



BANK OF ENGLAND



Building operational resilience: Impact tolerances for important business services

Bank CPs relating to FMIs | Bank of England (Bank)

CP29/19 | Prudential Regulation Authority (PRA)

CP19/32 | Financial Conduct Authority (FCA)

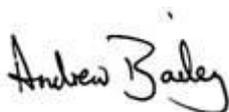
Foreword

A key priority for the Bank of England, Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) is to put in place a stronger regulatory framework to promote operational resilience of firms and financial market infrastructures (FMIs). To this end, we published our joint Discussion Paper on Operational Resilience last year to start a dialogue with the financial services industry. We received an impressive level of engagement from industry and two key conclusions have emerged: (1) there is strong support for our proposed approach but respondents asked for a fuller explanation; and (2) many stakeholders see a strong alignment between the goals of firms or FMIs and the authorities in this area.

As a consequence, the policy proposals we are bringing forward for consultation, we believe, go with the grain of thinking in the industry. While these proposals are tailored to the individual policy frameworks and supervisory approach of each respective authority, they share a common overarching approach to operational resilience. We strongly encourage firms to take ownership of their own operational resilience and to prioritise based on the impacts to the public interest, as represented by the authorities' objectives.

Specifically, we expect firms and FMIs to identify their important business services. While we are not introducing a definitive list, we are providing further guidance on the type of business services that boards and senior management could classify as 'important'. We then expect firms to set an impact tolerance for each of these services, quantifying the maximum acceptable level of disruption through severe (or extreme in the case of FMIs) but plausible scenarios. Firms and FMIs are responsible for setting their own tolerances, and boards and senior management should take actions to improve operational resilience where limitations are identified in a firm's or FMI's ability to remain within these tolerances. This is where firms and FMIs should expect close supervisory scrutiny and engagement.

Co-operation and close joint working between the authorities has been effective in developing this new thinking, and we would encourage a similar collaborative approach among firms, FMIs and industry bodies. Ultimately, operational failures undermine all of our objectives and we will all need to continue to make progress.



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

Contents	1
1 Introduction	2
Box A: The supervisory authorities' objectives	3
Significant changes since the DP	3
Summary of the approach	4
Treasury Select Committee (TSC) report on 'IT failures in the Financial Services Sector'	5
2 Important business services	6
Business services	7
'Important' business services	7
Identifying important business services	7
3 Impact tolerances	8
Setting impact tolerances	8
Impact tolerance and risk appetites	8
Impact tolerances for dual-regulated firms	9
4 Delivering operational resilience	9
Taking action to building operational resilience	9
Severe (or in the case of FMIs, extreme) but plausible scenarios	10
Scenario testing	11
Mapping	11
Existing requirements	12
5 Next steps	12
Policy proposals	12
Relationship with the Financial Policy Committee (FPC)	12
Industry engagement	13
International	13

1 Introduction

1.1 This paper 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'.

1.2 The Discussion Paper 'Building the UK Financial Sector's Operational Resilience' (the DP), published in July 2018, set out an approach to operational resilience.¹ On Thursday 5 December 2019, the supervisory authorities published a suite of documents² ('the proposals'), which would embed that approach into policy. This paper provides a summary of the overall approach and development since the DP.

1.3 A lack of operational resilience represents a threat to each of the supervisory authorities' objectives, as well as to their shared goal of maintaining financial stability (see Box A). Therefore the supervisory authorities have continued to work together to take a consistent approach in their proposed policies on operational resilience for firms and FMIs. There is benefit to firms and FMIs in having a consistent approach, and, in particular, the FCA and PRA supervisory teams will work together on consistent application of their respective policies to dual-regulated firms.³

1.4 The proposed policies will comprise new rules (for the FCA and PRA), principles, expectations and guidance, and will be implemented through the authorities' respective supervisory areas. Not all firms would be subject to the formal policy proposals. Readers should refer to the consultation documents for the proposed scope of the policies. Due to different legislation and regulatory frameworks under which the PRA, the FCA and the Bank operate, the approach taken by each supervisory authority is not identical but their intended outcomes are aligned.

