FINANCIAL CONDUCT AUTHORITY

Building operational resilience: impact tolerances for important business services and feedback to DP18/04

Consultation Paper
CP19/32***

December 2019

How to respond

We are asking for comments on this Consultation Paper (CP) by **3 April 2020**.

You can send them to us using the form on our website at: www.fca.org.uk/cp19-32-response-form

Or in writing to:
Governance & Professionalism Policy
Strategy & Competition
Financial Conduct Authority
12 Endeavour Square
London E20 1JN

Email:
cp1932@fca.org.uk

How to navigate this document

- returns you to the contents list
- takes you to helpful abbreviations
- takes you to the previous page
- takes you to the next page
- prints document
- email and share document

Sign up for our weekly
news and publications alerts

See all our latest press releases, consultations and speeches.

Contents

1 Summary

Why we are consulting

1.1 We are proposing changes to how firms approach their operational resilience.

1.2 Our proposals build on the approach first outlined in the Discussion Paper (DP) 'Building the UK Financial Sector's Operational Resilience' published in July 2018. Respondents were supportive of the ideas in the DP, and sought further information about how the ideas would work in practice.

1.3 This Consultation Paper (CP) aims to expand on and develop the ideas discussed in the DP based on the responses received and asks for your feedback on our proposals.

Who this applies to

1.4 This consultation affects banks, building societies, Prudential Regulation Authority (PRA) designated investment firms, Solvency II firms, Recognised Investment Exchanges (RIEs), Enhanced scope Senior Managers & Certification Regime (SM&CR) firms and entities authorised or registered under the Payment Services Regulations 2017 (PSRs 2017) and/or the Electronic Money Regulations 2011 (EMRs 2011).

1.5 This CP does not apply to European Economic Area (EEA) firms. Please see Appendix 1 (Draft Handbook text) for further details on our proposed application of the proposals in this consultation. Appendix 2 contains the version of the instrument that would be made if the UK exits the European Union prior to the rules being made.

1.6 Consumers may be interested in how operational resilience is being improved within firms.

Summary of our proposals

1.7 We propose firms:

- **identify their important business services** that if disrupted could cause harm to consumers or market integrity
- identify and document the people, processes, technology, facilities and information that support a firm's important business services (**mapping**)
- **set impact tolerances** for each important business service (ie thresholds for maximum tolerable disruption)
- **test** their ability to remain within their impact tolerances through a range of severe but plausible disruption scenarios
- **conduct lessons learned exercises** to identify, prioritise and invest in their ability to respond and recover from disruptions as effectively as possible

- develop internal and external **communications plans** for when important business services are disrupted
- create a **self-assessment document**

1.8 Our proposals are not intended to conflict with or supersede existing requirements to manage operational risk or business continuity planning, but rather aim to set new requirements that enhance operational resilience.

1.9 The Payment Services Regulations (PSRs 2017) require Payment Service Providers (PSPs) including credit institutions to establish a framework with appropriate mitigation measures and control mechanisms to manage their operational and security risks. As part of that framework they are required to establish and maintain effective incident management procedures, including for the detection and classification of major operational and security incidents.

1.10 On 12 December 2017, the European Banking Authority (EBA) issued detailed guidelines on the security measures for operational and security risk of payment services under the Payment Services Directive 2 (PSD2). The EBA Guidelines include steps to be undertaken by firms on a regular and ongoing basis to identify their supporting processes and assets, to establish and implement preventive security measures, to test and assess their resilience plans against a range of scenarios, and to prioritise business continuity actions using a risk-based approach. As the national competent authority, we announced that we would comply with these Guidelines.

1.11 Our analysis of the payments sector has concluded that even small payments firms can be highly impactful in terms of harm arising from operational disruptions as disruptions can quickly lead to consumers not having access to their money. Smaller payments firms are also more likely to be technology dependent in comparison to smaller FSMA-authorised firms. For example, Registered Account Information Service Providers (RAISPs), although small in size compared to other payments firms, are key repositories of consumer information and could cause significant harm should they suffer from a data breach.

1.12 On 28 November 2019, the EBA published its final guidelines on information and communications technology (ICT) and security risk management. These guidelines will replace the PSD2 guidelines and set out requirements for credit institutions, other payment service providers and Capital Requirements Regulation (CRR) investment firms. We will confirm during 2020 our approach to these guidelines. We will also provide further clarification on the links between our operational resilience policy and the EBA guidelines. While our proposals aim to set specific new requirements, Annex 4 highlights examples of existing Handbook provisions and other legislative provisions which could be interpreted as covering similar areas. We recognise that as a result of existing legislation some firms are already undertaking some of the practices recommended in this CP. We welcome feedback from firms on how they are doing so and any potential areas of overlap.

Next steps

1.13 We have developed the policy proposals and the underlying draft rules in the context of the existing UK and European Union (EU) regulatory framework. We will keep the policy proposals under review to assess whether any amendments will be required due to changes in the UK regulatory framework.

1.14 We want to know what you think of our proposals. Please send us your comments by 3 April 2020.

1.15 Use the response form on our website, email us at cp1932@fca.org.uk or write to us at the address on page 2.

1.16 We will consider all feedback and publish our finalised rules in a Policy Statement (PS) next year.

2 The wider context

2.1 The FCA, Bank of England in its capacity of supervising financial market infrastructures (FMIs) and PRA ('the supervisory authorities') continue to develop a policy framework for operational resilience based on the concepts in the DP. Our aim is to improve the resilience of the UK financial sector. The supervisory authorities have jointly published a policy summary of the key concepts outlined in our consultation papers. Dual-regulated firms should also consult the PRA's CP in addition to this CP.

2.2 This work has been undertaken as part of our long-term priority in relation to the resilience of firms and the wider FCA prioritisation of operational resilience for 2019/20.

2.3 Operational resilience is the ability of firms and the financial sector as a whole to prevent, adapt, respond to, recover and learn from operational disruptions. Operational disruptions and the unavailability of important business services have the potential to cause wide-reaching harm to consumers and market integrity, threaten the viability of firms and cause instability in the financial system. This CP focuses on how the provision of these services can be maintained in the event of disruptions.

2.4 Operational disruptions can have many causes including, for example, technology failures or when making changes to systems. Some disruptions may also be caused by matters outside of a firm's control, such as a cyber-attack or wider telecommunications or power failure.

2.5 Ultimately, our aim is to increase firms' operational resilience and drive change where it is needed. Where weaknesses in operational resilience are identified, firms will be expected to act. For example, by investing in improving processes, better infrastructure or training, building back-up systems, addressing vulnerabilities in legacy systems or improving contingency plans.

2.6 We propose to apply the proposals in this CP proportionately to firms reflecting the impact on consumers and market integrity if their services are disrupted. We consider the proposals to be helpful in increasing the resilience of all firms we regulate, as well as the wider industry. We will take into account the feedback to this consultation. After we publish our final rules, we will consider whether the proposals should be applied to other firms. If we decide they should, we will undertake a formal consultation and ensure that we coordinate our approach with the proposals in this CP.

2.7 Firms not subject to this CP should continue to meet their existing operational resilience obligations and may want to consider our proposals.

2.8 We want our policy framework to be proportionate and flexible enough to accommodate the different business models of firms. So, we have designed the framework to be dependent on the number of important business services that a firm has. We expect that the number of important business services offered by a firm will be proportionate to its role and size. Firms' mapping exercises would also be scaled according to this, with less complex firms likely to have simpler and fewer important business services to map.

2.9 We will expect firms to have regard to severe but plausible scenarios, but not every possible scenario. This is intended to reduce the burden on firms, as disruption to important business services are only considered in the context of severe scenarios. Multiple, but less severe scenarios should be covered by a firm's existing operational risk management practices.

How it links to our objectives

Consumer protection

Ongoing availability of business services reduces consumer harm

2.10 Asking firms to identify their important business services, set impact tolerances, and restore their important business services quickly following a disruption, will improve the way in which firms ensure the ongoing availability of business services and supply of new business services to consumers.

2.11 Where we refer to consumers in this CP we generally mean those that are the direct consumers of the firm's services or in other ways dependent upon them. This includes both retail and wholesale market participants.

Market integrity

Ongoing availability of business services reduces harm to market integrity

2.12 Operational disruptions pose risks to the soundness, stability and resilience of the UK financial system and the orderly operation of financial markets.

2.13 Our proposals will help build the resilience of the market to continue to function as effectively as possible and quickly return to full operations following a disruption.

2.14 Where we refer to market integrity in this CP we mean the soundness, stability or resilience of the UK financial system, and the orderly operation of the financial markets.

Effective Competition

Resilient firms can promote effective competition

2.15 We consider that consumers may be more likely to choose firms that are more resilient to operational disruptions. This may drive firms to improve their operational resilience as one way to compete for, and keep, customers.

Equality and diversity considerations

2.16 We have considered the equality and diversity issues that may arise from the proposals in this CP and remain especially mindful of the impact that resilience issues can have on vulnerable consumers, including the continuance of access to key financial services.

2.17 Overall, we do not consider that the proposals adversely impact any of the groups with protected characteristics under the Equality Act 2010. Given our express aim to strengthen the consideration given to vulnerable consumers during operational disruptions, we anticipate a positive impact on those who are vulnerable due to having

a protected characteristic. But we will continue to consider the equality and diversity implications of the proposals during the consultation period, and will revisit them when making the final rules.

2.18 In the meantime, we welcome your input on this consultation.

3 Example firms

3.1 Throughout this CP, our 4 example firms show how each of the elements might apply to different types of firms. We acknowledge that in practice firms delivering business services would consider many other operational issues, dependencies, and risk management considerations. These examples are non-exhaustive and purely illustrative. Firms will need to consider how the elements apply to their own circumstances.

Firm A

Firm A is a large dual-regulated high-street bank which provides online and telephone banking services for retail consumers.

Firm B

Firm B is an Enhanced scope SM&CR firm that provides wealth management services with a digital-first operating model. Firm B's consumers are regulated firms which rely on the investment, transaction and administration services provided through Firm B's online platform. The underlying consumers are primarily retail and institutional investors. Firm B employs over 2000 employees worldwide, with approximately 600 working on the platform's business.

Firm C

Firm C is part of a Group which provides custodian services to small and medium-sized asset managers and investment management firms across Europe, the Middle East, and Asia. The Group operates from 5 global locations; each subsidiary firm is in a different international regulatory jurisdiction. Firm C employs 120 staff globally, 40 of whom are based in the UK. Firm C's services include safekeeping of assets, settlements, collections and foreign exchange payments.

Firm D

Firm D is an insurer with 350 employees. It provides life, motor, home, and pet insurance.

4 Important business services

In this chapter, we summarise the feedback we received to the DP on the ways in which operational resilience could be improved through an approach based on identifying important business services. We also set out our proposals for firms to identify their important business services.

Overview

DP concepts

4.1 In the DP, we highlighted that operationally resilient business services provided by firms directly support resilient economic functions, enabling people to buy goods, borrow money and transact on financial markets.

4.2 The UK financial system is resilient if its economic functions can continue to operate during potentially disruptive incidents. Resilience of the financial system depends on both individual firms and the ways in which their services are interconnected with other firms.

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

4.4 In the DP, we suggested that firms should focus more effort and resources on achieving the continuity of their important business services in the event of severe operational disruption, and not just on recovery of the underlying systems and processes.

4.5 We also suggested that a business services approach may be an effective way to prioritise improvements to systems and processes. Firms 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 systems and processes based on the business services they support may bring more transparency to and improve the quality of decision making, thereby improving resilience.

Feedback on DP concepts

4.6 Many respondents to the DP broadly supported our suggested approach and said they recognised the potential benefits of the suggested focus on continuity of business services. This included, for example, better customer outcomes and as a way of breaking down silos that exist within their organisations.

4.7 Some respondents expressed concern that, for larger organisations with more complex business models and supplier relationships, identifying and mapping their business services and accountabilities could be complex, time-consuming, disruptive, and disproportionately expensive.

4.8 Some respondents said that taking a business services view of operational resilience is not new as it overlaps with existing arrangements for Operational Continuity in Resolution (OCIR). We are also aware that some organisations have already recognised the benefit of making business service mapping part of their information systems and technology strategies.

4.9 Many respondents asked us to comment in more detail on how organisations should identify business services and their most important business services. Additionally, they asked whether organisations would be expected to restructure themselves to create discrete operational business service units. Some respondents also advised against the supervisory authorities taking a prescriptive approach.

4.10 Some respondents said that aiming for continuity of business services seemed the right approach. However, in some circumstances taking the system (and therefore the business service) off-line might be the safest and most effective immediate response to an event, and in some severely disruptive events it would not be possible to achieve continuity of supply.

Our proposals

4.11 Given the positive feedback we received to the DP, we propose to use the business services approach as a way for firms to build their operational resilience. This means firms will be required to identify their important business services.

4.12 Focusing on business services encourages firms to consider alternative ways the service may be delivered, in a way that monitoring individual components and processes cannot. For example, an important business service of 'mortgage disbursement' might begin with an individual's request for funds, include internal authorisation and processing, and end with the confirmed payment of funds into the recipient's account.

4.13 We agree with respondents that in some circumstances, taking the systems and therefore the business service off-line might be the safest and most effective immediate response to the event. We also understand that firms will take this into account as part of their scenario testing. More detail on scenario testing can be found in Chapter 6.

4.14 Having considered the feedback, we believe that focusing on the possible impact of disruption to business services and, in particular, on identifying and continuing the supply of important business services, should help boards and senior managers make better-informed strategic, operational and investment decisions. It should also facilitate the management of aspects delivered by third-parties. This increased focus would contribute to the resilience of the wider financial system and the economy.

4.15 Firms business models and structure need to be consistent with the objectives of both authorities. We are not, however, proposing that firms restructure themselves as a result of this policy. Please see Chapter 7 for more information on governance.

4.16 We propose that firms should identify their important business services at least once a year. Firms should also do so whenever there is a material change to their business or the environment in which they operate. For example, where a firm is providing

additional new services, or a change in the market has led to the firm providing services to a significantly larger number of consumers or affected the vulnerability of its existing consumers, the firm should assess whether its current list of important business services is up to date.

Proposed guidance on identifying important business services

4.17 Identifying an important business service will be a matter of judgement for firms. We have considered whether to provide a fuller definition of 'important business services' and/or a new taxonomy of important business services.

4.18 We are not proposing to publish a detailed taxonomy of business services. We agree with industry feedback that firms (individually, collectively, and in discussion with their relevant trade associations) are best placed to identify their important business services. A detailed taxonomy of important business services may quickly become out-of-date. It may also encourage firms to take a prescriptive or inflexible approach to identifying their own important business services that does not reflect their size, complexity or focus on achieving operationally resilient outcomes which may evolve over time.

4.19 We consider important business services to be services that, if disrupted, would be most likely to cause intolerable levels of harm to consumers or market integrity. We have provided some general considerations below to help firms identify their important business services.

4.20 An important business service will also have the following characteristics:

- It should be clearly identifiable as a separate service, and not a collection of services. For example, withdrawal of cash at an ATM and the ability to check a balance online are 2 separate services, while the provision of packaged bank accounts is a collection of services.
- The users of the service should be identifiable so that the impacts of disruption (through process, cyber security or technology failures) are clear. These may include retail consumers, business consumers or market participants.

4.21 We are proposing the following factors as guidance for firms to consider when identifying their important business services.

The factors are not intended to be exhaustive or to restrict the approach that a firm decides is necessary to take.

a. a consideration of those potentially affected by disruption to the service (likely to cause consumer harm):

- the nature of the consumer base, including vulnerable consumers who are more susceptible to harm from a disruption
- the ability of consumers to obtain the service from other providers (substitutability, availability and accessibility)
- time criticality for consumers receiving the service
- the size of the consumer base to which the service is provided
- sensitivity of data held in the instance of a breach

b. a consideration of impact on the firm itself, where this could cause consumer harm or harm to market integrity:

- impact on the firm's financial position and potential to threaten the firm's viability
- potential to cause reputational damage
- potential to cause legal or regulatory censure
- level of inherent conduct and market risk

c. a consideration of the impact on the UK financial system (likely to cause harm to market integrity):

- the firm's potential to impact the soundness, stability or resilience of the UK financial system potential to inhibit the functioning of the UK financial system
- potential to cause knock-on effects for other market participants, particularly those that provide financial market infrastructure or critical national infrastructure
- the importance of that service to the UK financial system, which may include market share, sensitive consumers (for example, government services or pension funds) and consumer concentration

Example: How the example firms might identify their important business services

Firm A

Firm A identifies telephone banking consumer authentication as 1 of its important business services for the purposes of operational resilience. Firm A considers those potentially affected by disruption to the service. It concludes that consumer harm is likely as a significant number of their consumers use telephone banking as a primary channel to access several banking services.

Firm A analyses its consumer base and determines that there are consumers without access to alternative channels such as online banking or a nearby branch facility. They may, as a result, be more susceptible to harm if this business service is disrupted.

Firm B

Firm B identifies the administration of investments (consumer account and portfolio management) as 1 of its important business services for the purposes of operational resilience.

Firm B considers that disruption to the administration of investments could potentially harm market integrity due to the aggregate value of assets it administers. Firm B also considers such an event could cause it to suffer increased operational costs, loss of revenue and reputational damage.

The regulated firms which rely on the services provided through Firm B's online platform would also need to take account of the risk of harm to the underlying consumers as part of their own consideration of operational resilience obligations.

Firm C

Firm C identifies the safekeeping of securities for its consumers as 1 of its important business services.

Firm C considers the risk of consumer harm that could arise from disruption to trades and the misuse of consumers' data. Disruption to Firm C's safekeeping services could cause harm to other market participants' ability to complete trades of the securities over which it has accepted safekeeping responsibility.

Firm D

Firm D identifies the renewal of motor insurance as 1 of its important business services for the purposes of operational resilience.

Firm D determines that severe disruption to the supply of this business service could result in consumer harm, for example where auto-renewal of policies are not carried out and lead to consumers being uninsured.

