FINANCIAL CONDUCT AUTHORITY

Building operational resilience: Feedback to CP19/32 and final rules

Policy Statement
PS21/3

March 2021

This relates to

Consultation Paper 19/32
which is available on our website at
www.fca.org.uk/publications

Email:
cp19-32@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

Contents

1 Summary 3
2 Important business services 9
3 Impact tolerances 16
4 Transitional arrangements 26
5 Mapping and scenario testing 28
6 Communications, governance and self-assessment and responses to our cost benefit analysis 38

Annex 1
List of non-confidential respondents 48

Annex 2
Examples of relevant existing FCA requirements 50

Annex 3
Abbreviations used in this paper 56

Appendix 1
Made rules (legal instrument)

1 Summary

Introduction

1.1 In December 2019, we consulted on proposed changes to how firms approach their operational resilience. Our proposals were set out in CP19/32, 'Building operational resilience: impact tolerances for important business services and feedback to DP18/04'.

1.2 These proposals were developed in partnership with the Bank of England – in its capacity of supervising financial market infrastructures (FMIs) – and the Prudential Regulation Authority (PRA) to improve the operational resilience of the UK financial sector.

1.3 Ensuring the UK financial sector is operationally resilient is important for consumers, firms and financial markets. It ensures firms and the sector can 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 risk to market integrity, threaten the viability of firms and cause instability in the financial system. The disruption caused by the coronavirus (Covid-19) pandemic has shown why it is critically important for firms to understand the services they provide and invest in their resilience.

1.4 This Policy Statement (PS) summarises the feedback we received to CP19/32 and our response, and sets out final rules.

Who this applies to

1.5 These changes will affect banks, building societies, designated investment firms, insurers, Recognised Investment Exchanges (RIEs), enhanced scope senior managers' and certification regime (SM&CR) firms and entities authorised or registered under the Payment Services Regulations 2017 (PSRs 2017) or the Electronic Money Regulations 2011 (EMRs 2011).

1.6 Firms not subject to these rules should continue to meet their existing obligations. These are set out in Annex 4 of the CP and Annex 2 of this PS. Firms may also want to consider the policy framework set out in this PS.

The wider context of this Policy Statement

Our consultation

1.7 Operational disruptions can have many causes including system failures, changes to systems, people or processes. Some disruptions may be caused by matters outside of a firm's control, such as the pandemic, that lead to the unavailability of access to infrastructure or key people.

1.8 In CP19/32 we set out changes designed to increase and enhance firms' operational resilience. We proposed to apply these changes proportionately to firms, reflecting the impact on consumers and market integrity if their services are disrupted. We also proposed an approach that is proportionate and flexible enough to accommodate the different business models of firms.

1.9 Where we refer to consumers in this PS, 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. We use the defined Glossary term 'client' in our rules, as amended in SYSC 15A.

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

1.11 Our proposed rules were not intended to conflict with or supersede existing requirements on firms to manage operational risk or business continuity planning, but rather to set new requirements that enhance firms' resilience.

1.12 In Chapter 8 of the CP, we set out firms' existing obligations in relation to third-party service provision and outsourcing. We did not propose new requirements in this area, but reminded firms of the importance of any existing requirements which apply to them. Firms may find our information on the relationship between outsourcing and existing requirements helpful.

Summary of feedback and our response

1.13 We received 73 responses to CP19/32. Most respondents supported our proposals. In some cases, respondents asked us to clarify how the rules would apply. In a small number of cases, respondents opposed our other proposals or suggested changes to the proposed rules.

1.14 We have made changes to the policy position in response to feedback to provide firms with more time and flexibility to meet mapping and scenario testing requirements. More detail can be found in Chapters 4 and 5 of this PS.

1.15 In general, we have implemented our other proposals as consulted on, and have made amendments to reflect the feedback received. Key themes of the feedback included:

- Respondents asked for more clarity around the level of granularity to which they'll be expected to go to comply with different elements of our proposals.

- Firms were keen to better understand how they should treat different consumer groups, particularly vulnerable consumers.
- There was strong support for closer alignment between the PRA and FCA's approach, and with other regulators internationally.
- Some respondents commented on the extent of time and effort firms needed to get ready for the new rules and to be consistently able to operate within their impact tolerances. An impact tolerance reflects the first point at which a disruption to an important business service would cause intolerable levels of harm to consumers or risk to market integrity.
- Some respondents asked us to illustrate how firms, different to those example firms included in the CP, might approach applying our proposals.

1.16 We have addressed this feedback by:

- clarifying how our rules fit with the broader domestic and international regulatory landscape and other FCA policy initiatives, such as the treatment of vulnerable consumers
- setting out how we will further support firms in implementing the rules
- including more varied examples of how different types of firm might apply our proposals, eg with the inclusion of new examples, as outlined below

1.17 Feedback and our responses are set out in more detail in Chapters 2 – 6.

Example firms

1.18 We use 3 fictional example firms throughout this PS to illustrate how some elements of our rules might apply to different types of firms. We acknowledge that in practice firms delivering business services would consider many other operational issues, dependencies, nuances in business models 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 an electronic money institution authorised under the EMRs 2011, with global operations, servicing more than 8m retail customers and 200k business customers, with core markets in the UK and European Economic Areas (EEA). It offers multiple payment products including electronic money 'e-wallet accounts' and pre-paid cards. The firm currently serves around 1m daily active users and processes around 3m transactions daily – for users based in the UK, this encompasses 20% of daily active users and 25% of daily transactions.

Firm B

Firm B is an enhanced scope SM&CR firm that provides insurance intermediary services. It sells insurance products offered by insurers to retail customers to help them meet their specific needs. In addition, certain insurers have outsourced claims handling to Firm B and it holds claims money to be paid to customers under risk transfer agreements. Firm B offers its services mainly via its online portal as well as via agents in their contact centres.