1.5 Detailed proposals from each supervisory authority are set out in the package of publications:

- a PRA Consultation Paper (CP), which includes draft rules, a draft Statement of Policy (SoP), and a draft Supervisory Statement (SS). On Thursday 5 December 2019 the PRA also published a CP which includes a draft SS on outsourcing and third party risk management which is a key part of operational resilience, and firms are encouraged to read this alongside the PRA's operational resilience CP;⁴
- a CP issued by the FCA, which includes draft rules and draft guidance. The FCA CP also contains a chapter on outsourcing; and
- individual CPs and draft SSs issued by the Bank for central counterparties, and central securities depositories. The Bank is also publishing a CP, a draft SS and a draft operational resilience chapter of the Code of Practice for recognised payment system operators and specified service providers.

¹ Bank DP1/18, PRA DP1/18 and FCA DP18/04: <https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper>.

² PRA CP29/19: Operational resilience: impact tolerances for important business services, FCA CP19/32: Building operational resilience: impact tolerances for important business services and feedback to DP18/04, Bank CP Operational Resilience: Central counterparties, Bank CP Operational Resilience: Central securities depositories and Bank CP Operational Resilience: Recognised Payment Systems and Specified Service providers.

³ There are no dual supervised FMIs.

⁴ PRA CP30/19 'Outsourcing and third party risk management': <https://www.bankofengland.co.uk/prudential-regulation/publication/2019/outsourcing-and-third-party-risk-management>.

Box A: The supervisory authorities' objectives

The Bank has an objective to protect and enhance the financial stability of the United Kingdom.⁵ The Bank sets out in its Financial Stability Strategy⁶ that financial stability is the consistent supply of the vital services that the real economy demands from the wider financial sector. 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 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 securing 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's wider financial sector, and to promote effective competition in the interests of consumers. In achieving these objectives, both regulators seek to support financial stability.

Significant changes since the DP

1.6 The supervisory authorities received 95 responses to the DP. The respondents included trade associations, banks, investment firms, insurers, building societies, FMIs, other regulators and consultancy firms. Respondents supported the supervisory authorities' intention to focus on the delivery of important business services as a way of strengthening operational resilience.

1.7 Respondents sought further information about how the ideas in the DP would work in practice. This included: how business services would be defined; how impact tolerances would be set and tested; and what reliance firms and FMIs would be able to place on the resilience of their third party and intra-group service providers. Respondents indicated that the future policy would be easier to implement if international regulation of operational resilience was closely aligned across different jurisdictions (see Chapter 5).

1.8 The supervisory authorities have worked together to take into account the feedback they received on the DP. The most significant changes in the proposals when compared with the DP are:

- **The definition of important business service:** The DP defined business services as 'Products and services that a firm or FMI provides to its customers'. In the proposals, the supervisory authorities refine their definition of important business services. Firms and FMIs are required to consider the chain of activities which make up a business service, from taking on an obligation, to delivery of the service, and determine which part of the chain is critical to delivery. The

5 Bank of England Act 1998, section 2A: <https://www.legislation.gov.uk/ukpga/1998/11/section/2A#commentary-key-8734b5fd971e45bddd681573bfa3213>.

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

supervisory authorities propose that all resources that are required to deliver that part of the service, the important business service, should be operationally resilient (see Chapter 2).

- **The definition of impact tolerance:** The DP defined impact tolerances as firms' and FMIs' tolerance for disruption under the assumption that disruption to a particular business service will occur, expressed by reference to specific outcomes and metrics. In the proposals, the supervisory authorities clarify that impact tolerances should include the maximum tolerable level of such disruption. Where relevant, firms and FMIs may decide impact tolerances can also include other metrics such as volumes and values (see Chapter 3).
- **Actions to achieve operational resilience:** The DP did not detail the actions firms and FMIs would be expected to take after identifying vulnerabilities in their operational resilience. In the proposals, the supervisory authorities explain that firms and FMIs will be expected to ensure they are able to remain within impact tolerances. This means that where weaknesses in operational resilience are identified, firms and FMIs will be expected to act, for example, by replacing outdated or weak infrastructure, increasing system capacity, achieving full fail-over capability, addressing key person dependencies, and being able to communicate with all affected parties (see Chapter 4).
- **The expectations for testing:** The DP stated firms and FMIs could test themselves against their own severe but plausible operational scenarios to identify and address vulnerabilities. In the proposals, the supervisory authorities provide more detail on scenario testing. In particular, that firms and FMIs should assume failure of key resources and consider incidents that have happened elsewhere in the financial sector (see Chapter 4).
- **Link to other policies:** In the DP the supervisory authorities stated they would be drawing together existing policy material which is relevant for the resilience of firms and FMIs. In the proposals, the supervisory authorities have done this. In particular, the supervisory authorities have clarified that firms and FMIs should consider how other policies such as operational risk management and business continuity planning support the delivery of important business services (see Chapter 4).