Tell us what you think:

Q1: **Do you agree with our proposal for firms to identify their important business services? If not, please explain why.**

Q2: **Do you agree with our proposed guidance on identifying important business services? Are there any other factors for firms to consider?**

5 Impact tolerances

This chapter summarises the feedback we received in the DP and sets out our proposals for firms to set and manage to impact tolerances.

Overview

DP concepts

5.1 In the DP, we defined an impact tolerance as a firm's tolerance for disruption to a particular business service. We assumed that disruption to the systems and processes supporting that service will occur, and that impact tolerance is expressed by referring to specific outcomes and metrics.

5.2 We suggested that setting impact tolerances for providing important business services may help ensure that boards and senior management consider what the firm would do when a disruptive event occurs, rather than only trying to minimise the probability of disruption.

5.3 We also suggested that firms could use their impact tolerances in managing their businesses. For example, to take decisions on investments, risk management, business continuity planning and corporate structure.

Feedback to DP concepts

5.4 Most respondents supported setting impact tolerances. They recognised that a requirement to set impact tolerances would increase board-level engagement.

5.5 Respondents had mixed views about whether the supervisory authorities should set impact tolerances for firms or whether these should be set by firms.

5.6 Respondents also asked us to clarify the difference between an impact tolerance and business impact assessments and recovery time objectives (RTOs).

Our proposals

5.7 We propose that firms should set their impact tolerances at the first point at which a disruption to an important business service would cause intolerable levels of harm to consumers or market integrity. We consider that firms are best placed to determine the point at which to set their impact tolerance, taking on board the needs of their customers.

5.8 Setting impact tolerances is intended to change the mindset of firms' boards and senior management away from traditional risk management towards accepting that disruption to business services is inevitable, and needs to be managed actively.

5.9 Impact tolerance describes the maximum tolerable level of disruption to an important business service, assuming disruption to the supporting systems and processes will occur. It is expressed by reference to specific outcomes and metrics, which should always include the maximum tolerable duration and could also include other considerations such as volume of disruption (for example, the number and types of consumers affected) or a measure of data integrity. It is different from risk appetite because it assumes a risk has crystallised and may go beyond a firm's RTO. It is also different to business impact analysis as it is determined with reference to the FCA's public interest in reducing harm to consumers and market integrity.

5.10 Setting impact tolerances is a tool for planning and discovery purposes. It does not limit a firm's responsibility for compliance with conduct rules and other requirements (such as those set out in the PSRs 2017). Firms are still expected to take appropriate steps to avoid breaching requirements even where an impact tolerance would not be exceeded. Their legal duties in response to a breach, and the FCA's powers to take action, are unaffected by these proposals.

5.11 When setting tolerances, firms should consider different times of the day, different points in the year, or broader factors which may lead to activity within the important business service significantly increasing. This ensures that the firm's impact tolerance applies in peak times as well as under normal circumstances.

5.12 In determining the harms that can be caused to consumers and/or market integrity, we are proposing the following factors as guidance for firms to consider:

- the number and types (such as vulnerability) of consumers adversely affected, and nature of impact
- financial loss to consumers
- financial loss to the firm where this could harm the firm's consumers, the soundness, stability or resilience of the UK financial system or the orderly operation of the financial markets
- the level of reputational damage where this could harm the firm's consumers, the soundness, stability or resilience of the UK financial system or the orderly operation of the financial markets
- impacts to market or consumer confidence
- the spread of risks to their other business services, firms or the UK financial system
- loss of functionality or access for consumers
- any loss of confidentiality, integrity or availability of data

5.13 Firms could use a combination of metrics for their impact tolerances, or a single metric if appropriate. A duration-based metric for an impact tolerance should always specify that a particular important business service cannot be disrupted beyond a certain period of time, for example, 24 hours, without causing intolerable harm to consumers or market integrity. An impact tolerance that combines duration with another metric, such as a volume or value metric, might state that the firm will not tolerate the business service delivering at less than a certain percentage of normal operating capacity for a specified period of time.

5.14 We propose that firms set and review their impact tolerances at least once a year. Firms should also do so whenever there is a material change to their business or the environment in which they operate. For example, if a firm experiences a significant increase or decrease in the number of consumers it is providing an important business service to, it should review its existing impact tolerances to see if they are still appropriate.

Our proposed expectations

5.15 Firms should use impact tolerances as a planning tool and should assure themselves they are able to remain within them in severe but plausible scenarios. Delivering operational resilience requires firms to take decisive and effective actions. For example, by replacing outdated or weak infrastructure, increasing systems capacity or addressing key person dependencies. We anticipate that there may be circumstances where firms cannot meet their impact tolerances at all times. For example, a firm may identify that it will be outside its tolerance for a period while a technical vulnerability is resolved.

5.16 We do not expect firms to set their tolerances at excessively high levels. We will monitor this as part of our supervisory engagement with firms and intervene if appropriate.

5.17 Firms should take all possible actions to ensure that they are able to operate within their impact tolerances.

Dual-regulated firms

5.18 Dual-regulated firms will be expected to set and manage up to 2 impact tolerances for each of their important business services. Dual-regulated firms would set 1 impact tolerance at the first point at which there is an intolerable level of harm to consumers or market integrity for our purposes, and another tolerance at the first point at which financial stability is put at risk, and for the PRA's purposes, a firm's safety and soundness or policyholder protection is impacted. This is because we expect firms to have different strategic and investment plans to address resilience gaps depending on the nature of the disruption and potential harm. The 2 impact tolerances may be the same for each or they may differ. For example, the firm's viability might be affected after, before or at the same time as consumer harm occurs.

5.19 Firms will be required to consider the harms linked to the supervisory authorities' different objectives and the consequent requirements to address them in order to set the maximum impact the firm can tolerate. Dual-regulated firms should refer to the PRA's CP for more detail on setting impact tolerances.

FCA solo-regulated firms

5.20 We expect FCA solo-regulated firms to set 1 impact tolerance for each of their important business services by having regard to the potential harm posed to consumers, market integrity and, where appropriate, financial stability. For solo-regulated firms this will include the need for firms to assess if they have adequate financial resources to address potential harm. Some firms may conclude that there is no level of disruption to an important business service which would impact market

integrity. Firms may find it useful to refer to the considerations listed in paragraph 5.12 to determine whether they are likely to cause harm to market integrity.

5.21 We consider that both dual and solo-regulated firms are best placed to decide how to manage their impact tolerances, but we expect their methodology and description of potential of harm to be clear.

Transitional arrangements

5.22 We consider that it is beneficial to give firms time to ensure they can take the actions necessary to improve their operational resilience.

5.23 We propose that firms must be able to remain within their impact tolerances as soon as reasonably practicable, but no later than 3 years, after the rules come into effect.

5.24 We consider what is "reasonably practicable" will depend on a range of factors including the scale of a firm and its importance to the wider financial sector. These factors are unlikely to be outweighed by the complexity of operations, and we would expect in-scope financial institutions to be very active in addressing the vulnerabilities that they identify. Consistent with this a 'reasonable time' would typically mean that prompt action was appropriate.

5.25 New firms that are authorised within the transitional period will also be able to make use of the transitional period up to the 3-year deadline, eg a firm that is authorised 1 year into the transitional period will have up to 2 years to ensure it is able to remain within its impact tolerances.

5.26 We will expect firms to be able to show the actions that they are taking within the transitional period in their self-assessment document (please see Chapter 7 for further detail on the self-assessment document).

Examples: How the example firms might set and remain within impact tolerances

Firm A

When setting the impact tolerance, Firm A considers the potential harm in the event of loss of the telephone banking authentication service. Firm A considers that consumer harm is the most relevant harm and likely to occur first in the event of disruption.

Firm A quantifies the proportion of its consumers who have access to online services and/or branches and takes account of the capacity of the alternatives to manage additional consumers. Firm A also carries out analysis of its consumer base. It concludes that although most consumers can access their accounts through alternative channels, there are a sizeable number that cannot and they could be more susceptible to harm. Firm A also considers the financial losses that its consumers could incur through their inability to carry out typical transactions made by telephone banking.

Firm A reaches a conclusion that the appropriate impact tolerance is 12 hours to reflect the maximum disruption before there is an intolerable risk of consumer harm.

Firm B

Firm B identifies that the delivery of investment administration could be disrupted and harm to consumers could crystallise quickly if the platform it provides has operational issues.

Firm B has regard to the time-criticality in ensuring this service is available, the size of its market share and nature of its consumer base when it sets an impact tolerance. Firm B accordingly provides a methodology and rationale which supports its decision to set an impact tolerance of 8 hours for the administration of investments as an important business service.

Firm C

Firm C has identified the loss or unlawful disclosure of consumers' data as a metric for its impact tolerance for this service, and sets a tolerance of zero in recognition of the serious consequences of the loss, misuse or corruption of consumers' trade-related data.

Firm C also determines that the outage of the safekeeping service would result in consumers and other market participants not being able to settle transactions, and sets an impact tolerance of 6 hours.

Firm D

Firm D already has in place consumer vulnerability flags and controls that identify renewal requests that remain unprocessed within 12 hours of the policy renewal date.

In setting its impact tolerance for the renewal of motor insurance, Firm D considers the harm that can be caused if its consumers are unable to complete a motor insurance renewal, and sets an impact tolerance using a time-based metric.

Firm D considers that the maximum tolerable period of disruption to completion of motor insurance renewal requests is to be set at 24 hours after the policy renewal date. This means that even during severe disruption Firm D must be able to process all renewal requests no later than the day after the renewal date, and treat all outstanding applicants as at risk.

Tell us what you think:

Q3: **Do you agree with our proposals for firms to set impact tolerances? If not, please explain why.**

Q4: **Do you agree that duration (time) should always be used as 1 of the metrics in setting impact tolerances? Are there any other metrics that should also be mandatory?**

Q5: **Do you agree with our proposal for dual-regulated firms to set up to 2 impact tolerances and solo-regulated firms to set 1 impact tolerance per important business service?**

Q6: **Do you have any comments on our proposed transitional arrangements?**

6 Mapping and scenario testing

In this chapter, we set out our proposals for firms to:

- identify and document the people, processes, technology, facilities and information that support a firm's important business services (mapping)
- test their ability to remain within their impact tolerances through severe but plausible disruption scenarios
- conduct lessons learned exercises

Mapping

6.1 In the DP, we highlighted that an operationally resilient firm would be expected to have a comprehensive understanding and mapping of the systems and processes that support their business services. This includes those over which the firm may not have direct control ie outsourcing and third-party service providers, which we cover in more detail in Chapter 8.

6.2 To have a complete view of their resilience, firms will need to identify and document the people, processes, technology, facilities and information (hereafter resources) necessary to deliver each of a firm's important business services. Resources for important business services can potentially come from across business areas, entities and jurisdictions which gives need for a centralised identification for these inputs. By taking this approach, firms can be assured that an important business service can remain within the impact tolerance it has set.

6.3 We propose that firms should identify and document the resources that deliver and support their important business services. This identification process is referred to as **mapping**. Firms will only need to map their important business services, not all business services.

6.4 We will expect firms to ensure mapping is complete, accurate, documented and signed-off at an appropriate level by management (see Chapter 7 for more detail).

6.5 By looking at all the stages required in providing the business service, a firm will be able to develop a clearer picture of how best to support its resilience. The firm examples overleaf illustrate the variety of resources that could be considered.

6.6 Mapping should allow firms to meet the following outcomes:

- Identify vulnerabilities and remedy these as appropriate
  Mapping an important business service should help identify vulnerabilities and/or weaknesses in the delivery of important business services within an impact tolerance, and enable firms to act to remedy these as appropriate. Vulnerabilities and/or weaknesses may include lack of substitutability, high complexity, single points of failure, concentration risk, dependencies on third-parties and matters outside of a firm's control eg power failures.

- Enable firms to conduct scenario testing
  Mapping should allow firms to test their ability to stay within impact tolerances. To design and understand the full implications of scenarios, a complete map of the relevant business service(s) is necessary.

6.7 We consider that it is appropriate for firms to develop their own methodology that best fits their business, and to document their mapping in a way that is proportionate to their size, scale and complexity. This could be done via a tool, application or database and use methods such as process mapping, transaction life cycle documentation and consumer journeys.

Example: Resources that might support the example firms' important business services

Firm A

Firm A carries out a mapping exercise and identifies several supporting resources for continuity of their telephone banking authentication service. This includes key people within the business and escalation lines, a voice recognition software programme and third-party providers for the call centre staff, premises and telecommunications system.

The mapping also identifies interdependencies between the consumer account database which supports telephone authentication as well as online authentication. Firm A made use of existing maps developed for business continuity and disaster recovery during its mapping exercise.

Firm B

Firm B's mapping is complex due to the number of interconnecting systems and technology which support the platform service(s), some of which are outsourced to third party providers. The extent of customisation of its platforms and the way that they are integrated with consumers and counterparties increase this complexity further.

From its mapping, Firm B concludes that resilience considerations have been designed into the software and hardware systems' architecture, including monitoring systems for early detection of IT issues. Firm B reviews its reliance on third party service providers and engages with counterparties to understand their risk controls.

Firm B has staff supporting its platform 24/7. The mapping process identifies weaknesses in the resourcing of back office servicing, including high staff turnover, operational issues and a reliance on manual processing. While these have limited impact on day-to-day continuity of the platform service, Firm B identifies that these could weaken the firm's operational resilience if critical events occur.

Firm C

Firm C is a member of 2 clearing organisations for UK and international securities. Firm C's mapping reflects that data are stored at a third party's UK-based data centre. Back-up data facilities are provided by Firm C's Group in Frankfurt.

Firm C also takes into account that the Group is planning to make each firm under the Group self-sufficient in terms of data storage. It has started a 16-month change programme to migrate to a new solution which creates separate primary and back up data centres in each jurisdiction.

Firm D

Firm D undertakes a mapping exercise of the resources that support the delivery of motor insurance renewals. Firm D's mapping reflects that it employs 230 telephone sales agents (inbound call handlers) who work across two 8-hour shifts during office hours, and 40 on-line sales agents (live chat assistants) who work across three shifts over 24 hours.

Firm D also identifies that a digital sales support team, comprising of 6 people, is responsible for auto-renewals by email and that a third-party provider issues renewal correspondence by post.

Firm D includes in its mapping that it has sales agents operating from 2 premises in the same city. Fifteen of the on-line sales agents are trained and have the appropriate technology to work from home. The digital sales support team is based at only 1 of the 2 operations sites. A contract with the third-party service provider includes service level agreements containing volume, time and quality control/assurance metrics.

Each operational site is supported by independent servers which update to a shared database on a second server every 45 minutes (and all consumer data are saved to a back-up server at 8pm each evening).

Tell us what you think:

Q7: **Do you agree with our proposed approach to mapping? If not, please explain why.**

Scenario testing

6.8 We propose that firms should test their ability to remain within their impact tolerances for each of their important business services in the event of a severe but plausible disruption of its operations. This enables them to be assured of the resilience of their important business services, and identify where they might need to act to increase their operational resilience. In carrying out the scenario testing, firms should identify an appropriate range of adverse circumstances varying in nature, severity and duration relevant to its business and risk profile. They should then consider the risks to delivery of the firm's important business services in those circumstances.

6.9 Impact tolerances assume a disruption has occurred. So, testing the ability to stay within impact tolerances should not focus on preventing incidents from occurring or the probability of the incident taking place. Testing should instead focus on the response and recovery actions firms would take to continue the delivery of an important business service, assuming a disruption has occurred. In some circumstances taking the systems and therefore the business service off-line might be the safest and most effective immediate response to the event. Firms should consider whether a partial resumption, or the delivery of an alternative service, would mitigate impact even if their tolerance is breached.

6.10 Firms should test themselves against a range of scenarios in which the supporting resources for 1 or more of their important business services have been disrupted. Understanding the circumstances under which it is not possible to stay within an impact tolerance for a particular important business service will provide crucial

information to firms. This will enable firms to identify resilience gaps and assess the actions they may need to take to increase their operational resilience.

6.11 We consider that firms are best placed to determine the scenarios used for testing. When setting scenarios, firms could consider previous incidents or near misses within their organisation, across the financial sector and in other sectors and jurisdictions. Firms could also consider horizon risks, such as the evolving cyber threat, technological developments and business model changes.

6.12 Firms should be able to explain the level of resilience they have built by justifying the severity of scenarios in which they would be able to resume the delivery of an important business service within their impact tolerances.

6.13 To cover a range of severe but plausible scenarios, firms could use an incremental process. For example, firms could:

- start by assuming disruption to the resources key to the delivery of important business services (the cause not being material)
- increase severity by assuming simultaneous disruptions to key resources of their important business services or by resources being unavailable for longer time periods

6.14 Firms should ensure that testing considers realistic timelines, for example the time required for data analysis and decision making, and should develop as the firm learns from previous testing.

6.15 We propose the following scenario factors as guidance for firms to consider when testing:

- corruption, deletion or manipulation of data critical to the delivery of important business services
- unavailability of facilities or key people
- unavailability of third-party services which are critical to the delivery of important business services
- disruption to other market participants
- loss or reduced provision of technology underpinning the delivery of important business services

6.16 We propose that firms develop a testing plan that details how they will gain assurance that they can remain within impact tolerances. The testing plan should consider the following:

- the type of scenario testing. For example, whether it is paper-based, simulations or live-systems.
- the scenarios for which the firm expects to be able to remain within their impact tolerances and which ones they may not
- the number of important business services tested
- testing the availability and integrity of resources. A business service that is available but has compromised integrity is not remaining within the impact tolerance. For example, if a firm resumed service to remain within an impact tolerance when the firm knew there was a significant risk of spreading a computer virus.

- how communication strategies can be used to act quickly and effectively to reduce disruption by providing clear, timely and relevant information. See Chapter 7 for more detail on communications plans.

6.17 We propose that in conjunction with developing testing plans, firms should conduct lessons learned exercises. This is important as continuous improvements to operational resilience require firms to learn from experience as their operations and technology changes and their approach matures over time. Deficiencies, whether identified through scenario testing or through practical experience, should be addressed as a matter of priority. Firms should prioritise actions to address the risks posed by each deficiency.