Firm C

Firm C is an enhanced scope SM&CR firm that provides asset management services. Firm C is at the centre of a complex ecosystem. On the customer side, the firm is connected with retail and institutional investors as well as the advisers; wealth managers; investment consultants; fund platforms; transfer agents; and messaging systems through which these customers transact with the firm. On the operational and markets side, the firm's dependencies include: data and risk modelling tool providers; order management and execution tools to create trade instructions; custodians which safeguard client assets; depositaries which oversee them; fund accountants which value the investment funds; brokers which execute instructions; clearing houses which clear transactions; banks; transaction reporting specialists to comply with its regulatory obligations; and markets.

Firm C is critically dependent on third parties for the delivery of its core services. Some of these third parties are regulated firms. Examples include the firms providing middle and back office processing; custody; fund accounting; and transfer agency. Many, though not all, of the technology tools and messaging systems relied on are from unregulated firms. Outsourcing oversight is one of Firm C's highest priorities.

Impact of coronavirus

1.19 We recognise that the coronavirus pandemic has had a significant impact on the firms we regulate. The disruption caused has shown why it is critically important for firms to understand the services they provide and invest in their resilience to protect themselves, their consumers and the market from disruption. Some respondents included in their feedback to the CP experiences of the pandemic and lessons learned for the future. Key themes included:

a. **The 'interconnectedness' of the financial sector** – respondents identified coronavirus as an example of a 'severe but plausible' scenario. The pandemic showed dependencies across firms/sectors and markets. It also highlighted the importance of co-ordinating approaches to operational resilience at an international level due to the global nature of the pandemic.
b. **Third-party providers and risks** – generally respondents had a positive experience with the scalability and security of services received from cloud providers, but the pandemic highlighted increasing dependence on third parties and outsourcing arrangements. For example, some firms experienced challenges with offshore third-party providers, particularly where providers were under lockdown in another geographical location, which affected continuity of service to UK consumers.
c. **People risks** – mass remote working brought with it a range of challenges to resilience, conduct, data protection and professional indemnity. Firms had to adapt their systems, processes and controls to address emerging people risks.

1.20 The feedback we have received on the impact of the pandemic has reinforced the importance of our policy proposals. Our proposal to require firms to map their important business services, by identifying and documenting the people, processes, technology, facilities and information that support them, provides a useful example of this. By focusing on mapping, firms have a clear picture of the resources that enable an important business service to function, and the impact if any of these are disrupted.

1.21 Staff play an essential role in delivering those services and firms need to understand which staff are pivotal to delivering an important business service, with contingency plans if those staff become incapacitated. We have found that firms that had mapped their important business services ahead of the pandemic found themselves in a much stronger position. For example, they could identify their key workers more quickly in line with government guidance, and activate continuity plans for mass home working and staff unavailability.

1.22 Overall, firms have been able to maintain continuity of service for consumers during the pandemic and we've seen a good degree of resilience. This follows co-ordinated response and action from industry, the Government and the FCA alongside the PRA and the Bank of England. Other severe disruptions are likely to have different characteristics and could be more firm-specific. Firms should progress the implementation of our policy proposals to help them improve existing, and embed new, standards of resilience.

Outcome we are seeking and measuring success

1.23 In implementing the policy, we want firms and the financial sector to better prevent, adapt, respond to, recover and learn from operational disruptions. Through improvements to firms' operational resilience, we expect harm to consumers and risk to market integrity caused through disruption to be minimised.

1.24 Through our ongoing supervisory work, we will assess the impact of the policy to ensure its introduction is driving the right resilience changes within firms and minimising harm. Longer term we would expect to see a positive change in the number/type of incidents reported.

How it links to our objectives

1.25 **Market integrity:** Ongoing availability of business services reduces risk to market integrity. Operational disruptions pose risks to the soundness, stability and resilience of the UK financial system and the orderly operation of financial markets. Our final policy 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.

1.26 **Effective competition:** Resilient firms can promote effective competition. 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.

1.27 **Consumer protection:** Ongoing availability of business services reduces consumer harm. In identifying their important business services, setting impact tolerances and restoring their important business services quickly after a disruption, firms can ensure consistent provision of important business services and supply of new business to consumers.

Equality and diversity considerations

1.28 In the CP, we stated how we didn't consider our proposals would adversely impact any of the groups with protected characteristics under the Equality Act 2010. We set out how our aim to strengthen the consideration given to vulnerable consumers during operational disruptions would have a positive impact on some groups with protected characteristics who also have characteristics of vulnerability.

1.29 Some respondents asked us to clarify how different elements of our proposals interact with vulnerable consumers, specifically:

- how to correctly determine vulnerability of consumers given the transience of both vulnerability and harm
- whether separate impact tolerances were needed for vulnerable consumers, and how this should affect communications plans to effectively reach vulnerable consumers

1.30 We have considered the equality and diversity issues that may arise from the final rules in this PS. We remain mindful of the impact that resilience issues can have on some groups with protected characteristics and vulnerable consumers, including the continuance of access to key financial services. Further detail is included in Chapters 3 and 6.

