business services? Would a service rather than systems-based approach represent a significant change for firms and FMIs compared with existing practice? What other approaches could be considered?
- B) Would encouraging firms and FMIs to consider their contribution to the vital services that the real economy demands change the way they manage operational resilience, and if so how? What additional costs would this incur?
- C) How do boards and senior management currently prioritise their work on operational resilience?
- D) What changes are firms and FMIs planning to make to strengthen operational resilience over the next few years? How involved are board members in the planning, implementation and embedding of any changes? What are the likely benefits and costs involved?
- E) What are readers' views on the possibility of firms and FMIs being asked to set impact tolerances for their most important business services?
- F) What approach and metrics do firms and FMIs currently use?
- G) If these proposals would require some firms and FMIs to update part of their existing risk management framework, what would this involve?
- H) What are readers' views on producing an impact tolerance statement as described? What relevant operational resilience risk management documentation do firms and FMIs already produce, and how does this differ from impact tolerance statements?
- I) What operational resilience tests or scenarios do firms and FMIs already consider and undertake for their own risk management purposes? What factors do firms and FMIs take into account when devising operational resilience tests or scenarios?
- J) How do boards and senior management currently gain assurance over the operational resilience of their firm or FMI?
- K) What are readers' views on the proposed developments to the supervisory authorities' approach to operational resilience?

¹ Respondents should indicate if they wish all or part of a response to be kept confidential. For further information on how information provided in response to this DP may be used see the privacy notice on page 2.

Annexes

-
- | | |
|----------|--------------------------|
| 1 | Glossary of terms |
|----------|--------------------------|
-
- | | |
|----------|---|
| 2 | Economic functions listed in SS19/13 |
|----------|---|
-
- | | |
|----------|---|
| 3 | Examples of relevant existing requirements |
|----------|---|
-
- | | |
|-----------|---|
| 3A | Examples of relevant existing PRA requirements |
|-----------|---|
-
- | | |
|-----------|--|
| 3B | The Bank's regulatory framework for the supervision of FMIs |
|-----------|--|
-
- | | |
|-----------|---|
| 3C | Examples of relevant existing FCA requirements |
|-----------|---|

Annex 1: Glossary of terms

Business services

Products and services that a firm or FMI provides to its customers. These will vary by firm or FMI, but examples could include the delivery and management of particular loan or insurance products.

Capabilities

The practices, processes and culture within a firm or FMI that deliver operational resilience.

Clearing House Automated Payment System (CHAPS)

CHAPS is a sterling same-day system used to settle high-value wholesale payments as well as time-critical, lower-value payments like buying or paying a deposit on a property.

Cloud services

Cloud services are remote access services and infrastructure.

Continuity

In the context of this DP, continuity refers to the ongoing provision of a business service.

Economic functions

The broad set of services the financial sector provides to the UK economy, and hence an aggregation of business services that one, or more, firms or FMIs provide. For example, the economic function of retail mortgages and secured lending would comprise a number of individual business services. If sufficiently significant in terms of both size and function, these economic functions can become critical to the UK economy.

Financial Market Infrastructure (FMI)

A multilateral system among participating institutions, including the operator of the system, used for the purposes of clearing, settling, or recording payments, securities, derivatives, or other financial transactions.

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (Regulation 2016/679) regulates the processing of personal data relating to individuals in the EU by other individuals, companies or organisations.

Impact tolerances

Describe firms' and FMIs' tolerance for disruption, under the assumption that disruption to a particular business service will occur. Impact tolerance is expressed by reference to specific outcomes and metrics. Such metrics could include the maximum tolerable duration or volume of disruption, the criticality of ensuring data integrity or the number of customers affected. Impact tolerances are different from risk appetite, in the sense that they assume a particular risk has crystallised, but they will inform the risk appetite of a firm or FMI's board and senior management.

Impact tolerance statement

For the purposes of this DP, the supervisory authorities envisage that how impact tolerances are derived and justified might be set out in a single document called an impact tolerance statement.

Integrity

In the context of this DP, integrity describes data being accurate and complete.