Summary of the approach

1.9 Ultimately, the aim of the approach to operational resilience in the DP was to drive change where it is needed. The proposals aim to achieve this by building the approach into formal policies for each supervisory authority.

1.10 In the DP and the proposals operational resilience is:

Operational resilience: the ability of firms and FMIs and the financial sector as a whole to *prevent, adapt, respond to, recover and learn from* operational disruptions.

1.11 It is not possible to prevent every risk materialising, and dependencies are often only identified once something has gone wrong. Therefore the approach in the DP and the proposals is based on the assumption that major operational disruptions will occur.

1.12 The result of implementing the proposals should be that when a disruption occurs, firms and FMIs will have robust and reliable arrangements in place to deal with it. These arrangements will have previously been tested. Firms and FMIs will also be able to show that they are operationally resilient, both to themselves and to the supervisory authorities. The proposals are designed to promote stronger and more effective governance of operational resilience and more organisation and co-operation between market participants.

1.13 The proposals set requirements and expectations on firms and FMIs to:

- identify their important business services by considering how disruption to the business services they provide can have impacts beyond their own commercial interests including, where relevant, harm to consumers, harm to market integrity, and threats to policyholder protection, safety and soundness, and financial stability;⁷
- set a tolerance for disruption for each important business service at the first point at which a disruption would pose an intolerable risk:
 - of harm to consumers or market participants;
 - of harm to market integrity;
 - to policyholder protection;
 - to the firm's safety and soundness; or
 - to financial stability;⁸ and
- ensure they can continue to deliver their important business services and are able to remain within their impact tolerances during severe (or in the case of FMIs, extreme)⁹ but plausible scenarios.

1.14 The proposals do not replace existing rules, principles, expectations or guidance, for example those to manage operational risk or business continuity planning.

Treasury Select Committee (TSC) report on 'IT failures in the Financial Services Sector'¹⁰

1.15 On Monday 28 October 2019 the TSC published a report following its inquiry into IT failures in financial services, which included recommendations to improve operational resilience in the financial sector. The supervisory authorities have reviewed the TSC's report and note that the proposals are consistent with the TSC's recommendations where relevant. The supervisory authorities will provide a full response to all the TSC's recommendations in due course.

1.16 The CPs propose clear standards for operational resilience, connecting requirements and expectations to the supervisory authorities' public interest objectives. This will allow supervisors to use enforcement tools if firms or FMIs do not meet the policy's standards. For example, the proposals include standards relating to:

- the identification of important business services, including examples of such important business services which firms or FMIs might identify;
- setting impact tolerances for their important business services;

⁷ Guidance on how firms and FMIs should approach identification of important business services is provided in each supervisory authority's Consultation Papers.

⁸ Guidance on setting impact tolerances for important business services is provided in each supervisory authority's Consultation Papers.

⁹ Note, for FMIs the terminology 'extreme but plausible' is used to avoid confusion with other parts of their supervisory approach.

¹⁰ <https://www.parliament.uk/business/committees/committees-a-z/commons-select/treasury-committee/news-parliament-2017/it-failures-financials-services-sector-report-published-19-20/>.

- testing if firms or FMIs are able to remain within their impact tolerances in a range of scenarios, including those in which they anticipate exceeding their impact tolerance – firms and FMIs should be able to articulate in which scenarios (for example if essential infrastructure such as power, transport or telecommunications were unavailable) they would not be able to deliver their important business services within their impact tolerances;
- the management body’s role in approving important business services, impact tolerances and regular reviews of the self-assessment; and
- taking action to improve operational resilience, where a firm or FMI is not able to remain within the set tolerance for an important business service in a severe but plausible scenario (or in the case of FMIs, extreme but plausible scenario). This would include taking action to address vulnerabilities in legacy systems where they are identified.