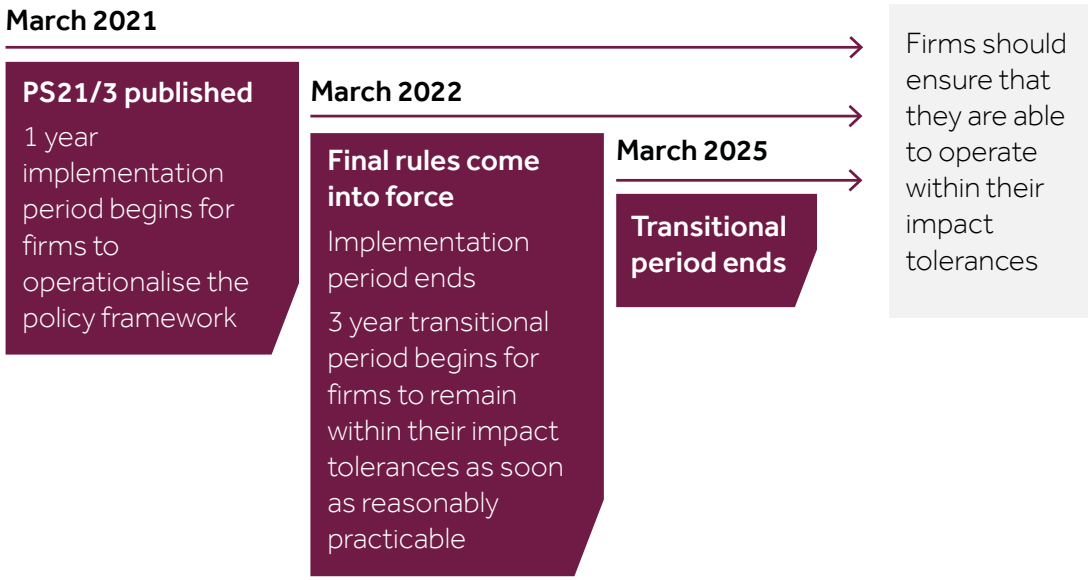
Next steps

1.31 The legal instrument accompanying this PS contains final rules and guidance. Our rules and guidance will come into force on 31 March 2022.

1.32 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 on 31 March 2022.

1.33 The implementation timeline is shown in Figure 1 below.

Figure 1



2 Important business services

2.1 In this chapter, we summarise the feedback received on our proposals for firms to identify their important business services and our responses.

CP proposals

2.2 We proposed that firms should identify their important business services. These are services which, if disrupted, could potentially cause intolerable harm to the consumers of the firm's services or risk to market integrity.

2.3 We proposed firms should identify their important business services at least once a year, or whenever there is a relevant change to their business or the market in which they operate.

2.4 We also proposed that important business services should be clearly identifiable as a separate service and not a collection of services. For example, accessing an online mortgage account and telephone mortgage banking are 2 separate services, while the provision of mortgages is a collection of services. The users of the important business service would also need to be clearly identifiable.

2.5 Finally, we included a list of factors for firms to consider when identifying their important business services. This was not an exhaustive list.

2.6 We asked 2 questions on important business services:

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?***

Feedback and responses

2.7 We received 62 responses to question 1 and 59 to question 2. While respondents were broadly in support of our proposals, they suggested areas where we should further clarify or refine the policy.

Process of identifying important business services

2.8 Some respondents commented on the process for identifying their important business service. Two respondents suggested that firms identify all their business services before going on to identify their important business services. Another respondent asked us to confirm the point at which they should consider new policyholders and when they would be at a greater risk of detriment than existing customers.

2.9 Some respondents provided feedback around when an internal service may be recognised as an important business service. This included payroll and treasury and liquidity management services, which if disrupted could affect the resilience of the business.

Our response

Identification of business services
We recognise that firms may find it helpful to identify all their business services before proceeding to identify which of these are 'important'. However, our rules only require firms to identify their important business services for the purposes of operational resilience.

Capturing internal processes
While internal processes (such as payroll) are important for maintaining a firm's operational resilience, they do not in of themselves constitute important business services. Instead, such processes which are necessary to the provision of important business services and should be captured by firms as part of their mapping exercises, where they identify and document the people, processes, technology, facilities and information that support their important business services.

Granularity and proportionality

2.10 Some respondents commented on the level of granularity they need to go to when defining their important business services. Some respondents felt that firms should have more flexibility in how, and to what granularity level, they define these services. One such respondent asked us to confirm if they should undertake a full detailed end-to-end analysis of a business service that is considered important or if they could instead document the processes that are key/critical to providing the service and those that are not and then focus on the key activities such as payment or settlement.

2.11 Additionally, 5 respondents requested more detail for smaller firms on how best to identify their important business services. One respondent also felt that the PRA and FCA consultations were inconsistent in how they presented granularity when identifying important business services.

2.12 Some respondents suggested it was harder to identify consumer harm in the wholesale sector, and highlighted that consumer harm is not relevant in global wholesale markets where professional and eligible counterparties come together.

2.13 Two respondents commented on the proportionality of our important business services proposals and, more specifically, how they should approach important business services where only a small number of customers would be adversely affected by disruption.

2.14 Two respondents asked if they would be able to review and update their important business services every 2 years, if there were no significant changes to their business/operations during that period. One other respondent asked us to clarify what constitutes a significant/material change.

Our response

Granularity and proportionality when identifying important business services

A common theme of the feedback was the level of granularity firms should go to when identifying their important business services. Our operational resilience framework is intended to provide firms with the flexibility to identify their important business services as appropriate in the context of their business.

Given feedback received to both the CP and earlier DP, we consider that firms are best placed to identify which of their services should be classed as important business services in the context of their business models. Firms can identify important business services in the way they consider most appropriate and effective, but ultimately must comply with our rules (SYSC 15A.2.1R–2R). We consider firms have the clearest understanding of the service disruption which would cause intolerable levels of harm to consumers or risk to market integrity.

We have included additional and varied firm examples in this PS, along with Handbook guidance, to help firms in identifying their important business services.