Example: How the example firms may carry out scenario testing

Firm A

Firm A designs severe but plausible scenarios to test the supporting resources for telephone consumer authentication, as identified through the mapping process.

During scenario testing, Firm A identifies challenges to stay within an impact tolerance of 12 hours due to legacy systems and interdependencies between systems supporting more than 1 business service. Firm A finds that the impact of a severe but plausible scenario may result in loss of both telephone banking and online authentication services.

Firm A uses these test results to inform its short and longer-term investment and strategic priorities. Firm A also reviews what operational changes can be made to reduce the risk of harm from a disruptive event. In the short-term, among other actions, this includes developing a communications plan to explain to consumers the alternative ways to access services and updates for service resumption. Firm A also looks for ways to prioritise services for vulnerable consumers.

Firm A prioritises a strategic review to reduce the interdependencies between the online and telephone authentication supporting resources. It brings forward plans to upgrade its legacy systems with a view to deciding what changes can be made in the short, medium and longer term.

Firm B

Firm B carries out regular reviews of its supporting resources. It engages with its business consumers and counterparties to enhance the validity of these tests eg carrying out end to end tests for particular services involving all relevant parties.

These tests indicate some resilience gaps when faced with a severe but plausible scenario. So, the firm instigates a review. Firm B identifies appropriate solutions to address the resilience gaps. These include investment in further back-up IT systems, staff training to support changes, and reduced reliance on manual processes in operational areas.

Firm B recognises that it must take further steps to invest in monitoring and early detection of potential data loss issues. Firm B also reviews its communications plans and works with the firms that use the services provided through Firm B's online platform to enhance their ability to communicate with underlying consumers and reduce the impact of disruption.

Firm C

Firm C uses the following tests to determine whether its controls are effective and that it can remain within tolerance: 1) custody files generated for Consumer A include data for Consumer B and 2) a contractor extracts data for Consumer C.

The tests identify weaknesses in Firm C's current controls (ie the automated alerts and detection of confidentiality and integrity breaches do not flag these events as very high risk). Firm C's senior management agree these weaknesses need to be addressed as a high priority.

Firm D

Firm D recognises that it has not attempted a full fail-over to the second server.

Firm D uses 3 severe but plausible scenarios to test the impact tolerance for motor insurance renewals: (1) complete power loss at 1 of its operations sites for 48 hours; (2) a water leak that causes the main server room at 1 of its operations sites to shut down; and (3) a Sunday evening fail-over test that results in the corruption of consumer data for all motor policy renewal requests received since 9am on Saturday.

In scenario 1, Firm D concludes that it is not able to remain within the impact tolerance so it identifies significant changes to its business continuity planning (which include a 9-month home-working technology upgrade and a training programme for 50 experienced call handlers based at each site). It proposes to repeat the test after 12 months to test its ability to remain within the impact tolerance.

In scenario 2, Firm D concludes that the re-routing arrangements to the second operational site and the server capacity at the second operational site function as expected, and that it is able to remain within the impact tolerance.

In scenario 3, Firm D concludes that it will not always be able to operate within the impact tolerance and safely complete all affected motor insurance renewals. Its board approves an independent review of all relevant controls and underlying potential causes of failure, and a 3-year strategy to move all back-up data storage to a cloud service provider with real-time back up capability.

Tell us what you think:

Q8: **Do you agree with our proposed approach to testing? If not, please explain why.**

7 Communications, governance and self-assessment

This chapter sets out our proposals for firms to:

- communicate effectively in the event of a disruption
- create a self-assessment document

This chapter also reminds firms of existing governance requirements and their relevance to operational resilience.

Communications

7.1 In our DP, we highlighted the important role that fast and effective communications can play in mitigating harm at times of operational disruption. It is important that firms' policies include prompt and meaningful communication arrangements for internal and external parties, including regulators, consumers and the media.

7.2 We propose that firms should have internal and external communication strategies in place. This will help them to act quickly and effectively to reduce the harm caused by operational disruptions by providing clear, timely and relevant communications.

7.3 Firms' internal communication plans should also include the escalation paths they would use to manage communications during an incident, and identify the appropriate decision makers. For example, the plan should address how to contact key individuals, operational staff suppliers and the appropriate regulators.

7.4 As part of their external communications plans, we expect firms to consider in advance of a disruption how they would provide important warnings or advice quickly to consumers and other stakeholders. This includes where there is no direct line of communication.

7.5 As guidance, we propose that firms should also use effective communication to gather information about the cause, extent and impact of operational incidents.

Governance

7.6 In the DP, we noted that firms' boards and senior management should be sufficiently engaged in setting effective standards for operational resilience. The board and senior management should have sufficient time to establish the business and risk strategies and the management of the main risks relevant to operational resilience. Firms should ensure that in meeting their responsibilities, board members and senior management have the knowledge, experience and skills necessary for the discharge of the responsibilities allocated to them.

7.7 There are many existing requirements relevant to a firm's governance of operational resilience. There are also individual, and collective, responsibility and accountability requirements applicable to boards and senior management. We expect firms to continue to meet their obligations under these existing requirements. More information on existing FCA requirements is detailed in Annex 4.

Senior manager expectations

7.8 In line with good standards of general governance and the Senior Managers & Certification Regime (SM&CR), all firms' senior management should know what they are responsible and accountable for. This includes establishing clear lines of responsibility for the management of operational resilience (including the relevant proposals outlined within this CP). More detail on our SM&CR rules can be found in our Handbook and Policy Statements.

7.9 Firms should structure oversight of operational resilience in a way that is effective and proportionate for their business, using existing committees or establishing new ones if necessary. Attention must be paid to achieving a clear delegation of responsibilities where an important business service is supported by a wide range of people and systems. Irrespective of firm size or complexity we expect clarity on who is responsible for what within a firm, including for operational resilience.

7.10 The SM&CR currently applies to banking firms and insurers and will apply to FCA solo-regulated firms from December 2019. Under the SM&CR, individuals that perform the Chief Operations Function (SMF24) are required to have responsibility for managing the internal operations or technology of the firm or of a part of the firm. This includes, but may not necessarily be limited to, responsibility for areas such as:

- business continuity
- cybersecurity
- information technology
- internal operations
- operational continuity, resilience and strategy
- outsourcing, procurement and vendor management
- management of services shared with other group members

7.11 Firms that have an individual performing the SMF24 function may find that responsibility for implementing the proposals outlined within this CP falls within the scope of the SMF24's responsibilities.

7.12 The SM&CR is designed to apply in a proportionate and flexible way to accommodate the different business models and governance structures of firms. We are not considering changing this approach for the oversight of operational resilience. Where firms do not have an individual performing the SMF24 function under the SM&CR, it will be for the firm to determine the most appropriate individual within the firm who is accountable for operational resilience.

Board expectations

7.13 We will expect boards, or a firm's equivalent management body, to have appropriate management information available to them to inform decision making which has consequences for operational resilience. Individual board members will not necessarily be required to be technical experts on operational resilience but should, collectively, have

adequate knowledge, skills and expertise to provide constructive challenge to senior management as part of their oversight responsibilities in relation to operational resilience.

7.14 To demonstrate appropriate and effective oversight of operational resilience within firms, we will expect that boards, or a firm's equivalent management body, should be able to evidence that they are satisfied that the firm is meeting its responsibilities in respect of operational resilience. This includes those aspects relating to the identification of important business services, mapping and setting impact tolerances, as well as the firm's ability to remain within these tolerances.

Self-assessment

7.15 We also consider that it is important for firms to be able to demonstrate to the relevant supervisory authority that they are meeting their responsibilities in respect of operational resilience.

7.16 We therefore propose that firms should create a self-assessment document. The self-assessment document should include:

- the firm's important business services
- the impact tolerances set for these important business services
- the firm's approach to mapping, including how the firm has identified its resources, and how it has used mapping to identify vulnerabilities and support scenario testing
- the firm's strategy for testing its ability to deliver important business services within impact tolerances through severe but plausible scenarios, including a description of the scenarios used, the types of testing undertaken and the scenarios under which firms could not remain within their impact tolerances
- an identification of the vulnerabilities that threaten the firm's ability to deliver its important business services within impact tolerances, including the actions taken or planned, and justifications for their completion time
- the firm's lessons learned exercise
- the methodologies used to undertake the above activities

7.17 We also propose that boards, or the firm's equivalent management body, review and approve the self-assessment document regularly. Where changes occur that may have a clear impact on the firm's operational resilience, eg structural changes to the firm, rapid expansion, poor trading or entry into new markets, more frequent reviews of the firm's self-assessment document will be required.

7.18 We want the self-assessment, methodologies and documentation to be carried out and set by firms with the principle of proportionality in mind. This means that a firm's self-assessment, the methodologies that it uses and its documentation should be consistent with its obligations under the proposed policy requirements of this paper, its risk profile, its nature and business model, and the size and complexity of its activities.

7.19 To further reduce the burden on firms, we are not intending to place a requirement on firms to periodically submit the self-assessment document. Instead, we propose that it be sent to us when requested or made available for inspection as part of firm engagement.

7.20 Firms should not treat the self-assessment document as a tick box exercise; it does not replace the need for firms to effectively embed operational resilience. We will expect firms to consider how applying these requirements will support the aims of improving their operational resilience.

Tell us what you think:

Q9: **Do you agree with our proposals for communication plans? If not, please explain why.**

Q10: **Do you have any comments on our proposed requirement for a self-assessment document?**

8 Outsourcing and third-party service provision

Introduction

8.1 This chapter outlines the importance of outsourcing and other third-party service provision, to operational resilience and our expectations of firms. We expect an operationally resilient firm to have a comprehensive understanding and mapping of the resources that support their business services. This includes those outsourced and third-party services over which the firm may not have direct control. We also expect firms to be able to identify and document the resources that support their important business services.

8.2 This chapter also reminds firms of the current UK and European rules and guidance relevant to outsourcing and third-party service provision, with a particular focus on the implications for operational resilience.

8.3 We are not proposing changes to the FCA's Handbook rules and guidance on outsourcing or third-party service provision as part of this consultation. However, there are important regulatory developments that are of relevance to outsourcing and other third-party service provision with implications for operational resilience, particularly in relation to guidelines provided by the European Supervisory Authorities (ESAs) that we detail below. This includes highlighting our approach to ESA guidelines in the context of Brexit, the introduction of the European Banking Authority's (EBA)'s 'register of outsourcing'.

Overview

8.4 Firms' business models and their dependency on outsourced and third-party service providers is increasing, including through greater use of data driven innovation. This means an increased need for firms to effectively manage their third-party (including outsourced) service providers to manage the risk of disruption and harm to their consumers.

8.5 In an increasingly complex and fast changing business environment, we want the delivery of important business services by firms to be able to prevent, adapt, respond, recover and learn from disruptive operational incidents. To achieve this outcome, firms need to consider their dependency on services supplied by third-parties and the resilience of these third-party services. This includes those third-parties typically outside the regulatory perimeter, where firms retain responsibility for the delivery of their regulated services, including any dependency on the third-party service provider.

8.6 In our 2019/20 Business Plan, we set out our key priorities and planned activities for this year. This includes addressing the risks of harm that could result from insufficient operational resilience in firms and poor governance of outsourcing and third-party service provision.

8.7 Our focus in this area is a continuation of work carried out previously, including a cross-sector survey in 2017-18 through which we identified that:

- issues at third-parties, such as an IT failure at an important supplier, accounted for 15% of the operational incidents reported to the FCA. This demonstrates how increasingly important third parties are to firms and their consumers, and the need to manage them effectively to manage the risk of disruption.
- IT changes caused 20% of the operational incidents reported to the FCA
- half of firms said that they do not maintain a comprehensive list of all third-parties with who they do business and who have access to their systems and data
- 26% of firms did not have a board approved information security strategy
- only 56% of firms said they could measure the effectiveness of their information asset controls

8.8 Additionally, we have observed other areas of concern in relation to outsourcing and third-party service provision that can affect operational resilience of a firm's business services, including:

- harms and risks that can arise from high levels of concentration within third party service provider arrangements. For example, high dependency on a single third-party service provider by multiple firms can present additional challenges if more than 1 firm wishes to exit an arrangement at the same or similar time, or if the service provider has an operational resilience failure affecting multiple firms simultaneously. This may particularly be the case where it takes a long time to migrate a large outsourcing relationship.
- high levels of concentration within third-party service provider arrangements, reducing or undermining firms' ability to exert sufficient influence and control over their third-parties
- some third-party service suppliers operating in multiple jurisdictions with different, or lower quality, resilience requirements than expected by us.
- reduced cyber resilience within the firm due to cyber risks that originate from within the third-party service provider.
- how intra-group outsourcing arrangements are managed.

The findings indicate that some of the concepts set out in this CP, such as the identification of important business services and firms' dependence on operational resilience of third-parties, are not yet part of all firms' thinking. This includes how firms manage third-parties to ensure operational resilience can be maintained in the event of disruptions, including when taking steps to remain within impact tolerances.

Existing expectations on outsourcing and third-party service provision

8.9 The purpose of the high-level regulatory obligations on firms which use outsourced and third-party service providers, such as Principle 3 in our Principles for Business (PRIN) sourcebook, amplified by our Senior Management Arrangements, Systems and Controls (SYSC) sourcebook, includes that a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems. There are also specific rules and guidance for outsourcing eg SYSC 8 and 13, including the directly applicable Markets in Financial Instruments

Directive (MiFID) Org Regulation. The application of the rules and guidance differ based on firm type. For further guidance see 'M2G' The MiFID 2 Guide and the detailed application provisions and summary in SYSC 1 Annex 1 and SYSC 1.1A respectively.

8.10 The requirements and guidance include appropriately identifying and managing the associated operational risks throughout the life span of third-party arrangements from inception and on-boarding, through business as usual operation and exit or termination of the arrangements. Our approach is risk-based and proportionate, considering the nature, scale and complexity of a firm's operations. Firms should take account of the principle of proportionality when complying with their obligations for outsourcing and third-parties. The proportionality principle focuses on the characteristics of the firm eg the firm's size and complexity, including those related to outsourcing and use of third-parties, and aims to ensure that the objectives of the regulatory requirements are effectively achieved.

8.11 Intra-group outsourcing, including cross-border outsourcing to parent companies outside the UK, is subject to the same requirements as outsourcing to an external third-party. It should not be treated as being inherently less risky. Firms may consider the extent to which they can exert influence and the control they have over their third-parties, where those parties are members of the same group.

8.12 We view the provision of cloud services to regulated firms as a form of outsourcing. All forms of outsourcing are a sub-set of third-party service provision. Firms should be able to assess the impact of these providers on their operational resilience. For example, how cloud service provision affects the assessment of a firm's important business services operational resilience. We see no fundamental reason why cloud services cannot be implemented, with appropriate consideration, in a manner that complies with our rules. Where relevant, domestic guidance and ESA guidelines on cloud outsourcing should be interpreted in a manner proportionate to the size, structure and operational environment of the firm, as well as the nature, scale and complexity of its activities.

8.13 It is possible to have a key third-party service provider relationship that may not be classified as outsourcing including for example, other arrangements between firms and financial market infrastructures, or strategic partnerships with non-financial third-parties. Where key third-party service providers support the delivery of important business services, firms should ensure they appropriately identify and manage the associated operational risks to their operational resilience obligations, as defined in this CP. They must also meet their other regulatory obligations, for example in PRIN and SYSC.

8.14 In all outsourcing or third-party service provision scenarios, regulated firms retain full responsibility and accountability for discharging all their regulatory responsibilities. Firms cannot delegate any part of this responsibility to a third-party. Our expectations within the SM&CR are consistent with this. Similar expectations for governance arrangements are referenced within the FCA's Payment Services and Electronic Money Approach Document.

8.15 Firms should ensure that their risk management systems and controls adequately manage the risks associated with their outsourcing and third-party service providers, including:

- that the firm effectively follows the relevant rules and guidance

- assessing whether the firm's third-party arrangements meet the definition of outsourcing
- effectively applying regulatory obligations that apply to the risk management of third-party relationships, whether deemed outsourcing or not
- effectively applying the rules and guidance through the extended supply chain

Our overriding requirement is that a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.

Existing rules and guidance on outsourcing and third-party provision

8.16 Rules and guidance relevant to the management of outsourcing and third-party service provision risks are extensive. Their application depends on the firm's regulated status. There can be no substitute for reading rules and guidance that apply to the firm based on the firm's regulatory status. Annex 4 provides a summary of examples of relevant existing requirements. We have also sought to ensure that our outsourcing requirements align with the PRA's.

8.17 Different requirements apply to different types of firm and may also be determined by the type of function being outsourced. Of particular relevance is whether the function being outsourced is considered *critical or important*, whether it is *material* outsourcing, or if it relates to important operational functions. These are specific outsourcing terms applicable to different types of firms and are defined in domestic and European legislation, as applicable.

8.18 Terminology used to describe the importance of services provided by outsourced and third-party service suppliers may differ but their essence is that responsibility for the management of risk accrues to the firm in a proportionate manner. Specifically, risk management expectations become incrementally higher when a firm increases its dependence on outsourced and third-party service providers for the delivery of important business services. This includes the delivery of services that could affect the firm's ability to remain authorised. Expectations for operational resilience apply to all firms, irrespective of whether third-parties are used. Consequently, the impact of third-party service provision on firms can change over time and should be managed accordingly.

8.19 Our expectations for the management of outsourcing and third-party service provision extend to the amount and criticality of firm data being stored, processed or transmitted by outsourcers or other third-party service providers.

8.20 Firms should understand their responsibilities for data and ensure an appropriate level of confidentiality, integrity and availability for this data. This includes how firms configure and monitor their cloud services to reduce security and compliance incidents.

ESA guidelines on outsourcing, including cloud

8.21 The FCA engages with all three ESAs relating to the supervision of EU financial markets. These are the EBA, the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA). The following paragraphs explain our approach to ESA guidelines on outsourcing, including cloud.