1.17 The proposals make a clear link to existing governance standards. For example:

- management bodies would need to have sufficient knowledge, skills and experience to meet their operational resilience responsibilities. This should ensure the management body can challenge senior management constructively on the firm’s or FMI’s operational resilience and the management body can meet its oversight responsibilities; and
- where the Senior Managers and Certification Regime applies, we clarify the interaction between Senior Management Function (SMF) 24 – Chief Operations and our operational resilience proposals.

1.18 Finally, the proposals are designed to build on the existing regulatory framework. For example the:

- supervisory authorities set out how they propose to supervise existing policies in light of the proposed new operational resilience rules and expectations;
- scope of a scenario test would include considering how a firm or FMI would respond to disruptions when they occur, including their incident management procedures; and
- supervisory authorities will consider developing further policy requirements in the future, including reporting. Operational resilience regulatory reporting would provide higher quality incident reporting and would allow the supervisory authorities to identify more effectively risks from operational failures, including IT failures. The PRA intends to consult on operational resilience regulatory reporting in 2020.

2 Important business services

2.1 The DP defined business services as ‘Products and services that a firm or FMI provides to its customers’. The DP stated that the continuity of important business services was an essential component of operational resilience. The supervisory authorities continue to think that concentrating on important business services is the right approach. To do so will encourage firms and FMIs to focus on services that, if disrupted, could lead to a threat to the viability of individual firms and FMIs, cause harm to consumers or market participants, harm to market integrity, or threaten policyholder protection, safety and soundness, or financial stability.

Business services

2.2 A business service is a service that a firm provides to an external end user or participant. Business services deliver a specific outcome or service and should be distinguished from lines of business, eg retail and commercial mortgages, which are a collection of services and activities. They will vary from firm to firm.

2.3 In the proposals, the supervisory authorities would require firms and FMIs to consider the chain of activities which make up a business service, from taking on an obligation, to delivery of the service, and determine which part of the chain is critical to delivery. The supervisory authorities propose that all resources that are required to deliver that part of the service should be operationally resilient.

'Important' business services

2.4 The supervisory authorities' view, originally set out in the DP, is that business services will qualify as 'important' when their failure could cause an intolerable level of harm to consumers or market participants, harm to market integrity, or threaten policyholder protection, the safety and soundness of individual firms, or financial stability. Often important business services will be linked to the ability to make timely payments such as making mortgage disbursements but this need not always be the case. Further guidance and expectations are provided in the proposals published by each supervisory authority.

2.5 In the proposals an important business service is:

Important business service: means a service provided by a firm or FMI to an external end user or participant where a disruption to the provision of the service could cause intolerable harm to consumers or market participants; harm market integrity; threaten policyholder protection; safety and soundness; or financial stability.¹¹

Identifying important business services

2.6 The supervisory authorities' view that firms and FMIs should be responsible for identifying their own important business services is also unchanged since the DP. Once identified, the supervisory authorities would require boards and senior management to prioritise the operational resilience of these important business services over other business services. The supervisory authorities expect that the important business services identified may vary across firms and FMIs reflecting their unique business models.

2.7 Important business services should be identified to a sufficiently granular level so that an impact tolerance can be applied and tested.

2.8 The supervisory authorities do not plan to introduce definitive lists or taxonomies of important business services, as specifying some services to always be an important business service is unlikely to be proportionate. For example, due to differing business models of each firm and FMI, the same business service may be important for one firm but not for another. The need to identify which services are important will help firms and FMIs embed the concept of important business services into their operations. However, to help explain the concepts, illustrative examples are included in the supervisory authorities' respective consultation documents.

¹¹ Guidance on how firms and FMIs should approach identification of important business services is provided in each supervisory authority's Consultation Papers.

3 Impact tolerances

3.1 The DP defined impact tolerances as ‘tolerance for disruption, under the assumption that disruption to a particular business service will occur’. The DP stated that this could be 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. The purpose of setting impact tolerances was to provide clear metrics so that management know the level of resilience they need to build for their important business services.

3.2 The supervisory authorities have refined the approach to impact tolerances, based on feedback from DP respondents and engagement with industry stakeholders.