Definition of important business services

We have reviewed the drafting of our proposed Handbook Glossary term 'important business service' and have made a small change to clarify the drafting to confirm that the definition only refers to 'intolerable levels of harm' to consumers and not to 'intolerable levels of risk' to market integrity. The change ensures our definition aligns with that of the Bank and the PRA. The revised definition for an 'important business service is:

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:

1. cause intolerable levels of harm to one or more of the firm's clients; or
2. pose a risk to the soundness, stability or resilience of the UK financial system or the orderly operation of financial markets.

Services where only a small number of consumers would be affected by disruption

In identifying their important business services firms should consider both the size and nature of the consumer base. It is reasonable to expect that in some cases only a small number of customers would be affected by disruption but having considered all other factors the firm still considers the service to be important. Firms are encouraged to identify their important business services holistically, considering them in the broader context of size, complexity and focus on achieving operationally resilient outcomes.

Reviewing important business services

Firms should, from 31 March 2021, begin identifying their important business services. Firms will need to have completed this exercise before the rules take effect, on 31 March 2022. After 31 March 2022, firms will

then need to review their important business services at least once per year, or whenever there is a material change to their business or the market in which they operate. We consider it necessary for firms to review their important business services at least once per year to ensure that no emerging vulnerabilities are overlooked. Firms do not need to undertake the whole exercise once a year. We are only requiring that they review their existing identification against changes to their business or operating market over the course of the year. Where there have been no material changes, we would expect this to be straightforward.

Material changes
We consider a 'material change', which would require a firm to review their important business services, to include:

- the firm beginning to carry out a new activity/ceasing to provide an existing activity, or
- the firm outsourcing a new/existing service to a third-party service provider, or
- changes to an existing service in terms of scale or potential impact (considering the factors set out in paragraph 4.21 of the CP, number of customers or substitutability of the service, for example)

Firms may wish to review other changes, that are not considered material, in line with the review of their self-assessment documentation.

Central shared services for groups and collections of services

2.15 Respondents were broadly supportive of our proposal not to publish a prescriptive taxonomy for firms to use when identifying their important business services. But several respondents asked us to clarify how group shared services should be viewed in terms of identifying important business services.

2.16 Some respondents asked us to clarify the distinction between a separate service and a collection of services.

2.17 Several respondents asked us to further clarify the taxonomy between collection of services, business service and process, and how they interact with critical functions and other existing taxonomies.

Our response

Central shared services
We have considered the feedback about central shared services within groups being defined as important business services. We have identified the following examples of central shared services:

- architecture and underlying technology provided centrally
- operational processes, such as transactions booking or risk management
- audit and other 2nd line functions
- IT services

We consider that such services are unlikely to constitute important business services. These enable the provision of an important business service and should be identified by firms when they carry out their mapping exercises. Services can only be identified as important business services where they are provided by a firm, or by another person on behalf of the firm, to one or more consumers.

2.18 For further information on important business services and critical functions please see the PRA's Policy Statement.

Interaction with existing/proposed frameworks

2.19 Some respondents commented on the interaction between FCA-defined terms, such as the Glossary definition of 'important business service' and other definitions such as 'critical operations' and 'critical business service' featured in the consultation published by the Basel Committee on Banking Supervision (BCBS) and the European Banking Authority (EBA) Guidelines. The respondents called for global regulatory alignment through a common lexicon of terms. A respondent also commented on the differences between the FCA's definition of 'important business service' and that of the PRA.

2.20 Two respondents asked us to consider the link between our important business service proposals and existing related legislation, such as the Payment Services Directive 2 (PSD 2) and Operational Continuity in Resolution (OCIR).

2.21 We proposed that users of the service should be identifiable so that the impacts of disruption (through process, cyber security or technology failures) are clear. Two respondents queried how this interacts with existing General Data Protection Regulation (GDPR) and Data Protection Act (DPA) requirements. More specifically, 1 respondent asked whether regulated entities within scope were required to contact individuals affected by service disruption or whether it was acceptable to have systems in place to notify such individuals automatically (eg through email notifications). This respondent added that it may be difficult to access information with which to contact individuals given this may be encrypted.

Our response

Links to existing requirements

As with the CP, we have considered in detail the interaction of our final rules with existing requirements and recent regulatory developments (see Annex 2). This includes the recent consultations published by the BCBS and the European Commission (EC) and international approaches (CPMI-IOSCO guidance; G7, FSB and IOSCO membership), with the objective to achieve greater consistency in global standards/mitigate the risk of divergence, through work in key global Standard Setting Bodies (SSBs).

A key driver for us in introducing a high-level, principles-based framework is to provide sufficient flexibility for firms to take account of all aspects of their approach to resilience. This includes those arising from other regulatory requirements through the lens of providing important business services to customers. We believe this delivers on our objectives in the context of the firms we regulate in the UK market.

'Identifiable' service users
Where we proposed that service users be 'identifiable', we intended that firms should be able to recognise which of their consumer base use a certain important business service. This does not require the firm to identify individual consumers by name, or change existing requirements for the handling of customer data. The final rules proceed with that intention.

Scope of the proposals

2.22 One respondent asked that we clarify the services to which a firm authorised or registered under the PSRs 17 or EMRs 2011 ('payments firms') would need to apply the policy. More specifically, the respondent felt a change was needed to clarify our expectations for firms who would be outside the scope of the policy, but for their PSRs 2017 or EMRs 2011 permission. The respondent stated that only those services operated under the PSRs 2017 should be in scope for consideration as important business services and subject to the requirements. It also asked us to clarify whether certain other regulated activities should or should not be identified as important services in the context of the proposals and the provider's SM&CR status.