Operational resilience

For the purposes of this DP, operational resilience refers to the ability of firms, FMIs and the system as a whole to prevent, adapt and respond to, recover and learn from, operational disruption. In this DP, the supervisory authorities focus on the continued delivery of business services or economic functions.

Operational risk

Operational risk refers to the risk of loss from inadequate or failed processes, people or systems or from external events. Threats to firms' and FMIs' operations take a wide variety of forms.

Risk appetite

A firm's risk appetite is the amount and type of risk a firm is willing to accept, or avoid, in order to achieve its business objectives. When aggregated in a single document, this is referred to as a risk appetite statement.

Real economy

The production of goods and services within an economy.

Real-Time Gross Settlement (RTGS) service

Infrastructure that holds accounts for banks, building societies and other institutions. The balances in these accounts can be used to move money in real time between these account holders. This delivers final and risk-free settlement.

Senior Manager's and Certification Regime (SM&CR) and Senior Insurance Managers Regime (SIMR)

Rules in the PRA Rulebook and FCA Handbook ('Senior Management Functions' (SMF)) requiring firms to appoint managers, approved by the regulator, who are responsible for specific areas and each of the firms' business functions and activities. SMF24 in particular is the Chief Operations function, which has responsibility for the internal operations and technology, currently of banks, dual-regulated investment firms and building societies.

Supervisory authorities

The collective term for the PRA, the FCA, and the Bank of England (in its capacity of supervising FMIs).

Systems and processes

The underlying software, people, assets, policies and procedures that support the delivery of business services.

Vital services

The key services that the real economy demands from the financial system: providing the main mechanism for paying for goods, services and financial assets; intermediating between savers and borrowers, and channelling savings into investment, via debt and equity instruments; and insuring against and dispersing risk.

Annex 2: Economic functions listed in SS19/13

The table below is reproduced from PRA Supervisory Statement 19/13 Resolution Planning.¹ It may be useful to firms and FMIs in identifying the business services they provide and considering how they may link to UK economic functions.

Economic Functions	
Deposit-taking and savings	Retail Current Accounts
	SME Current Accounts
	Retail Savings Accounts / Time Accounts
	SME Savings Accounts
	Corporate Deposits
Lending and loan servicing	Retail Mortgages / Other Secured (Auto)
	Retail Unsecured Personal Lending
	Retail Credit Cards
	SME Lending (Secured)
	Corporate Lending
	Trade Finance
	Infrastructure Lending
	Credit Card Merchant Services
Capital Markets & Investment	Derivatives
	Trading portfolio
	Asset Management
	General Insurance
	Life insurance, pensions, investments and annuities
Wholesale Funding Markets	Securities Financing
	Securities Lending
Payments, clearing, custody and settlement	Payment Services
	Settlement Services
	Cash Services
	Custody Services
	Third-Party Operational Services

¹ January 2015: www.bankofengland.co.uk/prudential-regulation/publication/2013/resolution-planning-ss.

Annex 3: Examples of relevant existing requirements

There is an existing body of rules, expectations, principles and guidance related to operational resilience which is applicable to PRA and FCA regulated firms and FMIs supervised by the Bank. This annex does not intend to provide a comprehensive list of relevant regulation but points to some of these by way of illustration.

Annex 3A: Examples of relevant existing PRA requirements

International and European Requirements

The Basel Committee on Banking Supervision (BCBS) has developed principles relevant to operational resilience. These include the *Corporate Governance Principles for Banks* (principles 6 to 10)¹ and the *Principles for the Sound Management of Operational Risk*.² The *Principles for the Sound Management of Operational Risk* have been taken into account in the development of relevant legislation, such as CRR and the Markets in Financial Instruments Directive (MiFID), and the *Corporate Governance Principles for Banks* are covered by the EBA's guidelines on internal governance.