Setting impact tolerances

3.3 Firms and FMIs should identify specific metrics for the maximum tolerable level of disruption. These should be measures that identify: harm to consumers or market participants;¹² harm to market integrity; threat to policyholder protection; safety and soundness; or financial stability. Such metrics could measure the extent of disruption, for example by including the maximum value of disruption, number of transactions, or the number of customers affected. All impact tolerances should include the maximum tolerable duration of such disruption, taking into account the criticality of the important business service. However, a metric based on time alone may be insufficient.

3.4 This differs from the definition in the DP and the clarification ensures consistency across firms and should be practical for boards, senior management and the supervisory authorities. A time-based metric is important as it means firms and FMIs will know how long an impact can be tolerated for and therefore how quickly any contingency arrangements will need to be able to come into effect.

3.5 Therefore, in the proposals, an impact tolerance is:

Impact tolerance: means the maximum tolerable level of disruption to an important business service, including the maximum tolerable duration of a disruption.

Impact tolerance and risk appetites

3.6 The supervisory authorities have not changed their view that impact tolerances are different from risk appetite. Unlike a risk appetite, impact tolerances assume a particular risk has crystallised. A risk appetite is the amount of risk that a firm or FMI is willing to take in pursuit of its strategic objectives.

3.7 Risk appetites focus management attention on managing the likelihood of operational risks occurring, and the impact if they do. The introduction of impact tolerances will increase the focus of firms and FMIs on their operational resilience before operational risks have crystallised. This should increase their capability to survive severe (or in the case of FMIs, extreme) disruptions when risk appetites are likely to have been exceeded. Impact tolerances are also set only in relation to harm to consumers or market participants, harm to market integrity, or threats to policyholder protection, safety and soundness, and the wider financial sector.¹³

¹² Market participants delivering business services through value chains may need to understand their respective impact tolerances to strengthen resilience in the value chain as a whole. They may also need to participate in joint testing to be properly sighted on weak points (for example in their connectivity or shared infrastructure) to address resilience gaps.

¹³ Specified service providers to recognised payments systems are not expected to set impact tolerances. Guidance on this issue is provided in the operational resilience consultation paper and draft supervisory statement relevant to recognised payment system operators and specified service providers.

Impact tolerances for dual-regulated firms

3.8 The DP did not comment on how the approach to operational resilience would work for dual-regulated firms. A firm regulated by both the PRA and the FCA could have up to two impact tolerances for each important business service – one considering financial stability, safety and soundness and policyholder protection, the other set with reference to consumer harm and harm to market integrity.

3.9 A dual-regulated firm will need to be able to tell the FCA and PRA the relevant impact tolerance for each important business service because of the different policies and requirements of each supervisory authority. The two impact tolerances may be the same for each or they may differ. For example, the firm's viability might be impacted after, before or at the same time as consumer harm. It is important firms and each supervisory authority know what the relevant individual impact tolerances are. The FCA and PRA will co-operate when supervising dual-regulated firms and understand that in some circumstances it may be appropriate for firms to focus on the impact tolerance which has the shortest duration when prioritising actions. A firm may be within the impact tolerance it has set for one supervisory authority while being unable to remain with its impact tolerance set for the other. See paragraph 4.6 for how dual-regulated firms should take action to be able to remain within their impact tolerances.

4 Delivering operational resilience

4.1 The DP outlined the expected benefits to firms, FMI and the public interest of implementing the supervisory authorities' approach to operational resilience, however it did not set out the actions firms and FMIs will be expected to take. The proposals set out how firms should focus on their important business services and ensure that they have the ability to remain within impact tolerances in severe but plausible scenarios.

Taking action to building operational resilience

4.2 Delivering operational resilience requires firms and FMIs to take decisive and effective actions to improve operational resilience, for example replacing outdated or weak infrastructure, increasing system capacity, achieving full fail-over capability, addressing key person dependencies, and being able to communicate with all affected parties. This would include taking action to address vulnerabilities in legacy systems.

4.3 Firms and FMIs should use impact tolerances as a planning tool and should assure themselves they are able to remain within them in severe but plausible scenarios.

4.4 The supervisory authorities propose that specific limitations that may prevent firms and FMIs from remaining within their impact tolerances should be identified by firms and FMIs completing mapping and scenario testing. The authorities' proposed approach to scenario testing and mapping is set out below.