2.23 One respondent considered that the proposals could go further in establishing service failure criteria. The respondent stated that it is crucial for firms to understand where a service is degraded to the point of failure (failover) but still operating. The respondent suggested that, given the interconnectedness between critical services, it is not just outage, but also service degradation thresholds, which are relevant.

2.24 Another respondent suggested that we may want to include products, in addition to services, as important business services. The respondent suggested that we could provide further guidance on services that are essentially comprised of multiple products and whether these products constitute important business services.

Our response

Payments and e-money firms in scope
We have considered the feedback in relation to payments and e-money firms and the services in scope of the proposals. Our proposals apply to payments firms, to all firms and entities authorised or registered under the PSRs 2017 or EMRs 2011. However, there are some payments firms which also have permissions to carry on FSMA regulated activities which would not be in scope of this policy based on these activities considered on a standalone basis. Where this is the case, payments firms only have to apply our operational resilience proposals to their payments and/or e-money activities.

To clarify this, we have amended SYSC 15A.1 (Application).

Service failure criteria
We acknowledge the feedback asking us to develop criteria in respect of service failure. We agree that there will be circumstances where a service is degraded but still operating. Chapter 3 on impact tolerances addresses this feedback in more detail.

Products
We consider it unnecessary to bring products into scope of the proposals. Most products are supported by, and offered because of, important business services. For example, a fixed-rate mortgage product provided by a retail bank would likely be underpinned by one or multiple important business services (customer access to online mortgage calculators and telephone provision of mortgage advice, for example). If the supporting service is captured as an important business service then there is no additional merit in separately identifying relevant products.

How our example firms might identify important business services

Firm A

Firm A identifies the provision of its multi-currency e-wallet account from which users can initiate electronic payment transactions as 1 of its important business services for the purposes of operational resilience. Users access their e-wallet account through the firm's proprietary Apple and Android mobile apps. Access is via App only, there is no web-browser option.

Firm A considers that loss of access to the e-wallet accounts can cause significant harm to its users, many of which are consumers, as that is the primary channel through which they manage payment transactions and interact with the firm.

Firm B

Firm B identifies claims handling for its customers as one of its important business services for the purposes of operational resilience.

Firm B considers that disruption to the claims handling process could cause intolerable harm to consumers. For example, if consumers are unable to notify Firm B of their claim, submit a claim and/or and receive a claims payout/benefit under the policy.

Firm C

Firm C identifies generating orders to meet client subscription and redemption requests as an important business service. The firm uses an order management system (OMS) to provide the service. The OMS is central to the firm's portfolio management activity as it is essential for generating orders and to adjust the portfolio so that it delivers the objectives of the mandates and funds for which the firm is responsible. Disruption to the OMS could cause operational challenges within hours. These may affect both the firm's customers and, potentially, the markets in which the firm operates.

Customer harm could include investors being unable to buy or redeem units in funds or their investments suffering from lower performance because of fund transactions being delayed or incorrect. Outage has the potential to lead to market harm to the extent that some of a firm's market abuse controls are embedded in the system. Both the firm's reputation and customer confidence could also suffer.

3 Impact tolerances

3.1 In this chapter, we summarise the feedback received on our proposals for firms to set impact tolerances for each important business service and our response.

CP proposals

3.2 We proposed 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 risk to market integrity. We provided further guidance on relevant considerations to help firms in making this judgement. We also proposed firms should set and review their impact tolerances at least once per year or if there is a relevant change to the firm's business or the market in which it operates.

3.3 We proposed that firms should use metrics, including a mandatory metric of time/duration, to measure their impact tolerances.

3.4 The FCA and PRA set out proposals for how dual-regulated firms should approach impact tolerances. We proposed firms would need to set 1 impact tolerance at the first point at which there is an intolerable level of harm to consumers or risk to market integrity for our purposes. And under the PRA's rules, another separate tolerance at the first point at which financial stability is put at risk or a firm's safety and soundness or, in the case of insurers, where policyholder protection is affected.

3.5 In the CP, we asked 3 questions on impact tolerances:

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?***

Feedback and responses

3.6 We received 64 responses to question 3, 53 responses to question 4 and 52 responses to question 5. Respondents were broadly in support of our proposals but asked for clarification and refinement in some areas. Any consequential amendments to the policy are set out in our response.

Implementation challenges

3.7 Some respondents suggested how we could clarify certain aspects of our proposals to make implementation more straightforward. Respondents suggested we could:

- benchmark tolerances across the sector and provide more sector-specific support
- align the factors for consideration across those 'important business services' and 'impact tolerances'
- review and clarify the differences between our proposals to set impact tolerances and Business Impact Analysis
- clarify what we mean by 'intolerable harm'

3.8 In addition, 1 respondent considered that setting impact tolerances at the point at which 'intolerable harm' would be caused to consumers/market integrity was too late. The respondent considered that impact tolerances should be set before this point is reached to enable preventative measures to be taken.

Our response

As with other areas of the policy, we consider firms are best placed to set their impact tolerances at the appropriate level. Firms should use the considerations we have provided to help inform their judgements when setting impact tolerances. This flexible and proportionate approach is important given the wide range of firms from different sectors and with varying customer bases which are in scope. So we are proceeding with our proposals largely as consulted on, with some minor changes and clarifications based on the feedback received. These are set out below.

We consider that requiring firms to set their impact tolerances at the point at which disruption would cause intolerable harm to consumers or risk to market integrity remains appropriate. Setting impact tolerances at this point does not hinder firms from taking appropriate steps to prevent disruption. Moreover, it aims to ensure that firms build sufficient resilience before they reach their impact tolerance. We expect that firms manage their business to ensure they can operate within tolerance at all times including during severe but plausible scenarios. Firms should still be mindful of existing requirements which focus on preventative measures.