8.22 The FCA has previously notified the EBA that it complies with the EBA's cloud recommendations (EBA/REC/2017/03).

8.23 Following the finalisation of the EBA's guidelines on outsourcing (EBA/GL/2019/02) in February 2019, which also subsumed the EBA's cloud recommendations, we have notified the EBA of our intent to comply with these EBA guidelines. The EBA guidelines are also addressed to credit institutions and investment firms, subject to the EU Capital Requirements Directive as well as to payment institutions and electronic money institutions. They do not apply to Account Information Service Providers (AISPs) that only provide the service in point 8 of Annex I of PSD2. This was confirmed in the FCA's August 2019 regulation round-up. The EBA guidelines applied from 30 September 2019 in respect of all outsourcing arrangements entered into, reviewed or amended on or after this date. There are also transitional arrangements extending up to 2021 relating to co-operation agreements, a register of outsourcing and the review of existing 'critical or important' outsourcing arrangements entered into before 30 September 2019. In-scope firms must make every effort to comply with the guidelines.

8.24 Our general approach to EU Level 3 materials (eg the ESA Guidelines) with regard to Brexit was confirmed in the FCA's Brexit Policy Statement (PS19/5) published in February 2019.

EBA 'register of outsourcing'

8.25 The EBA guidelines on outsourcing provide that those firms subject to the guidelines should maintain a 'register of outsourcing'. The EBA register builds on the existing EBA register introduced in the EBA's cloud recommendations. Firms subject to the EBA guidelines should address risks resulting from third-party service providers (EBA/GL/2019/02, Title III, paragraph 33) who may not be deemed to be outsourced service providers 'per se'.

8.26 In the face of continued risks and harms, we intend to explore the EBA 'register of outsourcing' concept more broadly at the domestic level using existing outsourcing reporting guidance that applies to firms (eg SYSC 8.1.12G, SYSC 13.9.2G and SUP 15.3.8G). We want to have consistent analytical capability on the amount and type of outsourcing that firms are undertaking, and the risks that it may present to the FCA's objectives, including resilience, concentration and competition risks.

8.27 This would be a step-change in our oversight of outsourcing, but one we believe could be beneficial. If progressed, we would undertake a formal consultation and seek to ensure that our approach is coordinated with any proposals that the PRA may make.

FCA FG16/5: Guidance for firms outsourcing to the 'cloud' and other third-party IT services

8.28 In July 2016, we published guidance to clarify the requirements for all FCA authorised firms when outsourcing to the cloud and other third-party IT services. Since publishing FG16/5, the EBA has finalised its own outsourcing cloud recommendations. In complying with the EBA cloud recommendations, the FCA altered the scope of its own FG16/5 guidance, so that firms subject to the EBA recommendations do not have to follow both.

8.29 We have taken a similar approach to the EBA's recently finalised outsourcing guidelines so that firms subject to the new EBA guidelines on outsourcing do not also need to follow the FCA's FG16/5.

Annex 1
Questions in this paper

Q1: Do you agree with our proposal for firms to identify their important business services? If not, please explain why.

Q2: Do you agree with our proposed guidance on identifying important business services? Are there any other factors for firms to consider?

Q3: Do you agree with our proposals for firms to set impact tolerances? If not, please explain why.

Q4: Do you agree that duration (time) should always be used as 1 of the metrics in setting impact tolerances? Are there any other metrics that should also be mandatory?

Q5: Do you agree with our proposal for dual-regulated firms to set up to 2 impact tolerances and solo-regulated firms to set 1 impact tolerance per important business service?

Q6: Do you have any comments on our proposed transitional arrangements?

Q7: Do you agree with our proposed approach to mapping? If not, please explain why.

Q8: Do you agree with our proposed approach to testing? If not, please explain why.

Q9: Do you agree with our proposals for communication plans? If not, please explain why.

Q10: Do you have any comments on our proposed requirement for a self-assessment document?

Q11: Do you have any comments on the cost benefit analysis?

Q12: Do you have any comments on the examples of existing legislation?

Annex 2
Cost benefit analysis

Introduction

1. In DP18/4 Building the UK financial sector's operational resilience, we suggested that operational resilience could be improved through an approach based on identifying important business services and setting impact tolerances for those services.

2. We considered the extent to which this approach might supplement existing policies to improve the resilience of the financial system and to increase the focus on this area within individual firms. This CP proposes a policy framework that aims to elaborate on the operational resilience outcomes being sought and details the requirements for firms.

3. FSMA, as amended by the Financial Services Act 2012, and including as applied by the Payment Services Regulations 2017 (PSRs 2017, SI 2017/752), requires us to publish a cost benefit analysis (CBA) of our proposed rules. Specifically, section 138I requires us to publish a CBA of proposed rules, defined as 'an analysis of the costs, together with an analysis of the benefits that will arise if the proposed rules are made'.

4. This analysis presents estimates of the impacts of our proposal. We provide monetary values for the impacts where we believe it is reasonably practicable to do so. For others, we provide estimates of outcomes in other dimensions. Our proposals are based on carefully weighing up these multiple dimensions and reaching a judgement about the appropriate level of consumer protection and market integrity, considering all the other impacts we foresee.

5. Regulation 106(3) of the PSRs 2017 states that we must have regard (among other things) to the principle that a burden or restriction which is imposed on a person, or on the carrying on of an activity, should be proportionate to the benefits. To assist us in assessing the proportionality of our proposals, we have considered whether they impose costs on PSPs beyond those costs which are inherent in the PSRs 2017.

Problem and rationale for intervention

6. Operational disruptions to the services that firms provide can potentially cause harm to consumers and market integrity.

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

- availability of existing business services: for example, when claiming on an insurance contract, making loan repayments, checking bank balances, redeeming investments in funds or accessing deposits and savings

- 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. This can result in delays, stress, reduced choices, additional or higher costs (including opportunity costs), and poor consumer service and treatment. Important consumer needs required by vulnerable consumers might not be met in a timely manner.

8. Harm to market participants and to the wider economy may arise from disruption to financial markets' operations, such as the forced closure of trading venues following a cyber-attack and the potential threat to market and supplier confidence that can result from a substantial disruption.

9. 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.

10. Operational risk management challenges have become more complex in recent years, due to an increased risk environment (technological changes and increasingly hostile cyber environment), firms' interconnectedness and reliance on third-parties.

11. Many firms have been, and can be, affected by operational disruption. Two common forms of failure are IT security breaches and third-party failures.

12. A UK Government survey in 2015 found that 90% of large businesses across all sectors had experienced a malicious IT security breach in the previous year. These breaches can disrupt the financial sector's operational capacity to provide important services to the economy. In financial year (FY) 2018/19, 852 technology and cyber incidents were reported by firms to the FCA. This is an increase of 272% from FY 2017/18 (when 229 technology and cyber incidents were reported), though this may reflect a change in reporting.

13. Third-party issues, such as an IT failure at an important supplier, accounted for 15% of the operational incidents reported to the FCA. This demonstrates how important third-parties are to firms and their consumers, and the need to manage them effectively to prevent disruption.

14. Operational disruptions can be considerably costly to consumers, firms and the wider economy, although it is difficult to place an estimate on the total cost of such disruptions. One way of understanding part of the costs is to look at the costs of regulatory fines imposed on firms, though operational disruptions can also incur costs beyond regulatory action and technological remediation. Examples of recent fines and associated disruption include:

- In May 2019, we issued a Final Notice to R. Raphael & Sons Plc imposing a fine of £775,100 (post-settlement) for regulatory failings in relation to its outsourcing arrangements. The PRA imposed a separate fine of £1.1 million (post-settlement) for the same failings.
- In a Final Notice published in 2014, the FCA fined RBS, NatWest and Ulster Bank £42 million for IT failures which occurred in June 2012. The PRA fined the banks £14 million. The IT failures affected over 6.5 million consumers in the UK for several weeks. Over the course of that period, consumers (both retail and wholesale) experienced considerable harm. This included: being unable to use online banking

facilities to access their accounts or obtain accurate account balances from ATMs; consumers were unable to make timely mortgage payments; consumers were left without cash in foreign countries; the banks applied incorrect credit and debit interest to consumers' accounts and produced inaccurate bank statements; and some organisations were unable to meet their payroll commitments or finalise their audited accounts.

- In a 2019 Final Notice following a cyber-attack, the FCA fined Tesco Personal Finance Plc £16.4 million for failing to exercise due skill, care and diligence in protecting its personal current account holders. Cyber attackers exploited deficiencies to carry out the attack. Those deficiencies left Tesco Bank's personal current account holders vulnerable to a largely avoidable incident that occurred over 48 hours and which netted the cyber attackers £2.26 million.
- The TSB migration failure in 2018 resulted in a loss of £330.2 million for TSB including consumer redress, rectification and associated remediation resource costs of £125.2 million. The FCA's investigation into this incident is ongoing.

Description of the drivers of harm

15. Market failures such as negative externalities, distorted incentives and imperfect information lead to suboptimal levels of operational resilience across firms and markets overall.

16. Negative externalities arise when consumers and other market participants may be viewed as third-parties and firms' approaches to the prioritisation of operational risks may not reflect the impact of operational disruptions on these third-parties. This is particularly an issue when the costs of such failures fall disproportionately on third-parties rather than firms themselves, reducing the incentive for firms to act without regulatory intervention. Consequently, firms may be investing less in operational resilience than the scale of the market and wider economic impact would justify.

17. Incentives to invest in operational resilience are distorted if firms do not face significant reputational costs from operational disruptions. This may happen when firms' consumers (ie the demand side of the market) do not react to such disruptions because of, for example, a lack of alternative providers or the perception that most firms in the market face similar disruptions.

18. Firms face imperfect information regarding operational resilience of their own systems. Operational resilience vulnerabilities often become apparent to firms only in the event of an operational incident and subsequent disruption. This suggests that firms may not be fully aware of their operational vulnerabilities.

Our proposed intervention

19. Operational resilience is already a responsibility of firms. However, it is a new and emerging area of regulation, where standards should be improved and current regulatory frameworks are not sufficiently driving change where it is needed.

20. This CP proposes a policy framework and details the requirements on firms, including that they:

- identify their important business services that, if disrupted, could cause harm to consumers or market integrity

- identify and document the people, processes, technology, facilities and information that support a firm's important business services (mapping)
- set impact tolerances for each important business service
- test their ability to remain within their impact tolerances through a range of severe but plausible disruption scenarios
- conduct lessons learned exercises to identify, prioritise and invest in their ability to respond and recover from disruptions as effectively as possible
- develop internal and external communications plans for when important business services are disrupted
- create a self-assessment document

Baseline and key assumptions

Baseline – existing regulatory frameworks

21. The costs and benefits of our proposed operational resilience framework need to be assessed against a baseline. Our proposed new rules and guidance build on existing regulatory frameworks which are relevant to operational resilience for all firms.

22. We have developed the policy proposals, the underlying draft rules and the CBA in the context of the existing UK and EU regulatory framework. We will keep the policy proposals and CBA under review to assess whether any amendments will be required due to changes in the UK regulatory framework.

23. Many existing statutory requirements, FCA rules and guidance and European legislation are relevant to a firm's operational resilience. At a high level, the FCA's Principles for Businesses (PRIN) set out general statements of the fundamental obligations for firms and The Threshold Conditions represent the minimum conditions which a firm is required to continuously 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. Additionally, SYSC includes rules and guidance about risk management and risk-centric governance arrangements.

24. PSPs are subject to the PSRs 2017 which implement the revised Payment Services Directive (PSD2). The Electronic Money Regulations 2011 (EMRs 2011, SI 2011/99) also contain requirements relevant to operational resilience. Firms should also be aware of the EBA Guidelines on the security measures for operational and security risks under PSD2, which contain requirements relevant to operational security.

25. Please refer to Annex 4 for more details about existing regulatory frameworks including further sector-specific examples.

26. We consider that the existing levels of regulatory requirements and the current market conditions are an appropriate baseline.

Affected firms

27. We are consulting on proposed new rules and guidance applicable to:

- c. 1,050 banks, building societies, PRA designated investment firms, Solvency II firms, Recognised Investment Exchanges and Enhanced scope SM&CR firms
- c. 1,100 Payment Institutions (PIs), Registered Account Information Service Providers (RAISPs) and Electronic Money Institutions (EMIs)

28. These figures are based on the number of authorised and registered firms at the time of writing this CP.

29. For dual-regulated firms, these costs are aligned with those presented in the PRA's CBA and do not reflect additional costs on top of the PRA's costs. Rather, these solely reflect the costs of the FCA's proposals, which we have calculated based on the baseline outlined in paragraphs 21 to 26. Both authorities have calculated the costs to our respective scopes using the data firms provided in response to the FCA's cost survey. Our average costs for large firms are lower than those for the PRA because we have a greater sample of large firms. The additional firms tend to be smaller than the average firm included in the PRA's large firm sample.

Data

30. We have asked firms to estimate the costs and benefits of implementing and operating the proposed policy framework relative to their firm. To assess these costs, we sent questionnaires to 1,562 firms at the legal entity level.

31. We drew randomised samples from each of the large, medium and small firm populations. We also drew a randomised sample of all sizes from the PI, RAISP and EMI population that are not also credit institutions to reflect that these firms are subject to specific requirements under the PSRs 2017 and EMRs 2011. Our initial questionnaire was sent to a wider population of firms than that proposed in this CP so our samples included firms that are out-of-scope, such as smaller firms. These out-of-scope firms have been excluded from our analysis.

32. We have excluded 4 observations from our analysis which appear to be significant outliers: 1 submitted by a large firm, 2 by medium sized firms and 1 by a PI firm. We have excluded these responses as their estimated total costs are of an order of magnitude larger than the rest of the responses of their respective subgroups. Where explanations of the costs have been provided in these responses, it is not clear that the identified costs truly represent incremental costs arising from the proposals.

33. By sampling across these categories, we sought to ensure that we received cost information from a range of firms that reflected the variety of firms and the important business services they provide.

Table 1: Firm type

Firm type	Number of firms in the market	Number of firms sampled	Number of firm responses
Large	184	110 (60%)	45 (41%)
Medium	870	144 (17%)	44 (31%)
PI/RAISP/EMI	1,097	445 (41%)	57 (13%)
Total	**2,151**	**699**	**146**

34. Please note that the percentages in the last column in Table 1 refer to the proportion of firms who responded in relation to the figure in the previous column.

Limitations, risks and uncertainties

35. Our CBA estimates are subject to several uncertainties and assumptions:

- Firms may have found it difficult when responding to our cost survey to envisage costs of operating and implementing the proposed policy framework without having sight of the final policy, potentially leading to the over- or understatement of the costs of different elements. Some firms may have misinterpreted how the requirements will apply or the extent to which they will replace existing compliance activities, thereby resulting in inaccurate cost estimations.
- A small sample size in subgroups reduces the reliability of conclusions that can be drawn from the data. There are issues with the statistical significance when collecting data from a small number of firms to reflect a large and diverse population. We have stratified responses by size to make the sample as representative as possible for the firms in scope of the proposed policy and make our estimates of industry costs as representative as possible of industry costs.
- Larger firms tend to be more likely to respond than smaller firms, as can be seen in Table 1 where 41% of all sampled large firms responded to our survey, while only 31% of medium firms and around 13% of PI/RAISP/EMI firms did. This tendency will also be the case within each size category, for example, 'larger' medium firms are more likely to respond than 'smaller' medium firms. This will likely bias the results of the survey upwards due to oversampling larger firms relative to smaller firms. This effect was also considered in the CBA for the Senior Managers & Certification Regime (SM&CR, paragraphs 3.11 and 3.12).
- Some firms provided figures in US Dollars (US$). We have used a fixed market exchange rate to ensure comparability for currency conversions.

Costs and benefits

Summary of costs and benefits

36. In the sections below, we have assessed the one-off and ongoing (annual) costs arising from each of the elements of the proposed framework. They include compliance costs directly arising from our intervention. They reflect the incremental changes that firms would not have undertaken in the absence of the regulation.

37. The following table sets out a summary of the estimated total costs of the proposals detailed in this CP. Similar to the approach outlined in the standardised cost model, we

have classified all regulated firms as large, medium or small using data from FCA annual fee blocks.

38. To calculate the values presented in this section, we have first excluded a small number of outliers from the submissions provided to us by firms, as explained in paragraph 32 above. We then calculated the average one-off and ongoing costs as the mean of the responses, broken down by cost type and size category (see Table 3). Finally, we multiplied these averages by the number of firms within each size category listed in Table 2 below to produce total cost estimates for the industry as a whole.

Table 2: Total costs for all firms, by firm size

Size of firm	One-off costs	Ongoing costs (annual)
Large	£142.6m	£75.8m
Medium	£315.3m	£128.2m
PI/RAISP/EMI	£34.3m	£27.4m
Total	**£492.3m**	**£231.3m**

39. Comparing the range of potential benefits with the estimated costs is difficult, but we have examined the extent to which consumers, firms or the wider economy would benefit if the proposed policy framework were to deter a number of incidents.

40. There are significant up-front costs in addition to the ongoing costs, while the benefits will solely be ongoing and will likely build over time. While it was not practicably possible to estimate the full value of the wide-ranging benefits of this intervention, the key benefits identified to consumers, firms, the FCA and wider stakeholders are material.

41. The submissions we received showed a large degree of heterogeneity of costs even within each of the size brackets we have considered. Many firms reported zero or relatively low incremental costs arising from our proposals, potentially reflecting that these firms are already operating on the basis of, or have set out independent plans towards, the framework set out in this document. However, in each size bracket there is also a long tail of responses that report high costs (in excess of the average costs used to calculate the above totals) that reflects their business models and the number of important business services they operate.

42. This wide variation in responses makes it especially difficult to estimate the expected cost that our proposals will have on industry and results in greater uncertainty over the total costs we have reported in Table 2. This skew in the distribution of responses is shown in the large differences between the mean and median values which we report later in Table 4 below.

43. In our assessment below (please refer to paragraph 78) we have used an average incident cost of £631.5k as reported to us across firms of all sizes) and the cost of a major disruption of £330 million to illustrate the break-even point to deliver net benefits. We believe that the introduction of our proposed policy framework is capable of delivering a reduction in the scale and frequency of disruptive incidents, and the potential harm these would cause, that would outweigh the expected costs of this market intervention over the medium term.