4.5 Deficiencies, whether identified through scenario testing or through practical experience, should be addressed as a matter of priority. By definition, these deficiencies risk an intolerable level of harm to consumers or market participants, harm to market integrity, or threaten policyholder protection, the safety and soundness of individual firms, or financial stability. Therefore firms and FMIs should prioritise actions to address the risks posed by each deficiency. Firms should prioritise actions to address vulnerabilities regardless of the complexity of their business and firms whose important business services may pose a significant risk to financial stability are expected to be particularly proactive in addressing vulnerabilities.

4.6 Dual-regulated firms will also be expected to be able to demonstrate to each supervisory authority why individual actions address gaps in resilience. Both the FCA and the PRA need to be satisfied that the actions firms take address the vulnerabilities in a firm's operational resilience. This should reflect the differences in the definitions in the FCA's and PRA's policies and their different statutory objectives. However, the FCA and PRA understand that in practice firms are likely to take actions so they are able to remain within the impact tolerance which has the shortest duration. The FCA and PRA will collaborate to apply their policies consistently.

4.7 In the event of an incident, an impact tolerance is likely to provide an informative benchmark for firms, FMIs and the supervisory authorities to work towards. However, the supervisory authorities wish to avoid creating perverse incentives for firms and FMIs. A firm or FMI should not, for example, resume the provision of an important business service in order to be able to remain within an impact tolerance if the firm or FMI knows there is a significant risk of spreading a computer virus. Therefore although firms and FMIs should be able to remain within impact tolerances, the particular circumstances of a disruption will influence whether it is appropriate for firms to exceed their impact tolerances.

Severe (or in the case of FMIs, extreme) but plausible scenarios

4.8 The DP did not set out how firms' and FMIs' boards and senior management should decide the appropriate impact tolerance(s) to set and remain within to ensure their firm or FMI's operational resilience. In the proposals, the supervisory authorities say that this could be achieved by identifying scenarios in which firms and FMIs would, and would not, be able to resume the delivery of an important business service within their impact tolerance. Once firms and FMIs have identified scenarios that would cause them to exceed an impact tolerance, their boards and senior management should judge whether failing to remain within the impact tolerance in those scenarios is acceptable.

4.9 The severity of scenarios used by firms for their testing could be varied by increasing the number or type of resources unavailable for delivering the important business service, or extending the period for which a particular resource is unavailable. Firms and FMIs could consider failures within their control (eg system failures) as well as those outside of their control (eg disruption to essential infrastructure such as power, transport or telecommunications).

4.10 As impact tolerances are set on the assumption that a severe (or in the case of FMIs, extreme) disruption will occur, firms' and FMIs' scenarios should not devote too much time to considering the relevant probability of incidents occurring. However, plausibility can be considered by modelling incidents or near misses that have occurred within their organisation, across the financial sector, or in other sectors and jurisdictions. Firms and FMIs should focus on the response and recovery actions they would take to continue the delivery of an important business service, assuming a disruption has occurred.

4.11 The supervisory authorities will want to understand the level of assurance boards and senior management have gained to ensure impact tolerances can be met. In particular, firms and FMIs should be clear on which scenarios they expect to be able to remain within their impact tolerances and which ones may not. Although the supervisory authorities do not currently propose to set scenarios, they may consider doing so at a future date, if they consider it necessary.

4.12 As the environment firms and FMIs operate in¹⁴ is constantly changing, the proposals clarify that firms and FMIs should monitor their operational resilience and identify their weaknesses on an ongoing basis.

Scenario testing

4.13 Identifying in which severe (or in the case of FMIs, extreme) but plausible scenarios firms are able to remain within their impact tolerances can be achieved through scenario testing. The approach to scenario testing has been refined in the proposals and the supervisory authorities are proposing expectations and requirements on firms.

4.14 In the proposals scenario testing is:

Scenario testing: is the testing of a firm or FMI's ability to remain within its impact tolerance for each of its important business services in the event of a severe (or in the case of FMIs, extreme) but plausible disruption of its operations. In carrying out the scenario testing, a firm must identify an appropriate range of adverse circumstances of varying nature, severity and duration relevant to its business and risk profile and consider the risks to delivery of the firm or FMI's important business services in those circumstances.

4.15 The proposals are designed to allow firms and FMIs to make appropriate judgements when completing scenario testing in a way that is systematic, transparent and open to supervisory challenge.