Intolerable harm

We didn't propose to define 'intolerable harm' as we consider what this constitutes will vary from firm-to-firm and across sectors. To identify intolerable harm, firms should have regard to various factors, some of which we set out in the CP. These were:

- 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

Additionally, we would advise firms that intolerable harm constitutes harm from which consumers cannot easily recover. This could be, for example, where a firm is unable to put a client back into a correct financial position, post-disruption, or where there have been serious non-financial impacts that cannot be effectively remedied. Intolerable harm is much more severe than inconvenience or harm. For both 'harm' and 'inconvenience' we would expect firms to be able to remediate any disruption so that no ill effects would be felt in the medium-/long-term by clients/markets.

Approach to vulnerable consumers

3.9 Five respondents had comments on how our proposals for impact tolerances interact with the needs of vulnerable consumers. More specifically, respondents asked us to clarify how impact tolerances should be set given consumer vulnerability and harm can be transient, and whether specific metrics could be used for vulnerable consumer sub-groups.

Our response

Vulnerable consumers

We have carefully considered how our proposal for firms to set impact tolerances interacts with the needs of, and considerations for, vulnerable consumers. Firms should consult our finalised guidance on the fair treatment of vulnerable customers.

More specifically for vulnerable consumers and impact tolerances, in the CP we emphasised that when identifying important business services, firms should consider their vulnerable consumers (see SYSC 15A.2.4G(1)). The concepts of first identifying important business services and then setting impact tolerances for each of these are inextricably linked. Consideration of the needs of vulnerable consumers is central to a firm's setting of an impact tolerance, and firms should consider these groups when considering how much disruption could be tolerated. Firms should also construct communications and alternative mechanisms to minimise harms arising for vulnerable consumers in the event of disruptions.

Given this, we do not consider it necessary for firms to set specific impact tolerances for vulnerable consumers as these should already be considered through the process of identifying important business services and setting impact tolerances. We have, however, amended SYSC 15A.2.7G to also make express reference to 'vulnerable consumers' in the guidance on factors to consider when setting impact tolerances.

Group approach to impact tolerances

3.10 One respondent asked us to clarify how competing impact tolerances set at group level and across different legal entities should be treated.

Our response

Impact tolerances at group and entity level

In situations where an entity sets an impact tolerance at a lower level than that set by the group, the group's Board should consider and approve that the entity can, and it is appropriate for it to, work towards that lower tolerance. The Board should also ensure that the entity has appropriate resources to meet its identified tolerance. More information can be found in the PRA's final policy documents.

Circumstances outside a firm's control

3.11 Four respondents asked us to clarify how we view circumstances outside of a firm's control in the context of remaining within impact tolerances. Two other respondents asked for further information on the circumstances in which it would be acceptable for a firm to deliberately not remain within its impact tolerances (for example, if doing so would further spread a computer virus).

Our response

Scenario testing as a tool to remain within tolerances

Our policy covers disruptions inside and outside of a firm's control. To prepare for such disruptions, firms need to test their impact tolerances in a range of severe but plausible scenarios. This approach will give firms a clear idea when they initially test their impact tolerances of where such unexpected events may mean they cannot remain within tolerance.

In the CP (paragraph 2.4), we gave examples of disruptions outside of a firm's control (for example, cyber-attacks and wider telecommunications/ power failures). We remind firms that operational resilience assumes that disruption is inevitable. While some situations cannot be predicted, and so will be outside of firms' severe but plausible testing scenarios, we encourage firms to approach such situations pragmatically.

If a firm has put in place procedures to improve its operational resilience and tested in a variety of severe but plausible scenarios it should be able to effectively translate that effort in the event of an unpredictable disruption. Firms should view testing in a range of severe but plausible scenarios as an effective planning tool to ensure services can remain within tolerance. However, if despite extensive scenario testing a firm finds itself not able to remain within impact tolerance for any reason, it should report the issue to the FCA in line with SYSC 15A.2.11G.

Circumstances where remaining within tolerance could cause further detriment

We know there may be some instances where a firm cannot remain within impact tolerances because doing so would cause further

detriment. For example, where resuming service could spread a computer virus. If a firm resumes a compromised service in such a case this does not constitute remaining within tolerance and neither does it show increased resilience, which is a key outcome we are seeking.

In line with the above, firms should consider such circumstances in their testing plans and report any issue with remaining in tolerance to the FCA in line with SYSC 15A.2.11G. There may be some occasions where a firm wishes to resume a degraded service. This is acceptable so long as the firm has assessed whether (a) the degraded service can safely resume without causing further detriment and (b) the benefits of resuming a degraded service outweigh the negatives of keeping the service unavailable until the issues have been remediated/the service is able to be fully restored to pre-disruption levels.

Multiple service disruptions

3.12 Some respondents asked us to clarify how firms should approach impact tolerances in the event of multiple disruptions to an important business service over a short time period and when multiple important business services are disrupted simultaneously. The respondents considered that such disruption could have a greater, and often faster, impact in aggregate and cause harm after a shorter duration.

Our response

Multiple disruptions to an important business service
In the CP, we focused on the disruption of single important business service.

We recognise there will be some occasions where a service could be affected by multiple disruptions over a short period of time. However, firms should continue to set their impact tolerances with reference to a single disruption rather than an aggregation of a number of disruptions. This is important for firms in maintaining an impact tolerance as an accurate metric for maximum tolerable disruption.

Aggregate harm when multiple business services are disrupted
When identifying their important business services and carrying out the mapping exercise (see Chapter 5 for more detail), firms should consider the lack of substitutability of a service and recognise where multiple business services rely on the same underlying system. In these cases, for substitute services which rely on the same systems, processes or people, firms should not assume, as part of their testing plans, that these services won't be affected in the event of disruption.