Costs

44. We asked firms, where possible, to categorise costs between implementation costs, IT costs and training costs. We also asked them to include costs of changes in governance with their implementation costs.

45. When our rules impact differently on different kinds of firms we recognise this by using 'average firm' figures for the types of firm affected (eg large vs small firms, or firms in different regimes, similar to the approach undertaken in the SM&CR extension CBA). However, it is important to note that firms will be affected by interventions differently according to their precise structure and existing approaches.

46. Therefore, the per-firm average estimated values provided in Table 3 below do not represent the costs we expect each firm of a given size to incur as a result of the proposals in this CP. Rather, these are averages published for the purposes of transparency for our calculations of the cost of these interventions. The size categories we have used are broad, and each encompasses a range of firm sizes, which in turn would have a range of compliance costs above or below the averages we have included.

Table 3: Average and median cost for an individual firm, by firm size

Size of firm	Average		Median	
	One-off costs	Ongoing costs (annual)	One-off costs	Ongoing costs (annual)
Large	£775.3k	£412.0k	£299.0k	£184.0k
Medium	£362.4k	£147.3k	£88.4k	£43.6k
PI/RAISP/EMI	£31.3k	£25.0k	£10.6k	£6.6k

47. We have also reported the per-firm median total costs in Table 3 above and broken down by different types of costs in Table 4 below, as these values differ significantly from the mean values. This highlights the fact that the distribution of costs reported to us includes many lower values and a few significantly higher values within each size category, which pulls up the mean of the distribution. The median may be a more accurate reflection of the costs expected to be incurred by a typical firm. However, the mean covers all outcomes including the lower frequency of higher costs expected by some firms. Therefore, for the purposes of the calculations within this CBA we have used the mean values, as a more conservative assumption.

Table 4: Mean and median one-off and ongoing costs for an individual firm, by firm size

Costs	Firm size	One-off costs		Ongoing costs (annual)	
		Mean	Median	Mean	Median
Implementation costs, including changes in governance	Large	£357.7k	£155.0k	£222.3k	£100.0k
	Medium	£218.3k	£63.1k	£76.6k	£30.0k
	PI/RAISP/EMI	£13.4k	£5.6k	£10.2k	£3.6k
IT costs	Large	£347.8k	£114.0k	£146.8k	£64.0k
	Medium	£127.5k	£20.1k	£61.0k	£10.0k
	PI/RAISP/EMI	£12.9k	£3.6k	£8.3k	£1.8k
Training costs	Large	£69.7k	£30.0k	£42.8k	£20.0k
	Medium	£16.7k	£5.1k	£9.8k	£3.6k
	PI/RAISP/EMI	£5.0k	£1.4k	£6.4k	£1.2k

48. We expect that firms will be required to incur costs to set up and maintain an implementation the proposed policy framework. Firms might further incur costs associated with the changes in governance as proposed in the CP. These costs could be one-off and ongoing, internal or outsourced. On the basis of the data provided to us by firms we expect these costs to correlate with firm size. We expect the one-off costs faced by large firms to average £357.7k, by medium firms to average £218.3k, and by PI/RAISP/EMI firms to average £13.4k. We expect the ongoing annual costs to be less than the one-off costs, but to still be significant as shown in Table 4.

Implementation costs, including changes in governance

49. Implementation costs include the time and resources spent by firms familiarising themselves with the proposals and performing a gap analysis to identify necessary changes as a result. These costs will be one-off and we would expect them to be reasonably small in comparison to other costs arising from these proposals.

50. To increase operational resilience, firms are expected to invest in better understanding their business services, adopt a model that treats disruption to business services as though it is inevitable and set appropriate tolerances. Firms are also expected to invest resources in people, processes, technology, facilities and information to ensure continuity, quick recoverability of their business services and contingency plans. Therefore, we believe firms will incur one-off costs through setting up the proposed framework and ongoing costs of maintaining it.

51. Firms are expected to change or revise their internal processes. Firms should ensure that in meeting their responsibilities, board members and senior management have the knowledge, experience and skills necessary for the discharge of the responsibilities allocated to them. Therefore, firms may incur one-off costs through changes to organisational structure and required adjustments, such as recruitment.

52. Any IT or training costs associated with the implementation and maintenance of the proposed framework are discussed in the paragraphs below and reported separately.

IT costs

53. We acknowledge that some firms will need to make adjustments to their IT systems when they implement the new proposals. For example, for setting impact tolerances, firms might need to capture how business services are distributed across different types of borrowers and so may need to change the existing IT systems to allow for such monitoring.

54. We expect that some firms will need to incur one-off investment costs in IT improvement to improve their standards in line with the policy proposals. For example, firms might invest in cybersecurity defences to reduce the risks of cyber-attacks.

55. Firms may incur ongoing maintenance costs that would require them to stay within the impact tolerances. We do not think that firms will need to have a significant upgrade of their IT systems on an ongoing basis, over and above the existing maintenance.

56. IT system costs will include not only the purchase or renting of hardware, but also staff and other costs associated with project management, programming, design and analysis. The implementation of the changes to IT systems could be undertaken by in-house teams or outsourced to third-parties. The IT costs are presented on a one-off and ongoing basis.

57. We expect the one-off IT costs faced by large firms to average £347.8k, by medium firms to average £127.5k, and by PI/RAISP/EMI firms to average £12.9k. We expect the ongoing annual costs to be less than the one-off costs, but to still be significant as shown in Table 4.

Training costs

58. Firms might need to brief or train existing personnel to ensure that the policy framework is implemented, maintained, revised and tested on an ongoing basis. Therefore, we expect firms to incur training costs. The training costs could be one-off and ongoing. We expect the one-off training costs faced by large firms to average £69.7k, by medium firms to average £16.7k, and by PI/RAISP/EMI firms to average £5.0k. We expect the ongoing annual costs to be less than the one-off costs, but to still be significant as shown in Table 4.

59. Training could encompass formal courses as well as informal dissemination via email or staff meetings. Some firms might have in-house training departments, where the costs include the time of internal staff to design and deliver training. Other firms might not have in-house training available and would incur the costs of purchasing training courses from external providers. These costs would also include e-training, development or purchase costs.

Costs to the FCA

60. We do not consider that our proposed approach will result in any significant increase in costs for the FCA. The proposed changes will build on existing regulatory frameworks which are relevant to operational resilience for all firms. The proposed changes will not result in any systems changes. We will include supervision of the new regulatory requirements into our existing supervisory and authorisation activities and allocate resources internally based on the prioritisation of arising risks.

Indirect impacts

61. Increased compliance costs, as set out above, will increase firms' operating costs. There may be additional costs for retail and wholesale consumers as they may be subject to price increases if firms seek to pass on the cost of implementing and operating the proposed policy framework.

62. In principle, increased compliance costs could have indirect effects on the market more widely such as increased barriers to entry and expansion and, possibly, as a result, have an impact on innovation, competition and choice for consumers.

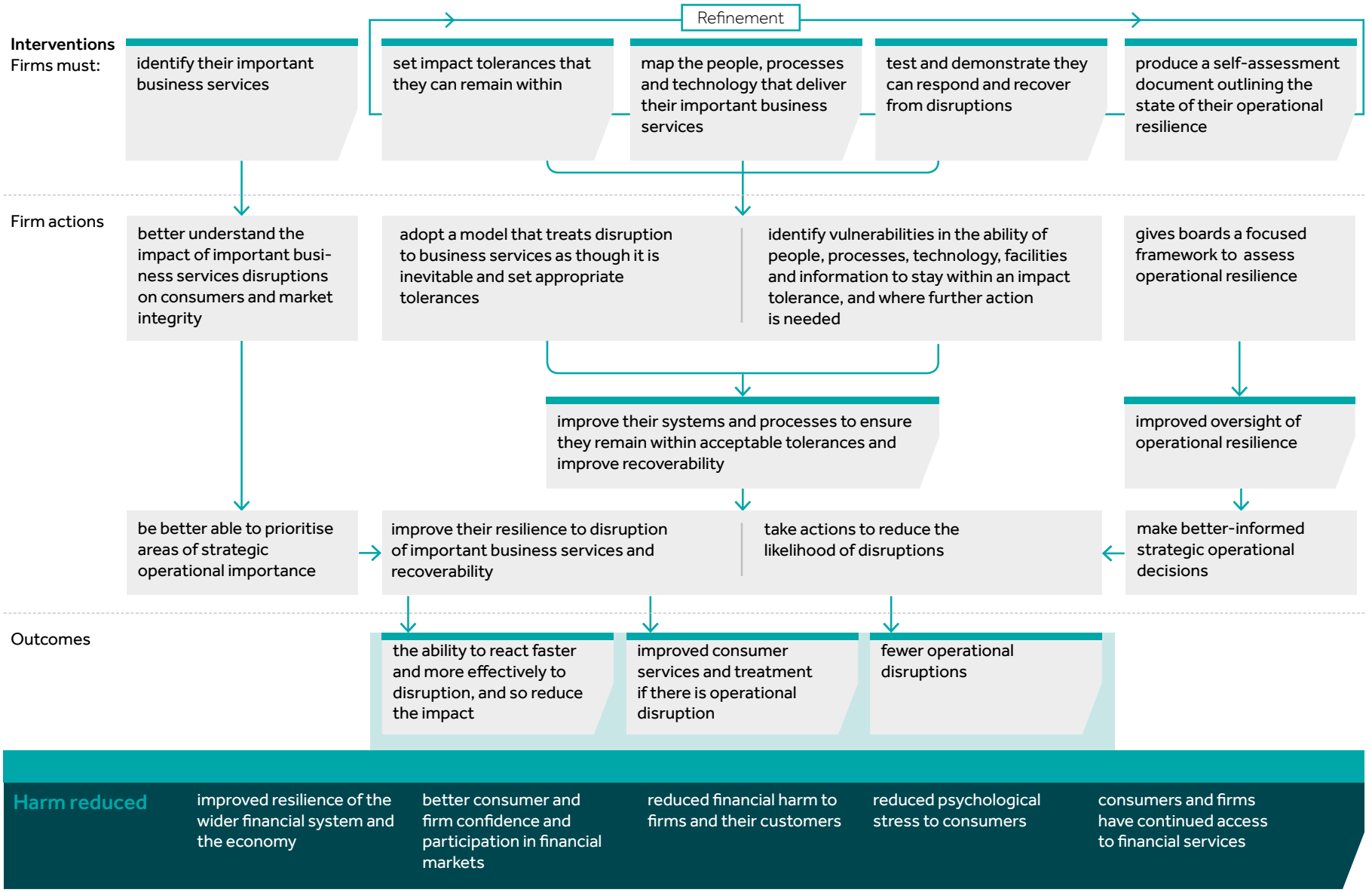
63. However, based on estimating costs provided by firms, we consider that these additional costs are likely to be manageable for firms as the overall increase in costs per firm is modest and is proportional to a firm's size. We do not expect the overall impact on innovation or prices across all sectors to be material or these proposals to act as a significant barrier to entry, and therefore we have not estimated them.

Benefits

64. The causal chain overleaf shows how these interventions will address the problem identified and lead to a reduction in harm. We believe our proposals help address the market failures we have outlined and will ultimately strengthen operational resilience within the firms that we regulate. This should lead to a mitigation of harm to consumers, market participants and the integrity of the UK financial system.

Causal chain

Figure 1: Operational resilience causal chain



Effects of the proposals

65. We expect that the package of proposals in this CP will help build firms' operational resilience, ensure the availability of business services and promote market integrity. As a result, the policy will benefit consumers, firms and the market as a whole. There are five distinct proposals within our package, the effects of which are each outlined below:

- Asking firms to identify their important business services and the impact which disruption to them will have on consumers and market integrity will improve firms' ability to prioritise areas of strategic operational importance, as they will understand the consequences of disruptions better. By prioritising these issues more effectively, firms will improve the resilience of their important business services and can identify areas where action can be taken to more effectively mitigate the risk of disruption or improve how quickly services can be restored when disruption happens.
- Asking firms to set and remain within impact tolerances will cause firms to move away from a traditional risk management approach, towards treating disruption to business services as though it were inevitable. Firms will assess their systems and processes, and make changes where these are currently not sufficiently robust to ensure that the firm will remain within acceptable tolerances in case of severe but plausible disruption.
- Asking firms to map the people, processes and technology that deliver their important business services will help firms to understand the resource and support requirements of these services and ensure that these requirements are met. Many firms have imperfect information and may only learn of their operational vulnerabilities after an incident has occurred. By mapping their people, processes and technology these firms will be able to identify vulnerabilities in their ability to deliver important business services and to recover from disruption before any incident occurs. For example, a firm may identify where significant elements of delivering its important business services are provided by external parties, highlighting where the firm's control over continual supply is more limited. As a result, firms will be able to improve their systems and processes to mitigate the vulnerabilities they have identified.
- This will also result from and be further reinforced by asking firms to test and demonstrate their ability to respond to and recover from disruptions. By testing against severe but plausible scenarios, firms will identify points of failure or weaknesses in a safe manner, allowing them to take action to correct and improve their systems and processes before disruption to their important business services actually occurs.
- Asking firms to produce a self-assessment document outlining the state of their operational resilience provides boards with a more robust framework to assess operational resilience. This will ensure that boards understand their responsibilities and act on them, improving oversight of operational resilience in the firm. With better oversight and a robust framework for assessment, firms will be able to make better-informed strategic, operational and investment decisions which will improve their operational resilience.

Benefits for consumers, firms and the wider economy

66. Each of these interventions leads to improvements in firms' operational resilience to disruption, whether by changes to firms' systems and processes or by providing better information to the decision-makers in firms. Importantly, however, the package of interventions works together, with each element facilitating or enhancing the effects of the others.

67. The improvements they make to operational resilience will allow firms to react faster and more effectively when their important business services are disrupted, thereby reducing the number of consumers affected and lessening the impact on those that are affected. As a direct benefit of this, their consumers will have continued access to financial services, and reduced psychological stress associated with inaccessibility of important business services, as these services will be disrupted for a shorter period of time.

68. Reduced severity and length of disruption will reduce the financial harm caused to consumers, as well as to the firm itself. Indirectly, these reductions in harm will also improve confidence in financial markets and consumer participation. Consumers may start using services that they did not use before, benefitting from the wider range of choices available to them.

69. These interventions will allow firms to identify ways in which they can avoid disruption altogether, for example, by resolving issues around single points of failure. Avoiding disruption will lead to significant harm being avoided. As above, consumers of the firm that would have been disrupted will have continued access to financial services and benefit from reduced financial harm. Avoiding disruption will also mean avoiding the significant financial costs that these events can cause to the firm through foregone and failed transactions, resources spent on recovery and redress, as well as any fines imposed by regulatory bodies.

70. In addition, by considering impact tolerances and assessing their systems and processes, firms are likely to be able to provide better customer service to their consumers in the event of operational disruption as they will have run through scenarios of what would happen during disruption rather than treating it simply as an unlikely adverse event. This may mitigate any reputational cost to firms of operational disruption.

71. Building up the operational resilience of firms across financial markets will improve the resilience of the wider financial system and the economy as a whole by reducing the likelihood of major incidents and market disruptions, ensuring market integrity of the financial sector. By reducing the frequency, severity and duration of disruptions to important business services, financial services will become more reliable.

Estimating benefits

72. Estimating and quantifying the range of potential benefits these proposals are designed to achieve is difficult. In some instances, we have not attempted to quantify benefits because we believe that the scale of such benefits cannot be reliably estimated. Instead, we have illustrated the extent to which consumers, firms or the wider economy would benefit if the proposed policy framework were to deter a number of incidents. We are unable to accurately predict the frequency and severity of disruptive incidents in the future and so have used incidents similar in significance and magnitude to the ones that have already happened in the UK financial markets as the best available proxy, noting the uncertainty inherent in this exercise.

73. Examples of such incidents have been included earlier in this Annex. The fines imposed alone on firms for their regulatory failings in these incidents range from hundreds of thousands to tens of millions of pounds. In the most severe case, the total cost of an incident in 2018 was over £330 million.

74. We also asked firms to provide an estimated cost of disruptions to the services provided to their consumers in the last 5 years. From these data, we can estimate the direct benefits to firms in terms of the reduction in costs arising from the operational disruptions.

75. This will not capture all benefits that we expect our proposals to deliver, for example it will not capture the cost of lost access to financial services and psychological distress resulting from disruption, except to the extent that this has resulted in redress being paid to consumers. Nor will it capture benefits to the stability of financial markets and to the wider economy.

76. The disruptions identified and quantified by firms varied considerably in nature and scale. They included cloud service connectivity problems, delays in executing payments to third-parties, service upgrade or migration problems, power outages, malicious attacks on their servers, and more. The cost of incidents ranged from hundreds to tens of millions of pounds.

77. Overall, in our sample of 306 respondents there were 87 firms that identified at least 1 incident in the last 5 years that led to quantifiable costs to their business, totalling £96.4 million. Some of these firms identified just the total cost of a range of incidents, others separately identified individual incidents. A total of 108 individual incidents were reported to us, accounting for £68.2 million of the total costs of £96.4 million identified and with an average cost per incident of £631.5k.

78. We have compared the evidence of the cost of disruptions against the total costs we expect to the industry as a whole over a 5-year horizon to illustrate how many incidents would need to be avoided for these proposals to be net beneficial. For illustration:

- Using an average incident cost of £631.5k, the average incident cost reported to us across firms of all sizes, and assuming no further benefit of the proposals beyond the direct costs avoided by firms, the proposals would be net beneficial if they led to the avoidance of around 530 incidents per year (please refer to paragraph 12 for more information on incident reporting), or if they reduced the severity of a proportionately higher number of such events. The number of incidents was calculated as the break-even point using a 5-year Net Present Value (NPV) with a discount rate of 3.5% in line with our approach to CBAs.
- In practice, far fewer incidents would need to be avoided for the proposals to be net beneficial including all expected benefits identified in the above section, but as we have not been able to quantify these benefits it is not possible to say exactly by how much the number of incidents avoided would need to be reduced.
- Taking the major disruption described above as an example, where the total cost of disruption was around £330 million, the proposals would be net beneficial if they led to the avoidance of around 1 such event per year, or if they reduced the severity of a proportionately higher number of such events. In this particular example, the estimated benefit is likely to be closer to the total cost of the incident as it includes significant consumer redress, rectification and remediation costs. However, there will still be benefits to the wider economy that are not represented in this cost figure and so the actual number of events needed to be avoided per year will be less than the figure we have calculated.