European law, including the Capital Requirements Directive (CRD IV),³ MiFID II,⁴ and Solvency II has requirements which support resilience:

- CRD IV states that firms should have effective processes to identify, manage, monitor and report the risks they are or might be exposed to.⁵ It also states that firms should ensure that contingency and business continuity plans are in place to ensure an institution's ability to operate on an ongoing basis and limit losses in the event of severe business disruption.⁶
- MiFID II states that investment firms should ensure, when relying on a third party for the performance of operational functions which are critical for the provision of continuous and satisfactory service to clients and the performance of investment activities on a continuous and satisfactory basis, that they takes reasonable steps to avoid undue additional operational risk.⁷
- Solvency II states that insurance and reinsurance undertakings shall have in place an effective risk management system comprising strategies, processes and reporting procedures necessary to identify, measure, monitor, manage and report, on a continuous basis the risks, at an individual and at an aggregated level, to which they are or could be exposed, and their interdependencies.⁸

1 BCBS 'Corporate governance principles for banks', July 2015: www.bis.org/bcbs/publ/d328.pdf.

2 BCBS, 'Principles for the Sound Management of Operational Risk', June 2011: <https://www.bis.org/publ/bcbs195.pdf>.

3 Capital Requirements Directive (2013/36/EU) (CRD) and Capital Requirements Regulation (575/2013) (CRR) – jointly 'CRD IV': <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0036&from=EN>.

4 Markets in Financial Instruments Directive (2014/65/EU) (MiFID II): <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0065&from=EN>.

5 Capital Requirements Directive (2013/36/EU) (CRD) and Capital Requirements Regulation (575/2013) (CRR) – jointly 'CRD IV', (74.1): <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0036&from=EN>.

6 Capital Requirements Directive (2013/36/EU) (CRD) and Capital Requirements Regulation (575/2013) (CRR) – jointly 'CRD IV', (85.2): <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0036&from=EN>.

7 Markets in Financial Instruments Directive (2014/65/EU) (MiFID II), (16.5): <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0065&from=EN>.

8 Solvency II Directive (2009/138/EC), (44.1): <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0138&from=EN>.

PRA Requirements

The PRA's Threshold Conditions require firms to conduct their business prudently.¹ This includes having appropriate non-financial resources to identify, monitor, measure and take action to remove or reduce risks to their safety and soundness.²

The PRA's Fundamental Rules build on this, and include the requirements that firms must:

- conduct business with due skill, care and diligence;³
- act in a prudent manner;⁴
- have in place effective risk strategies and risk management systems;⁵ and
- organise and control their affairs responsibly and effectively.⁶

The PRA Rulebook then contains detailed requirements that support firms' operational resilience. These include the General Organisational Requirements and Senior Managers Regime Parts, which are supported by clear expectations.

- The PRA's General Organisational Requirements contains rules on risk management, monitoring and reporting; the security, integrity and confidentiality of information; business continuity and contingency planning; and internal controls.⁷ These rules are supplemented by expectations around business continuity planning,⁸ the Chief Risk Officer's role,⁹ and the responsibilities of the governing body risk committee.¹⁰
- The Senior Managers Regime requires that lines of accountability are established within firms, including a Chief Operations Senior Management Function (SMF24), which has responsibility for the internal operations and technology of a firm, including cybersecurity, operational resilience and operational continuity.¹¹

1 See Box 1 of the PRA's Approach to Banking Supervision, <https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/approach/banking-approach-2016>.

2 Financial Services and Markets Act 2000 (FSMA), 2000, Part 1E 5D 4 (b): <https://www.legislation.gov.uk/ukdsi/2013/9780111533802>

3 Fundamental Rule 2 in the Fundamental Rules Part of the PRA Rulebook: <http://www.prarulebook.co.uk/rulebook/Content/Part/211136/30-11-2015>.

4 Fundamental Rule 3 in the Fundamental Rules Part of the PRA Rulebook: <http://www.prarulebook.co.uk/rulebook/Content/Part/211136/30-11-2015>.

5 Fundamental Rule 5 in the Fundamental Rules Part of the PRA Rulebook: <http://www.prarulebook.co.uk/rulebook/Content/Part/211136/30-11-2015>.

6 Fundamental Rule 6 in the Fundamental Rules Part of the PRA Rulebook: <http://www.prarulebook.co.uk/rulebook/Content/Part/211136/30-11-2015>.

7 Rules 2.1-2.8 in the General Organisational Requirements Part of the PRA Rulebook: www.prarulebook.co.uk/rulebook/Content/Part/214136/30-11-2019.