We agree that the simultaneous disruption of multiple important business services could mean that aggregate harm is felt more quickly and severely (for example, if telephone banking customer authentication went down at the same time as online banking and access to cash). We consider there are 2 situations in which such disruption is likely:

- Where multiple important business services rely on 1 common operational asset (such as key people or process), the disruption

of which could cause disruption to all reliant important business services. Such reliance would be captured in a firm's mapping exercise and be factored into testing plans.
- Where multiple important business services could be disrupted simultaneously due to an external factor directly affecting the service. For example, this could be due to a cyber-attack which hits a wide range of operational assets.

Firms should take steps to stay within set impact tolerances in both situations. Firms do not need to set separate tolerances to address the disruption of multiple services but should consider when setting their tolerances how aggregate impact may build in these situations and in turn, how aggregate impact could affect intolerable harm.

Cross-regulatory alignment

3.13 Four respondents commented on the differences in the FCA and PRA's respective definitions of 'impact tolerance'.

Our response

Amendments to our 'impact tolerance' definition

We have removed the reference to 'intolerable levels of risk' to instead refer to 'risk'. This aligns with the PRA's proposed approach. The PRA has also made a small amendment to its definition to refer to 'maximum tolerable level of disruption' (as opposed to 'maximum acceptable level of disruption') to mirror the drafting in our definition. We consider any other differences in the definitions necessary to accurately reflect our respective statutory objectives.

Outsourced services and impact tolerances

3.14 Five respondents asked for further guidance on how impact tolerances should be managed by firms outsourcing important business services to third parties.

Our response

Third parties providing important business services

When a firm is using a third-party provider in the provision of important business services, it should work effectively with that provider to set and remain within impact tolerances. Ultimately, the requirements to set and remain within impact tolerances remain the responsibility of the firm, regardless of whether it uses external parties for the provision of important business services.

Measuring impact tolerances

3.15 Most respondents agreed that time/duration should always be used as a mandatory metric when measuring impact tolerances. Respondents also appreciated the flexibility we provided in allowing firms to use other metrics in addition to time to measure impact tolerances.

3.16 A small number of respondents considered that firms should have greater autonomy when it comes to metrics, preferring that time/duration not be mandated. Some respondents suggested metrics firms may wish to use. These included:

- cost
- scale
- key business process
- potential value of market impact
- materiality (ie business/customer impact)
- volumes (eg data volume, transaction/account volume)
- type of transaction
- number of customers affected, and the nature of the consumer base

3.17 We also received some comments on how firms could use more than one metric to most effectively measure impact tolerance. One respondent considered that there may be occasions where time may not be the most effective metric.

Our response

Measuring impact tolerances
Based on the feedback received, we are proceeding as consulted to require that firms use time/duration as a mandatory metric to measure their impact tolerances. Using time/duration as a mandatory metric will ensure that firms plan for time-critical threats where there could be limited time to react to disruption before intolerable harm or risk to market integrity is caused. Additionally, the use of time as a common metric provides a clear standard, and enables comparison between firms.

To clarify, the time-based metric can be flexible and used in conjunction with other metrics. The impact tolerance should specify that an important business service should not be disrupted beyond a certain period of or point in time. As an example, this could be a number of hours/days or a point in time, such as the end of the day, in conjunction with, for example, a certain level of customer complaints.

Using a combination of metrics may be more appropriate for some important business services, eg where a service could run at a percentage capacity of its full capability for a certain period (time) before causing intolerable harm to consumers or risk to market integrity.

Examples of other metrics
We agree with respondents' suggestions, set out at paragraph 3.16 above, as to other metrics that may be used in addition to a time/duration-based metric. Firms are best placed to determine which metrics best measure impact tolerances for their important business services.

Dual-regulated firms' approach to impact tolerances

3.18 Most respondents agreed with our proposal for dual-regulated firms to set and manage to 'up to' 2 impact tolerances (1 for each regulator's objectives).

3.19 However, 2 respondents felt that mandating a set number of tolerances was too prescriptive. These respondents considered that firms should have flexibility to set as many impact tolerances as they wish. Four respondents also asked us to clarify our expectations around how dual-regulated firms should manage, in practice, 2 tolerances when they could vary in line with each regulator's objectives.

3.20 Some respondents also had comments on how smaller dual-regulated firms may find it more difficult to implement our proposals. More specifically, one respondent emphasised that, for smaller dual-regulated firms, important business services may be less likely to have a material impact on financial markets. Consequently, such firms may find it harder to differentiate between the respective regulatory (FCA/PRA) tolerances.

Our response

Up to 2 impact tolerances for dual-regulated firms

For dual-regulated firms, we maintain the position that these firms should set up to 2 impact tolerances. This is to ensure that firms consider their impact tolerances in line with the statutory objectives of each authority. Taking this focused approach ensures better outcomes for consumers and market integrity. Our expectation is that, while firms need to set tolerances for each important business service by reference to that authority's operational resilience rules, such firms will effectively manage the tolerances together.

Firms may set their separate impact tolerances at the same point if they deem it suitable for the purposes of each authority but will need to be able to justify this decision if challenged.

We understand that in practice dual-regulated firms may concentrate their efforts in ensuring they can remain within the more stringent tolerance. So it will be acceptable for a firm to show it can remain within the more stringent tolerance if it can demonstrate:

- how it has considered each of the FCA's and PRA's objectives when setting impact tolerances
- how its recovery and response arrangements are also appropriate for the longer tolerance (ie recovery and response arrangements must be viable for both shorter and longer time periods)
- that scenario testing has been performed with the longer tolerance in mind as a short tolerance might constrain the range of severe but plausible events a firm might consider

While we are requiring dual-regulated firms to set up to 2 clearly stated impact tolerances, if they find it beneficial to set additional sub-tolerances they can do so. Both the FCA and PRA will work collaboratively to ensure we supervise against tolerances efficiently.