79. These numbers are illustrative of the break-even point if the assumed avoided cost of disruption were the only benefit of our proposals. However, there is great uncertainty over the number and scale of disruptive incidents that firms will experience in the future.

80. We believe that the benefits of our proposals will actually be delivered in the form of a combination of avoidable costs such as regulatory fines, the costs of operational disruptions of various scales and of the infrequent but extreme disruptions experienced by large (and often systemically-important) firms. In addition, there will be benefits in the form of continued access, avoided psychological stress and benefits to the stability of the financial system and wider economy that we have not been able to quantify, but which will be a part of the overall package of benefits that we expect these proposals to deliver.

81. Taking all these benefits in the round and noting the difficulty of quantifying many of them, we believe that our proposals will be net beneficial in the short to medium term.

Q11: Do you have any comments on the cost benefit analysis?

Annex 3
Compatibility statement

Compliance with legal requirements

1. This Annex records the FCA's compliance with a number of legal requirements applicable to the proposals in this consultation, including an explanation of the FCA's reasons for concluding that our proposals in this consultation are compatible with certain requirements under the Financial Services and Markets Act 2000 (FSMA).

2. When consulting on new rules, the FCA is required by section 138I(2)(d) FSMA to include an explanation of why it believes making the proposed rules is (a) compatible with its general duty, under s. 1B(1) FSMA, so far as reasonably possible, to act in a way which is compatible with its strategic objective and advances 1 or more of its operational objectives, and (b) its general duty under s. 1B(5)(a) FSMA to have regard to the regulatory principles in s. 3B FSMA. The FCA is also required by s. 138K(2) FSMA to state its opinion on whether the proposed rules will have a significantly different impact on mutual societies as opposed to other authorised persons.

3. This Annex also sets out the FCA's view of how the proposed rules are compatible with the duty on the FCA to discharge its general functions (which include rule-making) in a way which promotes effective competition in the interests of consumers (s. 1B(4)). This duty applies in so far as promoting competition is compatible with advancing the FCA's consumer protection and/or integrity objectives.

4. In addition, this Annex explains how we have considered the recommendations made by the Treasury under s. 1JA FSMA about aspects of the economic policy of Her Majesty's Government to which we should have regard in connection with our general duties.

5. This Annex includes our assessment of the equality and diversity implications of these proposals.

6. Under the Legislative and Regulatory Reform Act 2006 (LRRA) the FCA is subject to requirements to have regard to a number of high-level 'Principles' in the exercise of some of our regulatory functions and to have regard to a 'Regulators' Code' when determining general policies and principles and giving general guidance (but not when exercising other legislative functions like making rules). This Annex sets out how we have complied with requirements under the LRRA.

The FCA's objectives and regulatory principles: Compatibility statement

7. The proposals set out in this consultation are primarily intended to advance the FCA's objectives of reducing harm to consumers and market integrity.

8. The proposals will improve the way in which firms ensure the ongoing availability of business services to consumers and help build the resilience of the market to continue to function as effectively as possible and return to full effectiveness quickly following a disruption.

9. In preparing the proposals set out in this consultation, the FCA has had regard to the regulatory principles set out in s.3B FSMA.

The need to use our resources in the most efficient and economic way

10. Our proposals are designed to be as proportionate as possible and ensure that firms have clarity about our expectations.

The principle that a burden or restriction should be proportionate to the benefits

11. The CBA in Annex 2 sets out the costs and benefits of the proposals in this CP. We believe that the benefits of these proposals outweigh the costs.

The desirability of sustainable growth in the economy of the United Kingdom in the medium or long term

12. These proposals support the UK financial sector's operational resilience, which is intended to have a positive impact on firms' ability to recover from operational disruptions, creating greater sustainability of any market growth.

The general principle that consumers should take responsibility for their decisions

13. The proposals strengthen operational resilience frameworks. Consumers do not have any influence over these.

The desirability of recognising differences in the nature of, and objectives of, businesses carried on by different persons including mutual societies and other kinds of business organisation

14. We believe our proposals do not undermine this principle and in tailoring them to different firm types we believe that we have recognised the variety of firms affected.

The principle that we should exercise our functions as transparently as possible

15. We continue to engage with industry and other stakeholders to obtain feedback during the consultation process.

Expected effect on mutual societies

16. The FCA does not expect the proposals in this paper to have a significantly different impact on mutual societies. Only Building Societies and large Friendly Societies covered by Solvency II are in scope of the policy framework.

Compatibility with the duty to promote effective competition in the interests of consumers

17. In preparing the proposals as set out in this consultation, we have had regard to the FCA's duty to promote effective competition in the interests of consumers.

18. We consider that consumers may be more likely to choose firms that are more resilient to operational disruptions and that this may drive firms to compete for, and retain, consumers by improving their operational resilience.

19. We have also kept the competition objective in mind when framing how these proposals should be implemented, with a particular focus on whether there is a risk of weakening competitive pressure, disadvantaging smaller firms and potential new entrants.

Equality and diversity

20. We are required under the Equality Act 2010 in exercising our functions to 'have due regard' to the need to eliminate discrimination, harassment, victimisation and any other conduct prohibited by or under the Act, advance equality of opportunity between persons who share a relevant protected characteristic and those who do not, to and foster good relations between people who share a protected characteristic and those who do not.

21. As part of this, we ensure the equality and diversity implications of any new policy proposals are considered. The outcome of our consideration in relation to these matters in this case is stated in paragraph 2.15 of this CP.

Legislative and Regulatory Reform Act 2006 (LRRA)

22. We have considered the principles in the LRRA for the proposals that consist of general policies, principles or guidance and think that they will help firms understand and meet the regulatory requirements associated with existing and proposed operational resilience frameworks, leading to better outcomes for consumers and market integrity. We also believe the proposals are proportionate and take account of the variety of firms in scope.

23. We have considered the Regulators' Code for the parts of the proposals that consist of general policies, principles or guidance and believe that the proposals are proportionate and do not create an unnecessary burden on firms, or adversely affect competition.

HM Treasury recommendations about economic policy

24. These are the HM Treasury recommendations most relevant to our proposals, specifically the government's economic policy:

- 'continuing to strengthen the financial system, improving the regulatory framework to reduce risks to the taxpayer and building resilience, so that it can provide finance and financial services to the real economy and realise better outcomes for consumers, supporting sustainable economic growth and encouraging productive investment.'
- aspects of the government's economic policy that relate to Growth, Better outcomes for consumers and Competition.

25. Our proposals aim to strengthen the UK financial sector's operational resilience, ensuring that firms have a robust framework by which to measure their ability to recover from operational disruptions and continue to deliver important business services.

26. We believe that our proposals do not undermine the Treasury's Competition recommendations.

Annex 4
Examples of relevant existing FCA requirements

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

The Principles

2. The FCA's Principles for Businesses (PRIN) set out high-level general statements of the fundamental obligations for firms. They include: 'A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems' (Principle 3, PRIN 2.1).

The Threshold Conditions and Threshold Conditions Sourcebook

3. The Threshold Conditions (Schedule 6 to FSMA 2000) represent the minimum conditions which a firm is required to continuously satisfy at all times to be given and retain permission to carry on regulated activities under Part 4A FSMA. The Threshold Conditions Sourcebook (COND) provides guidance on how the FCA will approach its assessment of applicable threshold conditions.

4. 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 firms (Paragraph 3C of Schedule 6 to FSMA) or the appropriate resources threshold condition for solo-regulated firms (Paragraph 2D of Schedule 6 to FSMA).

5. COND 2.4.4G provides guidance on the assessment of this Threshold Condition. It includes: 'whether the firm has taken reasonable steps to identify and measure any risks of regulatory concern that it may encounter in conducting its business (see COND 2.4.6G) and has installed appropriate systems and controls and appointed appropriate human resources to measure them prudently at all times' (COND 2.4.4G(2)(d)).

6. When considering the 'Business Model' Threshold Condition guidance (Paragraph 2F of Schedule 6 to FSMA for solo-regulated firms, Paragraph 3E of schedule 6 to FSMA for dual-regulated firms), 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' (COND 2.7.10G).

SYSC – Senior Management Arrangements, Systems and Controls

7. SYSC includes rules and guidance about risk management and risk-centric governance arrangements (for the detailed application of the SYSC Sourcebook see SYSC 1 Annex 1 and the text in relevant SYSC chapters). For example:

- SYSC 4.1.1R(1) states that: 'A firm must have robust governance arrangements, which include a clear organisational structure with well defined, transparent and consistent lines of 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'. See SYSC 3.1 and 3.2 (especially SYSC 3.1.1R and 3.2.6R for insurers, managing agents and the Society) and the Investment Funds Sourcebook (FUND) 3.7 for a full-scope UK Alternative Investment Fund Manager (AIFM) of an authorised Alternative Investment Fund (AIF).
- SYSC 4.1.6R and 4.1.7R set out rules relating to business continuity for common platform firms, CRR firms and management companies as defined in the FCA Handbook Glossary. 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. 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 on the appointment of a Chief Risk Officer and the role of a governing body risk committee.
- 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 on 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 in the FCA Handbook or in other legislation, which may apply. This includes any relevant European Supervisory Authorities' (ESAs) guidelines and directly applicable EU legislation, such as the MiFID Org Regulation (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). This Regulation includes requirements relevant to operational resilience that apply to some firms. The MiFID 2 Guide (M2G) in the FCA Handbook provides guidance on the application of the MiFID Org Regulation as do relevant parts of SYSC.

Sector specific requirements (examples)

Trading venues – Recognised Investment Exchanges (RIEs) – Recognised Investment Exchanges Sourcebook (REC)

8. All UK investment exchanges must meet certain requirements to obtain recognition from the FCA. Recognition requirements include UK RIEs ensuring that their systems and controls are adequate, effective and appropriate for the scale and nature of their 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 (Schedule to the Recognition Requirements for Investment Exchanges and Clearing Houses Regulations, paragraph 3).

9. REC 2.5.5G to REC 2.5.20G in the FCA Handbook provides guidance on matters to which the FCA may have regard in assessing such systems and controls and certain other aspects of RIE operations.

Multilateral trading facilities (as defined in the FCA Handbook) and Organised trading facilities (as defined in the FCA Handbook) – Market Conduct Sourcebook (MAR)

10. MAR contains rules and guidance regarding risk management and contingency arrangements. 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 the 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 (as defined in the FCA Handbook)

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

- Article 15 of Commission Delegated Regulation (EU) 2017/584 of 14 July 2016 supplementing MiFID II with regard to RTS 7 specifying organisational requirements of trading venues 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 2 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) and Electronic Money Regulations 2011 (EMRs 2011)

12. The Payment Services Regulations 2017 (PSRs 2017) and Electronic Money Regulations 2011 (EMRs 2011) contain requirements relevant to operational resilience. For example:

- Regulation 6 PSRs 2017 (Conditions for authorisation as a payment institution) and Regulation 6 EMRs (Conditions for authorisation) – the authorisation and registration conditions for Payment Service Providers (PSP) that are Payment Institutions and Electronic Money Institutions only (i.e. not banks, building societies or credit unions).
- Regulations 85 – 89 PSRs 2017 (Execution time and value date) – PSPs must execute payment transactions within specific time limits.
- Regulation 98 PSRs 2017 (Management of operational and security risks) – PSPs must establish a framework, with appropriate mitigation measures and control mechanisms, to manage the operational and security risks relating to the payment services they provide and must also provide the FCA, on at least an annual basis, with an updated and comprehensive assessment of those risks.
- Regulation 99 PSRs 2017 (Incident reporting) – requires PSPs to (a) notify the FCA of major operational or security incidents and (b) if the incident has or may have an impact on the financial interests of its payment service users, inform users without delay.

13. Additional guidance on these issues can be found in Chapters 13 and 18 of Payment Services and Electronic Money – Our Approach

14. EBA Guidelines on the security measures for operational and security risks under PSD2 includes requirements relevant to operational security. For example:

- Guideline 2: Governance
- Guideline 3: Risk Assessment
- Guideline 7: Testing of security measures

15. Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing PSD2 with regard to RTS on strong customer authentication and secure communication contains requirements for dedicated interfaces (for third party access to payment accounts). These include requirements for performance indicators and service level targets, and contingency measures in the event of the failure of the interface.

16. In respect of PSPs that are Payment Institutions and Electronic Money Institutions only the 2017 EBA Guidelines under Directive (EU) 2015/2366 (PSD2) on the information to be provided for the authorisation of payment institutions and e-money institutions and for the registration of account information service providers, particularly:

- Guideline 9 on the procedure for monitoring, handling and following up on security incidents and security-related customer complaints
- Guideline 11 on business continuity arrangements
- Guideline 12 on the principles and definitions applicable to the collection of statistical data on performance, transactions and fraud

Q12: Do you have any comments on the examples of existing legislation?

Annex 5
Abbreviations in this paper

AIFMD	Alternative Investment Fund Managers Directive
AISP	Account Information Service Provider
CBA	Cost Benefit Analysis
COCON	Conduct Rules (Handbook)
COND	Threshold Conditions
CP	Consultation Paper
CRD	Capital Requirements Directive
CRR	Capital Requirements Regulation
DP	Discussion Paper
EBA	European Banking Authority
EEA	European Economic Area
EIOPA	European Insurance and Occupational Pensions Authority
EMI	Electronic Money Institution
EMR	Electronic Money Regulation 2011
ESA	European Supervisory Authorities
ESMA	European Securities and Markets Authority
EU	European Union
FCA	Financial Conduct Authority
FSMA	Financial Services and Markets Act 2000
MiFID	Markets in Financial Instruments Directive
MTF	Multilateral Trading Facility
OTF	Organised Trading Facility

PI	Payment Institution
PRA	Prudential Regulation Authority
PRIN	Principles of Business
PS	Policy Statement
PSD2	Revised Payment Services Directive
PSP	Payment service provider
PSRs 2017	Payments Services Regulations 2017
RAISP	Registered Account Information Service Provider
RIE	Recognised Investment Exchanges
SM&CR	Senior Managers & Certification Regime
SMF	Senior Management Function
SUP	Supervision Manual (Handbook)
SYSC	Senior Management Arrangements, Systems and Controls (Handbook)
UCITS	Undertakings for Collective Investment in Transferable Securities
UK	United Kingdom

We have developed the policy in this Consultation Paper in the context of the existing UK and EU regulatory framework. The Government has made clear that it will continue to implement and apply EU law until the UK has left the EU. We will keep the proposals under review to assess whether any amendments may be required in the event of changes in the UK regulatory framework in the future.

We make all responses to formal consultation available for public inspection unless the respondent requests otherwise. We will not regard a standard confidentiality statement in an email message as a request for non-disclosure.

Despite this, we may be asked to disclose a confidential response under the Freedom of Information Act 2000. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by the Information Commissioner and the Information Rights Tribunal.

All our publications are available to download from www.fca.org.uk. If you would like to receive this paper in an alternative format, please call 020 7066 7948 or email: publications_graphics@fca.org.uk or write to: Editorial and Digital team, Financial Conduct Authority, 12 Endeavour Square, London E20 1JN

Appendix 1
Draft Handbook text

OPERATIONAL RESILIENCE INSTRUMENT 2020

Powers exercised

A. The Financial Conduct Authority ("the FCA") makes this instrument in the exercise of the powers and related provisions in or under:

(1) the following sections of the Financial Services and Markets Act 2000 ("the Act"), including as applied by paragraph 3 of Schedule 6 to the Payment Services Regulations 2017 (SI 2017/752) ("the PSRs") and paragraph 2A of Schedule 3 to the Electronic Money Regulations 2011 ("SI 2011/99") ("the EMRs"):

(a) section 137A (The FCA's general rule-making power);
(b) section 138D (Actions for damages);
(c) section 137T (General supplementary powers);
(d) section 139A (Guidance);
(e) section 247 (Trust scheme rules);
(f) section 261I (Contractual scheme rules); and

(2) regulation 120 (Guidance) of the PSRs;

(3) regulation 60 (Guidance) of the EMRs;

(4) regulation 11 of the Financial Services and Markets Act 2000 (Recognition Requirements for Investment Exchanges and Clearing Houses) Regulations 2001 (SI 2001/995); and

(5) the other powers and related provisions listed in Schedule 4 (Powers exercised) to the General Provisions of the Handbook.

B. The rule-making provisions referred to above are specified for the purposes of section 138G(2) (Rule-making instruments) of the Act.

Commencement

C. This instrument comes into force on [*date*].

Amendments to the Handbook

D. The modules of the FCA's Handbook of rules and guidance listed in column (1) below are amended in accordance with the Annexes to this instrument listed in column (2) below:

(1)	(2)
Glossary of definitions	Annex A
Senior Management Arrangements, Systems and Controls sourcebook (SYSC)	Annex B

Supervision manual (SUP)	Annex C
Recognised Investment Exchanges sourcebook (REC)	Annex D

Citation

E. This instrument may be cited as the Operational Resilience Instrument 2020.

By order of the Board
[*date*]

Annex A

Amendments to the Glossary of definitions

Insert the following new definitions in the appropriate alphabetical position. The text is not underlined.

important business service	means a service provided by a *firm*, or by another *person* on behalf of the *firm*, to one or more *clients* of the *firm* which, if disrupted, could cause intolerable levels of: (1) harm to any one or more of the *firm*'s *clients*; or (2) risk to the soundness, stability or resilience of the *UK financial system* or the orderly operation of the financial markets.
impact tolerance	means the maximum tolerable level of disruption to an *important business service*, as measured by a length of time and other relevant metrics, reflecting the point at which any further disruption to the *important business service* could pose intolerable harm to any one or more of the *firm*'s *clients* or intolerable risk to the soundness, stability or resilience of the *UK financial system* or the orderly operation of the financial markets.