8 Paragraph 2.1, PRA Supervisory Statement 21/15, 'Internal Governance', April 2017: www.bankofengland.co.uk/prudential-regulation/publication/2015/internal-governance-ss.

9 Paragraph 2.28-31, April 2017: www.bankofengland.co.uk/prudential-regulation/publication/2015/internal-governance-ss.

10 Paragraph 2.32-35, April 2017: www.bankofengland.co.uk/prudential-regulation/publication/2015/internal-governance-ss.

11 PRA Supervisory Statement 28/15, 'Strengthening individual accountability in banking', May 2017: www.bankofengland.co.uk/prudential-regulation/publication/2015/strengthening-individual-accountability-in-banking-ss.

Annex 3B: The Bank's regulatory framework for the supervision of FMIs

FMIs are required to consider their operational risk and reliability by the CPMI-IOSCO *Principles for Financial Market Infrastructures* (PFMI).¹ The principles set out international standards that FMIs should follow in areas such as governance arrangements, financial resources and risk management. The principles that deal with financial resources also include some operational standards in respect of the processes that deliver financial resilience.

The Bank's supervisory approach is based on application of the principles to FMIs. The key outcomes it seeks to achieve in applying the principles are the continuity of service of the FMI and the FMI's effective management of systemic risk.

The most relevant Principle to operational resilience is Principle 17 (Operational risk). It includes recommendations around the themes of:

- operational risk management (3.17.4-3.17.8)
- operational reliability (3.17.9)
- incident management (3.17.10)
- operational capacity (3.17.11)
- physical and information security (3.17.12)
- business continuity management (3.17.13-3.17.17)
- interdependencies between the FMI and its participants (3.17.18-3.17.22)

Other sections of the PFMI are also relevant to operational resilience, such as:

- FMIs 'should have objectives that place a high priority on the safety and efficiency of the FMI and explicitly support financial stability and other relevant public interest considerations' (Principle 2, Key Consideration 1).
- FMI's board should 'establish a clear, documented risk management framework that includes the FMI's risk tolerance policy, assigns responsibilities and accountability for risk decisions, and addresses decision making in crises and emergencies' (Principle 2, Key Consideration 6).
- FMI should 'regularly review the material risks it bears from and poses to other entities² as a result of interdependencies and develop appropriate risk-management tools to address these risks' (Principle 3, Key Consideration 3).
- FMI should 'identify scenarios that may potentially prevent it from being able to provide its critical operations and services as a going concern and assess the effectiveness of a full range of option for its recovery or orderly wind-down based on the result of that assessment' (Principle 3, Key Consideration 4).

1 The International Organization of Securities Commissions (IOSCO), along with the Committee on Payments Systems and Market Infrastructures (CPMI) published the PFMI in 2012. The Bank contributed to the development of the PFMIs.

2 Such as other FMIs, settlement banks, liquidity providers and service providers.

- A critical service provider is expected to identify and manage relevant operational and financial risks to its critical services and ensure that its risk-management processes are adequate. The operational reliability of an FMI may be dependent on the continuing provision of critical services (Annex F).

The PFMI are formally applied to Central Counter Parties and Central Securities Depositories through the European regulatory regimes (EMIR and CSDR). There is, however, no equivalent legislative framework applying the PFMI to payment systems.

Annex 3C: Examples of relevant existing FCA requirements

Many existing statutory requirements, FCA rules and guidance and European legislation are relevant to a firm's operational resilience. The examples summarised below start with general requirements that apply to the majority of firms we supervise, and then refer to some sector-specific requirements.

The Principles

At a high level, the FCA's Principles for Business set out general statements of the fundamental obligations for firms and includes: *'A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems'*.¹

The Threshold Conditions and COND

The Threshold Conditions² represent the minimum conditions which a firm is required to continue to satisfy to be given and retain permission to carry on regulated activities under Part 4A FSMA. COND in the FCA handbook provides guidance on how the FCA will approach its assessment of applicable threshold conditions.