Mapping

4.16 The DP stated that an operationally resilient firm or FMI would have in place a comprehensive understanding and mapping of the systems and processes that support its business services, including those over which the firm or FMI may not have direct control. In the proposals, the supervisory authorities have detailed how firms and FMIs would be expected to achieve this.

4.17 In the proposals the term mapping is:

Mapping: a firm or FMI must identify and document the necessary people, processes, technology, facilities and information (referred to as resources) required to deliver each of its important business services.

4.18 In the proposals, the supervisory authorities say that mapping will enable firms and FMIs to understand how their important business services are delivered and how they could be disrupted. The proposals clarify the expectation in the DP that firms and FMIs only need to map their important business services, not all business services.

4.19 In particular, mapping should enable firms and FMIs to deliver the following outcomes:

- (i) identify vulnerabilities in delivery of important business services within an impact tolerance;
- (ii) take action to remedy vulnerabilities as appropriate; and
- (iii) test their ability to remain within impact tolerances.

¹⁴ This could also include the impact of firms and FMI's internal environment, for example the impact of restructuring.

4.20 Examples of the vulnerabilities firms' and FMIs' mapping could highlight are: limited substitutability of resources; high complexity; single points of failure; and a concentration of reliance on a single resource.

4.21 The supervisory authorities do not propose to be prescriptive on a mapping process. Firms and FMIs can develop their own methodology and assumptions to best fit their business. This allows firms and FMIs to be proportionate and identify the level of detail necessary to deliver the desired outcomes listed in paragraph 4.19 above. Firms and FMIs could use methods such as process mapping, transaction life cycle documentation, and customer journeys.

Existing requirements

4.22 Operational resilience is an outcome that depends on numerous factors. In the DP the supervisory authorities stated that, in addition to developing policy proposals, they would be drawing together existing policy material which is relevant for the operational resilience of firms and FMIs. When considering other policies such as operational risk and business continuity planning, firms and FMIs should consider how the application of these policies support the delivery of important business services.

4.23 For example, DP respondents queried the reliance firms and FMIs would be able to place on the resilience of their service providers. Consistent with existing policies, firms and FMIs retain full responsibility and accountability for discharging all their regulatory responsibilities and cannot delegate any part of this responsibility to a third-party. Therefore firms and FMIs should be able to remain within their impact tolerances for important business services, irrespective of whether they use third parties to deliver them. This means mapping should include the third parties used to deliver important business services and scenario testing should include third parties where appropriate. For PRA-regulated firms, reference should be made to the cloud and outsourcing policy publications¹⁵ when considering the risks introduced by third parties.

5 Next steps

Policy proposals

5.1 The supervisory authorities are consulting on all the publications that form this package for a period of four months. The consultation period will end on Friday 3 April 2020.

5.2 The supervisory authorities will consider developing further policy requirements in the future, including reporting.

Relationship with the Financial Policy Committee (FPC)

5.3 The FPC has stated that it will 'set tolerances for how quickly critical financial companies must be able to restore vital financial services following a severe but plausible cyber incident [...] calibrated to ensure financial stability and avoid material economic harm'.¹⁶

5.4 While the FPC is considering resilience in the context of cyber, the supervisory authorities anticipate that firms and FMIs will take into account any tolerances set by the FPC when setting their own impact tolerances.

¹⁵ PRA CP30/19 'Outsourcing and third party risk management' and FCA CP19/32 Chapter 9 'Outsourcing and third-party service provision'.

¹⁶ Financial Policy Summary and Record, Bank of England, March 2019 paragraph 91: <https://www.bankofengland.co.uk/financial-policy-summary-and-record/2019/march-2019>.

Industry engagement

5.5 We will continue to engage with firms and FMIs during the consultation period about the concepts we have outlined. We welcome views about these and any other measure that would help build operational resilience across the financial sector. This will be through a combination of roundtable discussions, industry fora, speeches and more focussed group discussions.

International

5.6 The UK's supervisory authorities will continue to engage with international policy development processes. For example, by working with the Basel Committee on Banking Supervision as they develop an international approach to operational resilience.

5.7 The UK supervisory authorities will consider the approach as international standards develop and will complete peer comparison with other jurisdictions. This could result in their approach being refined and reviewed in the future