Annex B

Amendments to the Senior Management Arrangements, Systems and Controls sourcebook (SYSC)

In this Annex, underlining indicates new text, unless otherwise stated.

1 Application and purpose

1.1A Application

…

1.1A.1 G The application of this sourcebook is summarised at a high level in the following table. The detailed application is cut back in *SYSC* 1 Annex 1 and in the text of each chapter.

Type of firm	Applicable chapters
Insurer, *UK ISPV*	Chapters 2, 3, 12 to 18, 19F.2, 21, 22, 23, 24, 25, 26, 27, 28
Managing agent	Chapters 2, 3, 11, 12, 15A, 18, 19F.2, 21, 22, 23, 24, 25, 26, 27, 28
Society	Chapters 2, 3, 12, 15A, 18, 19F.2, 21, 22, 23, 24, 25, 26, 27, 28
Any other *SMCR firm*	Chapters 4 to 12, 15A, 18, 19D, 19F.2, 21, 22, 23, 24, 25, 26, 27, 28
Every other *firm*	Chapters 4 to 12, 15A, 18, 19D, 19F.2, 21, 22, 28

…

1.1A.1B G Chapter 15A of this sourcebook also applies to:

(1) an *electronic money institution*, a *payment institution* and a *registered account information service provider*;

(2) the provision of *payment services* and the issuing of *electronic money* (where the activity is not issuing electronic money specified in article 9B of the *Regulated Activities Order)*;

as set out in the text of that chapter.

…

1.4.2 R A contravention of a *rule* in *SYSC* 11 to *SYSC* 14, *SYSC* 18 to *SYSC* 21, *SYSC* 22.8.1R, *SYSC* 22.9.1R or *SYSC* 23 to *SYSC* 28 does not give rise to a right of action by a *private person* under section 138D of the *Act* (and each of those *rules* is specified under section 138D(3) of the *Act* as a provision giving rise to no such right of action).

Insert the following new chapter, SYSC 15A, after SYSC 14 (Risk management and associated systems and controls for insurers). The text is not underlined.

15A Operational resilience

15A.1 Application

Application

15A.1.1 R This chapter applies to:

(1) a *firm* that is:

(a) an *enhanced scope SMCR firm*;

(b) a *bank*;

(c) a *designated investment firm*;

(d) a *building society*;

(e) a *Solvency II firm*,

that is not:

(f) an *incoming EEA firm*; or

(g) an *incoming Treaty firm*;

(2) a *UK RIE*.

(3) an *electronic money institution*, a *payment institution* or a *registered account information service provider.*

15A.1.2 R In this chapter, a reference to a *firm* includes a *UK RIE*, an *electronic money institution*, a *payment institution* and a *registered account information service provider*.

15A.1.3 R In this chapter, a reference to a *client* in relation to a *UK RIE* includes a *person* who is entitled, under an arrangement or agreement between them and that *UK RIE*, to use the *UK RIE*'s *facilities*.

15A.1.4 R In this chapter, a reference to a *client* in relation to a *firm* carrying on the activity of *managing a UCITS* or *managing an AIF* includes:

(1) a *Unitholder*;

(2) an investor in an *AIF*.

15A.1.5 R The requirements in this chapter apply with respect to the carrying on of:

(1) *regulated activities*;

(2) activities that constitute *dealing in investments* as principal, disregarding the exclusion in article 15 of the *Regulated Activities Order* (Absence of holding out etc);

(3) *ancillary activities*;

(4) in relation to *MiFID or equivalent third country business*, *ancillary services*;

(5) *collective portfolio management*;

(6) the provision of *payment services* and the issuance of *electronic money*; and

(7) any other *unregulated activities*, but only in a *prudential context*.

15A.2 Operational resilience requirements

Important business services

15A.2.1 R A *firm* must identify its *important business services*.

15A.2.2 R A *firm* must keep its compliance with *SYSC* 15A.2.1R under review and, in particular, consider its compliance in the following circumstances:

(1) if there is a relevant change to the *firm*'s business or the market in which it operates; and

(2) in any event, no later than 1 year after it last carried out the relevant assessment.

15A.2.3 G In the course of identifying its *important business services* under *SYSC* 15A.2.1R, a *firm* should treat each distinct relevant service separately, and should not identify a collection of services as a single *important business service*.

15A.2.4 G The factors that a *firm* should consider when identifying its *important business services* include, but are not limited to:

(1) the nature of the *client* base, including vulnerable *client*s who are more susceptible to harm from a disruption;

(2) the ability of *client*s to obtain the service from other providers (substitutability, availability and accessibility);

(3) time criticality for *client*s receiving the service;

(4) the number of *clients* to whom the service is provided;

(5) sensitivity of data held;

(6) potential to inhibit the functioning of the *UK financial system*;

(7) the *firm*'s potential to impact the soundness, stability or resilience of the *UK financial system*;

(8) the possible impact on the *firm*'s financial position and potential to threaten the *firm*'s viability where this could harm the *firm*'s *client*s or pose a risk to the soundness, stability or resilience of the *UK financial system* or the orderly operation of the financial markets;

(9) potential to cause reputational damage to the *firm*, where this could harm the *firm*'s *client*s or pose a risk to the soundness, stability or resilience of the *UK financial system* or the orderly operation of the financial markets;

(10) whether disruption to the services could amount to a breach of a legal or regulatory obligation;

(11) the level of inherent conduct and *market risk*;

(12) potential to cause knock-on effects for other market participants, particularly those that provide financial market infrastructure or critical national infrastructure; and

(13) the importance of that service to the *UK financial system*, which may include market share, *client* concentration and sensitive *clients* (for example, governments or pension funds).

Impact tolerances

15A.2.5 R A *firm* must, for each of its *important business services*, set an *impact tolerance*.

15A.2.6 R A *firm* must keep its compliance with *SYSC* 15A.2.5R under review and, in particular, consider its compliance in the following circumstances:

(1) if there is a relevant change to the *firm*'s business or the market in which it operates; and

(2) in any event, no later than 1 year after it last carried out the relevant assessment.

15A.2.7 G The factors that a *firm* should consider when setting its *impact tolerance* include, but are not limited to:

(1) the number of *client*s that may be adversely impacted and the nature of impact;

(2) the potential financial loss to *client*s;

(3) the potential financial loss to the *firm* where this could harm the *firm*'s *client*s or pose a risk to the soundness, stability or resilience of the *UK financial system* or the orderly operation of the financial markets;

(4) the potential level of reputational damage to the *firm* where this could harm the *firm*'s *client*s or pose a risk to the soundness, stability or resilience of the *UK financial system* or the orderly operation of the financial markets;

(5) the potential impact on market or consumer confidence;

(6) potential spread of risks to their other business services, other *firms* or the *UK financial system*;

(7) the potential loss of functionality or access for *client*s; and

(8) any potential loss of confidentiality, integrity or availability of data.

15A.2.8 G When setting its *impact tolerance*, the *FCA* expects a *firm* to take account of the fluctuations in demand for its *important business service* at different times of the day and throughout the year in order to ensure that its *impact tolerance* reflects these fluctuations and is appropriate in light of the peak demand for the *important business service*.

15A.2.9 R A *firm* must ensure it can remain within its *impact tolerance* for each *important business service* in the event of a severe but plausible disruption to its operations.

15A.2.10 G While under *SYSC* 15A.2.9R a *firm* must ensure it is able to remain within its *impact tolerance*, it is not required to in fact remain within its *impact tolerance* where doing so would put the *firm* in breach of a regulatory obligation, conflict with the proper exercise of a discretion granted to it under any *rule* or regulation, or result in increased risk of harm to its *clients* or the soundness, stability or resilience of the *UK financial system* or the orderly operation of the financial markets.

15A.2.11 G Under *Principle* 11, the *FCA* expects to be notified of any failure by a *firm* to meet an *impact tolerance*.

15A.2.12 G When setting *impact tolerances* under *SYSC* 15A.2.5R a *payment services provider* should have regard to its obligations under the *EBA* Guidelines on ICT and security risk management.

15A.2.13 G *Payment service providers* should have regard to the *impact tolerance* set under *SYSC* 15A.2.5R when complying with the *EBA* Guidelines on ICT

and security risk management. In particular, they should, as part of their continuity planning and testing, consider their ability to remain within their *impact tolerance* through a range of severe but plausible disruption scenarios.

15A.3 Strategies, Processes and Systems

15A.3.1 R A *firm* must have in place sound, effective and comprehensive strategies, processes and systems to enable it to comply with its obligations under this chapter.

15A.3.2 R The processes, strategies and systems required under *SYSC* 15A.3.1R must be comprehensive and proportionate to the nature, scale and complexity of the *firm*'s activities.

15A.4 Mapping

15A.4.1 R A *firm* must identify and document the people, processes, technology, facilities and information necessary to deliver each of its *important business services*. This must be sufficient to allow the *firm* to identify vulnerabilities and remedy these as appropriate.

R A *firm* must keep its compliance with *SYSC* 15A.4.1R under review and, in particular, review its compliance in the following circumstances:

(1) if there is a material change to the *firm*'s business, the *important business services* identified in accordance with *SYSC* 15A.2.1R or *impact tolerances* set in accordance with *SYSC* 15A.2.5R; and

(2) in any event, no later than 1 year after it last carried out the relevant assessment.

15A.5 Scenario testing

Testing plan

15A.5.1 R A *firm* must develop and keep up to date a testing plan that appropriately details how it will gain assurance that it can remain within *the impact tolerances* for each of its *important business services*.

15A.5.2 G *Firms* should ensure that the testing plan takes account of a number of factors, including but not limited to:

(1) the type of scenario testing undertaken. For example, whether it is paper based, simulations or through the use of live-systems;

(2) the scenarios which the *firm* expects to be able to remain within their *impact tolerances* and which ones they may not;

(3) the frequency of the testing;

(4) the number of *important business services* tested;

(5) the availability and integrity of supporting assets;

(6) how the *firm* would communicate with internal and external stakeholders effectively to reduce the harm caused by operational disruptions.

Testing

15A.5.3 R A *firm* must carry out scenario testing of its ability to remain within its *impact tolerance* for each of its *important business services* in the event of a severe but plausible disruption of its operations.

15A.5.4 R In carrying out the scenario testing required by *SYSC* 15A.5.3R, 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 the delivery of the *firm*'s *important business services* in those circumstances.

15A.5.5 G In carrying out the scenario testing required by *SYSC* 15A.5.3R, a *firm* should, among other things, consider the following scenarios:

(1) corruption, deletion or manipulation of data critical to the delivery of its *important business services*;

(2) unavailability of facilities or key people;

(3) unavailability of third-party services, which are critical to the delivery of its *important business services*;

(4) disruption to other market participants, where applicable; and

(5) loss or reduced provision of technology underpinning the delivery of *important business services*.

15A.5.6 R A *firm* must carry out scenario testing under *SYSC* 15A.5.3R:

(1) if there is a material change to the *firm*'s business, the *important business services* identified in accordance with *SYSC* 15A.2.1R or *impact tolerances* set in accordance with *SYSC* 15A.2.5R;

(2) following any improvements made by the *firm* in response to a previous test; and

(3) in any event, no later than 1 year after it last carried out scenario testing.

Lessons learned

15A.5.7 R A *firm* must, following scenario testing or, in the event of an operational disruption, after such event, conduct a lessons learned exercise that

allows the *firm* to identify weaknesses and take action to improve its ability to effectively respond and recover from future disruptions.

15A.5.8 R Following the lessons learned exercise, a *firm* must make necessary improvements to address weaknesses identified to ensure that it can remain within its *impact tolerances* in accordance with *SYSC* 15A.2.9R.

15A.6 Self-assessment and lessons learned exercise documentation

15A.6.1 R A *firm* must make, and keep up to date, a written record of its assessment of its compliance with the requirements in this chapter, including, but not limited to, a written record of:

(1) *important business services* identified by the *firm* and the justification for the determination made;

(2) the *firm*'s *impact tolerances* and the justification for the level at which they have been set by the *firm*;

(3) the *firm*'s approach to mapping under *SYSC* 15A.4.1R, including how the *firm* has used mapping to:

(a) identify the people, processes, technology, facilities and information necessary to deliver each of its *important business services*;

(b) identify vulnerabilities;

(b) support scenario testing;

(4) the *firm*'s testing plan and a justification for the plan adopted;

(5) details of the scenario testing carried out as part of its obligations under *SYSC* 15A.5, including a description and justification of the assumptions made in relation to scenario design and any identified risks to the *firm*'s ability to meet its *impact tolerances*;

(6) any lessons learned exercise conducted under *SYSC* 15A.5.7R;

(7) an identification of the vulnerabilities that threaten the *firm*'s ability to deliver its *important business services* within the *impact tolerances* set, including the actions taken or planned and justifications for their completion time;

(8) its communication strategy under *SYSC* 15A.8.1R and an explanation of how it will enable it to reduce the anticipated harm caused by operational disruptions; and

(9) the methodologies used to undertake the above activities.

15A.6.2 R A *firm* must retain each version of the records referred to in *SYSC* 15A.6.1R for at least 6 years and, on request, provide these to the *FCA*.

15A.7 Governance

15A.7.1 R A *firm* must ensure that its *governing body* approves and regularly reviews the written records required under *SYSC* 15A.6 (Self-assessment and lessons learned exercise documentation).

15A.8 Communications

15A.8.1 R A *firm* must maintain an internal and external communication strategy to act quickly and effectively to reduce the anticipated harm caused by operational disruptions.

15A.8.2 G As part of a *firm*'s communications strategy, the *FCA* expects the *firm* to:

(1) consider, in advance of a disruption, how it would provide important warnings or advice quickly to consumers and other stakeholders, including where there is no direct line of communication.

(2) use effective communication to gather information about the cause, extent, and impact of operational incidents.

15A.8.3 R A *firm* must provide clear, timely and relevant communications to stakeholders in the event of an operational disruption.

15A.9 Supervisory review and feedback

15A.9.1 G The *FCA* may provide individual *guidance* as to whether a *firm*'s compliance with this chapter is adequate and, if necessary, require a *firm* to take the necessary actions or steps to address any failure to meet the requirements in this chapter.

15A.9.2 G A *firm* should have regard to the views provided by the *FCA* in relation to the *firm*'s compliance. If a *firm* considers that any individual *guidance* given to it is inappropriate to its circumstances it should, consistent with *Principle* 11 (Relations with regulators), inform the *FCA* that it disagrees with that *guidance*. The *FCA* may reissue the individual *guidance* if, after discussion with the *firm*, the *FCA* concludes that the appropriate actions or steps a *firm* should take is different from that initially suggested by the *FCA*.

15A.9.3 G If, after discussion, the *FCA* and a *firm* still do not agree, the *FCA* may consider other tools available to it, including its powers under sections 55J and 55L of the *Act* on its own initiative to require the *firm* to take specific steps in line with the *FCA's* view to comply with the requirements in this chapter.

Insert the following new transitional provision, SYSC TP 9, after SYSC TP 8 (Bank of England and Financial Services Act 2016: Application to claims management companies). The text is not underlined.

SYSC TP 9 Operational Resilience

(1)	(2) Material to which the transitional provision applies	(3)	(4) Transitional provision	(5) Transitional provision: dates in force	(6) Handbook provisions: dates in force
9.1	*SYSC* 15A.2.9	R	The provision in column (2) does not apply. However, a *firm* must ensure that, as soon as reasonably practicable after [the date the rules come into effect] can remain within its *impact tolerance* for each *important business service* in the event of a severe but plausible disruption to its operations.	From [the date the rules come into effect] to [3 years after the date the rules come into effect].	[the date the rules come into effect].

Annex C

Amendments to the Supervision manual (SUP)

In this Annex, underlining indicates new text.

16 Reporting requirements

…

16.13 Reporting under the Payment Services Regulations

…

16.13.17A	G	*SUP* 15A (Operational resilience) makes further provision which is relevant to a *payment service provider*'s Operational and Security Risk assessment.

Annex D

Amendments to the Recognised Investment Exchanges sourcebook (REC)

In this Annex, underlining indicates new text.

2.5 Systems and controls, algorithmic trading and conflicts

…

2.5.1 Schedule to the Recognition Requirements Regulations, paragraphs 3 – 3H

…

(1) The [*UK RIE*] must ensure that the systems and controls, including procedures and arrangements, used in the performance of its functions and the functions of the trading venues it operates are adequate, effective and appropriate for the scale and nature of its business.

[**Note:** *SYSC* 15A contains requirements relating to the operational resilience of *UK RIE*s]

…

Appendix 2
Draft Handbook text (Exiting the European Union)

OPERATIONAL RESILIENCE INSTRUMENT 2020

Powers exercised

A. The Financial Conduct Authority ("the FCA") makes this instrument in the exercise of the powers and related provisions in or under:

(1) the following sections of the Financial Services and Markets Act 2000 ("the Act"), including as applied by paragraph 3 of Schedule 6 to the Payment Services Regulations 2017 (SI 2017/752) ("the PSRs") and paragraph 2A of Schedule 3 to the Electronic Money Regulations 2011 ("SI 2011/99") ("the EMRs"):

(a) section 137A (The FCA's general rule-making power);
(b) section 138D (Actions for damages);
(c) section 137T (General supplementary powers);
(d) section 139A (Guidance);
(e) section 247 (Trust scheme rules);
(f) section 261I (Contractual scheme rules); and

(2) regulation 120 (Guidance) of the PSRs;

(3) regulation 60 (Guidance) of the EMRs;

(4) regulation 11 of the Financial Services and Markets Act 2000 (Recognition Requirements for Investment Exchanges and Clearing Houses) Regulations 2001 (SI 2001/995); and

(5) the other powers and related provisions listed in Schedule 4 (Powers exercised) to the General Provisions of the Handbook.