Of particular relevance is the FCA's assessment of the risks to the continuity of the services under the appropriate non-financial resources threshold condition for dual-regulated firms³ or the appropriate resources threshold condition for solo-regulated firms.⁴ COND 2.4.4G, which provides guidance on the assessment of this Threshold Condition includes the following: *'whether the firm has taken reasonable steps to identify and measure any risks of regulatory concern that it may encounter in conducting its business and has installed appropriate systems and controls and appointed appropriate human resources to measure them prudently at all times.'*⁵

When considering the 'Business Model' Threshold Condition⁶ guidance, COND provides: *'Firms should consider scenarios which may negatively impact on the firm's business model with a view to ensuring the sustainability of the firm and, further, to consider the vulnerability of the business model to specific events and the risks and consequences that might arise. Where appropriate, this might include reverse stress-testing (see SYSC 20 'Reverse stress testing'). A firm should put in place a credible plan to minimise the risks that it identifies from, or in relation to, its business model and a contingency plan for dealing with risks that have crystallised.'*⁷

SYSC - Senior Management Arrangements, Systems and Controls

SYSC includes rules and guidance about risk management and risk-centric governance arrangements.⁸ Many of these rules derive from European law, such as the Markets in Financial Instruments Directive (MiFID)⁹ and the Capital Requirements Directive (CRD).¹⁰ For example:

- SYSC 4.1.1R(1)¹ states that: 'A firm must have robust governance arrangements, which include a clear organisational structure with well defined, transparent and consistent lines of

1 Principle 3, PRIN 2.1.

2 Schedule 6 to Financial Services and Markets Act 2000 (FSMA).

3 Paragraph 3C to Schedule 6 of FSMA.

4 Paragraph 2D to Schedule 6 of FSMA.

5 COND 2.4.4G(2)(d).

6 Paragraph 2F to Schedule 6 of FSMA for solo-regulated firms, Paragraph 3E to schedule 6 of FSMA for dual-regulated firms.

7 COND 2.7.10G.

8 For the detailed application of the SYSC Sourcebook see SYSC 1 Annex 1 and the text in relevant chapters in SYSC.

9 Markets in Financial Instruments Directive 2014/65/EU.

10 Capital Requirements Directive 2013/36/EU.

responsibility, effective processes to identify, manage, monitor and report the risks it is or might be exposed to, and internal control mechanisms, including sound administrative and accounting procedures and effective control and safeguard arrangements for information processing systems'.²

- SYSC 4.1.6R to 4.1.7R³ sets out rules relating to business continuity for common platform firms, CRR firms and management companies as defined in the FCA handbook⁴. For example SYSC 4.1.6R provides: *'A common platform firm must take reasonable steps to ensure continuity and regularity in the performance of its regulated activities. To this end the common platform firm must employ appropriate and proportionate systems, resources and procedures'*. SYSC 4.1.8G gives guidance on the matters that should be dealt with in a business continuity plan.
- SYSC 7.1 includes further provisions on risk control for certain firms and SYSC 21.1 provides guidance on risk-centric governance arrangements, including guidance on whether a Chief Risk Officer should be appointed and a governing body risk committee established.
- SYSC 13 sets out detailed guidance for insurers about management of operational risk. For example, SYSC 13.8.5G says: *'A firm should consider the likelihood and impact of a disruption to the continuity of its operations from unexpected events. This should include assessing the disruptions to which it is particularly susceptible (and the likely timescale of those disruptions) including through: (1) loss or failure of internal and external resources (such as people, systems and other assets); (2) the loss or corruption of its information; and (3) external events (such as vandalism, war and 'acts of God')'*.
- SYSC 8.1 contains provisions relating to outsourcing. The FCA has also published 'Guidance for firms outsourcing to the 'cloud' and other third-party IT services', FG 16/5.
- Firms should be aware of other outsourcing and risk-management related requirements that may apply within the FCA Handbook and in other legislation including directly applicable EU legislation, such as the MiFID Org Regulation⁵ and relevant ESA guidelines.