B. The rule-making provisions referred to above are specified for the purposes of section 138G(2) (Rule-making instruments) of the Act.

Commencement

C. This instrument comes into force on [*date*].

Amendments to the Handbook

D. The modules of the FCA's Handbook of rules and guidance listed in column (1) below are amended in accordance with the Annexes to this instrument listed in column (2) below:

(1)	(2)
Glossary of definitions	Annex A
Senior Management Arrangements, Systems and Controls sourcebook (SYSC)	Annex B

Supervision manual (SUP)	Annex C
Recognised Investment Exchanges sourcebook (REC)	Annex D

Citation

E. This instrument may be cited as the Operational Resilience Instrument 2020.

By order of the Board
[*date*]

Annex A

Amendments to the Glossary of definitions

Insert the following new definitions in the appropriate alphabetical position. The text is not underlined.

important business service	means a service provided by a *firm*, or by another *person* on behalf of the *firm*, to one or more *clients* of the *firm* which, if disrupted, could cause intolerable levels of: (1) harm to any one or more of the *firm*'s *clients*; or (2) risk to the soundness, stability or resilience of the *UK financial system* or the orderly operation of the financial markets.
impact tolerance	means the maximum tolerable level of disruption to an *important business service*, as measured by a length of time and other relevant metrics, reflecting the point at which any further disruption to the *important business service* could pose intolerable harm to any one or more of the *firm*'s *clients* or intolerable risk to the soundness, stability or resilience of the *UK financial system* or the orderly operation of the financial markets.

Annex B

Amendments to the Senior Management Arrangements, Systems and Controls sourcebook (SYSC)

In this Annex, underlining indicates new text, unless otherwise stated.

1 Application and purpose

1.1A Application

…

1.1A.1 G The application of this sourcebook is summarised at a high level in the following table. The detailed application is cut back in *SYSC* 1 Annex 1 and in the text of each chapter.

Type of firm	Applicable chapters
Insurer, *UK ISPV*	Chapters 2, 3, 12 to 18, 19F.2, 21, 22, 23, 24, 25, 26, 27, 28
Managing agent	Chapters 2, 3, 11, 12, 15A, 18, 19F.2, 21, 22, 23, 24, 25, 26, 27, 28
Society	Chapters 2, 3, 12, 15A, 18, 19F.2, 21, 22, 23, 24, 25, 26, 27, 28
Any other *SMCR firm*	Chapters 4 to 12, 15A, 18, 19D, 19F.2, 21, 22, 23, 24, 25, 26, 27, 28
Every other *firm*	Chapters 4 to 12, 15A, 18, 19D, 19F.2, 21, 22, 28

…

1.1A.1B G Chapter 15A of this sourcebook also applies to:

(1) an *electronic money institution*, a *payment institution* and a *registered account information service provider*;

(2) the provision of *payment services* and the issuing of *electronic money* (where the activity is not issuing electronic money specified in article 9B of the *Regulated Activities Order)*;

as set out in the text of that chapter.

…

1.4.2 R A contravention of a *rule* in *SYSC* 11 to *SYSC* 14, *SYSC* 18 to *SYSC* 21, *SYSC* 22.8.1R, *SYSC* 22.9.1R or *SYSC* 23 to *SYSC* 28 does not give rise to a right of action by a *private person* under section 138D of the *Act* (and each of those *rules* is specified under section 138D(3) of the *Act* as a provision giving rise to no such right of action).

Insert the following new chapter, SYSC 15A, after SYSC 14 (Risk management and associated systems and controls for insurers). The text is not underlined.

15A Operational resilience

15A.1 Application

Application

15A.1.1 R This chapter applies to:

(1) a *firm* that is:

(a) an *enhanced scope SMCR firm*;

(b) a *bank*;

(c) a *designated investment firm*;

(d) a *building society*;

(e) a *Solvency II firm*.

(2) a *UK RIE*.

(3) an *electronic money institution*, a *payment institution* or a *registered account information service provider*.

15A.1.2 R In this chapter, a reference to a *firm* includes a *UK RIE*, an *electronic money institution*, a *payment institution* and a *registered account information service provider*.

15A.1.3 R In this chapter, a reference to a *client* in relation to a *UK RIE* includes a *person* who is entitled, under an arrangement or agreement between them and that *UK RIE*, to use the *UK RIE*'s *facilities*.

15A.1.4 R In this chapter, a reference to a *client* in relation to a *firm* carrying on the activity of *managing a UK UCITS* or *managing an AIF* includes:

(1) a *Unitholder*;

(2) an investor in an *AIF*.

15A.1.5 R The requirements in this chapter apply with respect to the carrying on of:

(1) *regulated activities*;

(2) activities that constitute *dealing in investments* as principal, disregarding the exclusion in article 15 of the *Regulated Activities Order* (Absence of holding out etc);

(3) *ancillary activities*;

(4) in relation to *MiFID or equivalent third country business*, *ancillary services*;

(5) *collective portfolio management*;

(6) the provision of *payment services* and the issuance of *electronic money*; and

(7) any other *unregulated activities*, but only in a *prudential context*.

15A.2 Operational resilience requirements

Important business services

15A.2.1 R A *firm* must identify its *important business services*.

15A.2.2 R A *firm* must keep its compliance with *SYSC* 15A.2.1R under review and, in particular, consider its compliance in the following circumstances:

(1) if there is a relevant change to the *firm*'s business or the market in which it operates; and

(2) in any event, no later than 1 year after it last carried out the relevant assessment.

15A.2.3 G In the course of identifying its *important business services* under *SYSC* 15A.2.1R, a *firm* should treat each distinct relevant service separately, and should not identify a collection of services as a single *important business service*.

15A.2.4 G The factors that a *firm* should consider when identifying its *important business services* include, but are not limited to:

(1) the nature of the *client* base, including vulnerable *client*s who are more susceptible to harm from a disruption;

(2) the ability of *client*s to obtain the service from other providers (substitutability, availability and accessibility);

(3) time criticality for *client*s receiving the service;

(4) the number of *clients* to whom the service is provided;

(5) sensitivity of data held;

(6) potential to inhibit the functioning of the *UK financial system*;

(7) the *firm*'s potential to impact the soundness, stability or resilience of the *UK financial system*;

(8) the possible impact on the *firm*'s financial position and potential to threaten the *firm*'s viability where this could harm the *firm*'s *client*s or pose a risk to the soundness, stability or resilience of the *UK financial system* or the orderly operation of the financial markets;

(9) potential to cause reputational damage to the *firm*, where this could harm the *firm*'s *client*s or pose a risk to the soundness, stability or resilience of the *UK financial system* or the orderly operation of the financial markets;

(10) whether disruption to the services could amount to a breach of a legal or regulatory obligation;

(11) the level of inherent conduct and *market risk*;

(12) potential to cause knock-on effects for other market participants, particularly those that provide financial market infrastructure or critical national infrastructure; and

(13) the importance of that service to the *UK financial system*, which may include market share, *client* concentration and sensitive *client*s (for example, governments or pension funds).

Impact tolerances

15A.2.5 R A *firm* must, for each of its *important business services*, set an *impact tolerance*.

15A.2.6 R A *firm* must keep its compliance with *SYSC* 15A.2.5R under review and, in particular, consider its compliance in the following circumstances:

(1) if there is a relevant change to the *firm*'s business or the market in which it operates; and

(2) in any event, no later than 1 year after it last carried out the relevant assessment.

15A.2.7 G The factors that a *firm* should consider when setting its *impact tolerance* include, but are not limited to:

(1) the number of *client*s that may be adversely impacted and the nature of impact;

(2) the potential financial loss to *client*s;

(3) the potential financial loss to the *firm* where this could harm the *firm*'s *client*s or pose a risk to the soundness, stability or resilience of the *UK financial system* or the orderly operation of the financial markets;

(4) the potential level of reputational damage to the *firm* where this could harm the *firm*'s *client*s or pose a risk to the soundness, stability or resilience of the *UK financial system* or the orderly operation of the financial markets;

(5) the potential impact on market or consumer confidence;

(6) potential spread of risks to their other business services, other *firms* or the *UK financial system*;

(7) the potential loss of functionality or access for *client*s; and

(8) any potential loss of confidentiality, integrity or availability of data.

15A.2.8 G When setting its *impact tolerance*, the *FCA* expects a *firm* to take account of the fluctuations in demand for its *important business service* at different times of the day and throughout the year in order to ensure that its *impact tolerance* reflects these fluctuations and is appropriate in light of the peak demand for the *important business service*.

15A.2.9 R A *firm* must ensure it can remain within its *impact tolerance* for each *important business service* in the event of a severe but plausible disruption to its operations.

15A.2.10 G While under *SYSC* 15A.2.9R a *firm* must ensure it is able to remain within its *impact tolerance*, it is not required to in fact remain within its *impact tolerance* where doing so would put the *firm* in breach of a regulatory obligation, conflict with the proper exercise of a discretion granted to it under any *rule* or regulation, or result in increased risk of harm to its *clients* or the soundness, stability or resilience of the *UK financial system* or the orderly operation of the financial markets.

15A.2.11 G Under *Principle* 11, the *FCA* expects to be notified of any failure by a *firm* to meet an *impact tolerance*.

15A.2.12 G When setting *impact tolerances* under *SYSC* 15A.2.5R a *payment services provider* should have regard to its obligations under the *EBA* Guidelines on ICT and security risk management.

15A.2.13 G *Payment service providers* should have regard to the *impact tolerance* set under *SYSC* 15A.2.5R when complying with the *EBA* Guidelines on ICT and security risk management. In particular, they should, as part of their continuity planning and testing, consider their ability to remain within their *impact tolerance* through a range of severe but plausible disruption scenarios.

15A.3 Strategies, Processes and Systems

15A.3.1 R A *firm* must have in place sound, effective and comprehensive strategies, processes and systems to enable it to comply with its obligations under this chapter.

15A.3.2 R The processes, strategies and systems required under *SYSC* 15A.3.1R must be comprehensive and proportionate to the nature, scale and complexity of the *firm*'s activities.

15A.4 Mapping

15A.4.1 R A *firm* must identify and document the people, processes, technology, facilities and information necessary to deliver each of its *important business services*. This must be sufficient to allow the *firm* to identify vulnerabilities and remedy these as appropriate.

R A *firm* must keep its compliance with *SYSC* 15A.4.1R under review and, in particular, review its compliance in the following circumstances:

(1) if there is a material change to the *firm*'s business, the *important business services* identified in accordance with *SYSC* 15A.2.1R or *impact tolerances* set in accordance with *SYSC* 15A.2.5R; and

(2) in any event, no later than 1 year after it last carried out the relevant assessment.

15A.5 Scenario testing

Testing plan

15A.5.1 R A *firm* must develop and keep up to date a testing plan that appropriately details how it will gain assurance that it can remain within *the impact tolerances* for each of its *important business services*.

15A.5.2 G *Firms* should ensure that the testing plan takes account of a number of factors, including but not limited to:

(1) the type of scenario testing undertaken. For example, whether it is paper based, simulations or through the use of live-systems;

(2) the scenarios which the *firm* expects to be able to remain within their *impact tolerances* and which ones they may not;

(3) the frequency of the testing;

(4) the number of *important business services* tested;

(5) the availability and integrity of supporting assets;

(6) how the *firm* would communicate with internal and external stakeholders effectively to reduce the harm caused by operational disruptions.

Testing

15A.5.3 R A *firm* must carry out scenario testing of its ability to remain within its *impact tolerance* for each of its *important business services* in the event of a severe but plausible disruption of its operations.

15A.5.4 R In carrying out the scenario testing required by *SYSC* 15A.5.3R, 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 the delivery of the *firm*'s *important business services* in those circumstances.

15A.5.5 G In carrying out the scenario testing required by *SYSC* 15A.5.3R, a *firm* should, among other things, consider the following scenarios:

(1) corruption, deletion or manipulation of data critical to the delivery of its *important business services*;

(2) unavailability of facilities or key people;

(3) unavailability of third-party services, which are critical to the delivery of its *important business services*;

(4) disruption to other market participants, where applicable; and

(5) loss or reduced provision of technology underpinning the delivery of *important business services*.

15A.5.6 R A *firm* must carry out scenario testing under *SYSC* 15A.5.3R:

(1) if there is a material change to the *firm*'s business, the *important business services* identified in accordance with *SYSC* 15A.2.1R or *impact tolerances* set in accordance with *SYSC* 15A.2.5R;

(2) following any improvements made by the *firm* in response to a previous test; and

(3) in any event, no later than 1 year after it last carried out scenario testing.

Lessons learned

15A.5.7 R A *firm* must, following scenario testing or, in the event of an operational disruption, after such event, conduct a lessons learned exercise that allows the *firm* to identify weaknesses and take action to improve its ability to effectively respond and recover from future disruptions.

15A.5.8 R Following the lessons learned exercise, a *firm* must make necessary improvements to address weaknesses identified to ensure that it can remain within its *impact tolerances* in accordance with *SYSC* 15A.2.9R.

15A.6 Self-assessment and lessons learned exercise documentation

15A.6.1 R A *firm* must make, and keep up to date, a written record of its assessment of its compliance with the requirements in this chapter, including, but not limited to, a written record of:

(1) *important business services* identified by the *firm* and the justification for the determination made;

(2) the *firm*'s *impact tolerances* and the justification for the level at which they have been set by the *firm*;

(3) the *firm*'s approach to mapping under *SYSC* 15A.4.1R, including how the *firm* has used mapping to:

(a) identify the people, processes, technology, facilities and information necessary to deliver each of its *important business services*;

(b) identify vulnerabilities;

(b) support scenario testing;

(4) the *firm*'s testing plan and a justification for the plan adopted;

(5) details of the scenario testing carried out as part of its obligations under *SYSC* 15A.5, including a description and justification of the assumptions made in relation to scenario design and any identified risks to the *firm*'s ability to meet its *impact tolerances*;

(6) any lessons learned exercise conducted under *SYSC* 15A.5.7R;

(7) an identification of the vulnerabilities that threaten the *firm*'s ability to deliver its *important business services* within the *impact tolerances* set, including the actions taken or planned and justifications for their completion time;

(8) its communication strategy under *SYSC* 15A.8.1R and an explanation of how it will enable it to reduce the anticipated harm caused by operational disruptions; and

(9) the methodologies used to undertake the above activities.

15A.6.2 R A *firm* must retain each version of the records referred to in *SYSC* 15A.6.1R for at least 6 years and, on request, provide these to the *FCA*.

15A.7 Governance

15A.7.1 R A *firm* must ensure that its *governing body* approves and regularly reviews the written records required under *SYSC* 15A.6 (Self-assessment and lessons learned exercise documentation).

15A.8 Communications

15A.8.1 R A *firm* must maintain an internal and external communication strategy to act quickly and effectively to reduce the anticipated harm caused by operational disruptions.

15A.8.2 G As part of a *firm*'s communications strategy, the *FCA* expects the *firm* to:

(1) consider, in advance of a disruption, how it would provide important warnings or advice quickly to consumers and other stakeholders, including where there is no direct line of communication.

(2) use effective communication to gather information about the cause, extent, and impact of operational incidents.

15A.8.3 R A *firm* must provide clear, timely and relevant communications to stakeholders in the event of an operational disruption.

15A.9 Supervisory review and feedback

15A.9.1 G The *FCA* may provide individual *guidance* as to whether a *firm*'s compliance with this chapter is adequate and, if necessary, require a *firm* to take the necessary actions or steps to address any failure to meet the requirements in this chapter.

15A.9.2 G A *firm* should have regard to the views provided by the *FCA* in relation to the *firm*'s compliance. If a *firm* considers that any individual *guidance* given to it is inappropriate to its circumstances it should, consistent with *Principle* 11 (Relations with regulators), inform the *FCA* that it disagrees with that *guidance*. The *FCA* may reissue the individual *guidance* if, after discussion with the *firm*, the *FCA* concludes that the appropriate actions or steps a *firm* should take is different from that initially suggested by the *FCA*.

15A.9.3 G If, after discussion, the *FCA* and a *firm* still do not agree, the *FCA* may consider other tools available to it, including its powers under sections 55J and 55L of the *Act* on its own initiative to require the *firm* to take specific steps in line with the *FCA's* view to comply with the requirements in this chapter.

Insert the following new transitional provision, SYSC TP 9, after SYSC TP 8 (Bank of England and Financial Services Act 2016: Application to claims management companies). The text is not underlined.

SYSC TP 9 Operational Resilience

(1)	(2) Material to which the transitional provision applies	(3)	(4) Transitional provision	(5) Transitional provision: dates in force	(6) Handbook provisions: dates in force
9.1	*SYSC* 15A.2.9	R	The provision in column (2) does not apply. However, a *firm* must ensure that, as soon as reasonably practicable after [the date the rules come into effect] can remain within its *impact tolerance* for each *important business service* in the event of a severe but plausible disruption to its operations.	From [the date the rules come into effect] to [3 years after the date the rules come into effect].	[the date the rules come into effect].

Annex C

Amendments to the Supervision manual (SUP)

In this Annex, underlining indicates new text.

16 Reporting requirements

…

16.13 Reporting under the Payment Services Regulations

…

16.13.17A	G	*SUP* 15A (Operational resilience) makes further provision which is relevant to a *payment service provider*'s Operational and Security Risk assessment.

Annex D

Amendments to the Recognised Investment Exchanges sourcebook (REC)

In this Annex, underlining indicates new text.

2.5 Systems and controls, algorithmic trading and conflicts

…

2.5.1 Schedule to the Recognition Requirements Regulations, paragraphs 3 – 3H

…

(1) The [*UK RIE*] must ensure that the systems and controls, including procedures and arrangements, used in the performance of its functions and the functions of the trading venues it operates are adequate, effective and appropriate for the scale and nature of its business.

[**Note:** *SYSC* 15A contains requirements relating to the operational resilience of *UK RIE*s]

…

Pub ref: 006098

© Financial Conduct Authority 2019
12 Endeavour Square London E20 1JN
Telephone: +44 (0)20 7066 1000
Website: www.fca.org.uk
All rights reserved