Sector specific requirements (examples)

Trading venues - Recognised Investment Exchanges (RIEs) - REC

All UK investment exchanges must meet certain requirements to obtain recognition from the FCA⁶. Recognition requirements include the UK RIE ensuring that its systems and controls are adequate, effective and appropriate for the scale and nature of its business. Systems and controls relevant to operational resilience include those concerning: risk management; technical operation of the exchange including contingency arrangements, the resilience of its trading systems and the effectiveness of business continuity arrangements.⁷ REC 2.5.5G to REC 2.5.20G in the FCA Handbook

1 SYSC 4.1.1R(1) transposes article 74 (1) of CRD, article 16(5) second paragraph of MiFID, article 12(1)(a) of the UCITS Directive (Undertakings for collective investment in transferable securities 2009/65/EC), and article 18(1) of AIFMD (Alternative Investment Fund Managers Directive 2011/61/EU).

2 See SYSC 3.1 and 3.2, especially SYSC 3.1.1R and 3.2.6R for insurers, managing agents and the Society and FUND 3.7 for full-scope UK AIFM of an authorised AIF.

3 SYSC 4.1.6R transposes article 16(4) of MiFID and SYSC 4.1.7R transposes article 4(3) of the UCITS Implementing Directive and article 85(2) of CRD.

4 Other firms should take account of the business continuity rules at SYSC 4.1.6 R and 4.1.7 R as if they were guidance – SYSC 4.1.7AG.

5 Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing MiFID of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive. The MiFID Org Regulation contains requirements relevant to operational resilience that apply to some firms. As regards the application of the MiFID Org Regulation see MG2 The MiFID 2 Guide in the FCA Handbook and relevant parts of SYSC.

6 Recognition is given under Part 18 FSMA. The recognition requirements are contained in the Financial Services and Markets Act 2000 Recognition Requirements for Investment Exchanges Clearing Houses and Central Securities Depositories Regulations 2001 (SI 2001/995) – the Recognition Requirements Regulations.

7 Schedule to the Recognition Requirements Regulations, part 1, paragraphs 3.

provides guidance on matters to which the FCA may have regard in assessing such systems and controls and certain other aspects of the RIE's operations.

Multilateral trading facilities¹ and Organised trading facilities² - MAR- Market Conduct

MAR contains rules and guidance regarding risk management and contingency arrangements also derived from MiFID. Examples of relevant rules include:

- For Multilateral trading facilities (MTFs) - MAR 5.3.1R(2A) (contingency arrangements to cope with the risks of system disruption) and 5.3.1AR(2) (risk management).
- For Organised trading facilities (OTFs) - MAR 5A.4.1R(3) (contingency arrangements to cope with risks of systems disruption).
- Rules and guidance relating to systems and controls for algorithmic trading are contained in MAR 5.3A for MTFs, MAR 5A.5 for OTFs and MAR 7A.3 for UK MiFID investment firms and third country investment firms.³

Directly applicable European legislation relevant to operational resilience may also apply. For example:

- Article 15 of MiFID RTS 74 relates to business continuity arrangements for trading venues and requires that: '1. Trading venues shall be able to demonstrate at all times that their systems have sufficient stability by having effective business continuity arrangements to address disruptive incidents. 2. The business continuity arrangements shall ensure that trading can be resumed within or close to two hours of a disruptive incident and that the maximum amount of data that may be lost from any IT service of the trading venue after a disruptive incident is close to zero.'

Payment Services Regulations (PSRs 2017)⁵ and Electronic Money Regulations 2011 (EMRs 2011)⁶

Both Regulations contain requirements relevant to operational resilience. See, for example, Regulation 98 *Management of operational and security risks* and Regulation 99 *Incident reporting* in the PSRs 2017. Further information can be found in the FCA publication - *Payment Services and Electronic Money – Our Approach*.

1 As defined in the FCA Handbook.

2 As defined in the FCA Handbook.

3 As defined in the FCA Handbook.

4 Commission Delegated Regulation (EU) No 2017/584 of 14 July 2016 supplementing MiFID with regard to regulatory technical standards specifying organisational requirements of regulated markets, multilateral trading facilities and organised trading facilities enabling or allowing algorithmic trading through their systems.

5 The Payment Services Regulations 2017 (SI 2017/752) which implement the revised Payment services Directive PSD2.

6 The Electronic Money Regulations 2011 (SI 2011/99).