Smaller firms' approach to impact tolerances

To address the feedback on how small firms may find it challenging to set impact tolerances for financial stability, the PRA is narrowing the scope of its rules so that smaller firms will not need to consider financial stability when setting impact tolerances. Thresholds will be set to clarify those firms that fall within the scope. For more detail please see the PRA's final policy documents.

How our example firms might set impact tolerances

Firm A

To set an impact tolerance relevant to its important business service of the provision of multi-currency e-wallet accounts from which users can initiate electronic payment transactions, Firm A considers the potential harm in the event of loss of its mobile app platform functionality. It identifies that consumer harm is the most relevant harm given the number of consumers affected and their reliance on the service for bill payments.

Firm A quantifies the proportion of daily active users of its platform including the average volume of transactions and determines that there are a sizable number of consumers who may rely solely on its service to manage their finances (including to make bill payments) and are therefore susceptible to greater detriment.

Firm A also considers substitutability from the users' perspectives and concludes that the unavailability of its e-wallet account will be particularly detrimental to users whose e-wallet accounts do not have card or ATM functionality, thereby leaving users with no alternative way to access their funds.

Using a time-sensitive metric, Firm A concludes that the appropriate impact tolerance is 2 hours to reflect the maximum disruption before there is an intolerable risk of consumer harm.

Firm B

Firm B has identified that disruption to its claims handling process for motor insurance could lead to potential consumer harm. For example, consumers being unable to obtain a courtesy car in a timely manner which could cause further disruptions in their lives.

Firm B expects that consumers may want to notify them of a claim as soon as possible in order to progress their claim and obtain peace of mind. It further recognises that customers with courtesy car cover are likely to be seeking the courtesy vehicle soon after the accident. So, Firm B considers the maximum tolerable period for disruption to both their online portal and contact centre should be set at 2 days. Firm B considers it is important to have both channels available as some consumers may not have access to one channel or have preferences to use one channel over another.

Firm C

Firm C recognises that the order management system (OMS), which is fundamental to the provision of the firm's important business service of generating orders to meet client subscription and redemption requests, does not exist in isolation. Failures in other business services such as market data flows or visibility of subscription & redemption activity may mean the OMS is not fully reliable or usable for a period, in turn causing harm to consumers and risk to market integrity.

Firm C considers potential disruption to its important business service of generating orders to meet client subscription and redemption requests and cannot identify one overall tolerance. However, Firm C recognises the impact that disruption of the OMS could have on other processes/services, for which it already has tolerances in place. For example, failures in investment processes can lead to an incorrect or late order being sent to the Central Dealing Desk or failure in dealing processes leading to an incorrect or late trade being placed in the market leading to client detriment and financial loss to the firm. The firm has a defined tolerance threshold of £30m to pay-out on trade errors. This could be increased by taking into other factors such as market volatility or other plausible scenarios.

4 Transitional arrangements

4.1 In this chapter, we summarise the feedback received on our transitional proposals for firms to embed and meet the requirements, along with our response.

4.2 In the CP, we asked 1 question on the proposed transitional period:

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

CP proposals

4.3 We proposed that firms would have a year implementation period after the publication of the final rules and guidance until the rules take effect. Firms would then, as soon as reasonably practicable and no later than 3 years, need to show that they can remain within their impact tolerances.

4.4 Our expectation was that firms would use the first year, before the rules take effect, to implement all aspects of the policy, except being able to stay within their impact tolerances at all times. This may require further change and investment within the 3-year transition period to achieve, but should be completed as soon as possible.

Feedback and responses

4.5 We received 52 responses to our question on proposed transitional arrangements. Seventeen respondents agreed with the proposed timeframe. One respondent considered that the 3-year transitional period was too long and may not provide appropriate incentive for firms to change. All other respondents considered that the timeframe should either be extended, or should factor in contingency for certain circumstances where firms may find it challenging to implement the policy within the specified period.

Our response

Changes to the timeframe for mapping and scenario testing

In response to the feedback received, we have concluded it would be appropriate to give firms more time and flexibility around how they perform mapping and scenario testing.

During the implementation period which runs to 31 March 2022, firms will only need to carry out mapping and scenario testing to a level of sophistication necessary to accurately identify their important business services, set impact tolerances and identify any vulnerabilities in their operational resilience. By level of sophistication, we mean the breadth and level of detail sufficient to achieve the policy outcomes of appropriately identifying important business services, setting impact tolerances and identifying vulnerabilities. Firms will not need to have performed scenario testing of every important business service by this date. We would also expect the level of sophistication of mapping and testing to increase over time.

We are not changing the requirement for firms to be able to stay consistently within impact tolerances by 31 March 2025. Given the importance of mapping and testing to identifying and addressing vulnerabilities to service provision,

firms will need to complete this in good time ahead of the end of the transitional period to be able to make the investments and other changes necessary to be able to stay within tolerances.

Retaining the 3-year transitional period

While we recognise some firms' desire for more time, we must balance the need to give firms time to implement the policy with achieving the benefits of improved resilience for consumers and markets.

Firms will have the significant period of 4 years from the date this PS publishes to be able to stay within their impact tolerances, made up of a 1-year implementation period and a 3-year transitional period. We note that one respondent argued this time period be reduced. We consider 4 years to be an appropriate amount of time to allow firms to embed the changes within their business, including to make the necessary investment and any operational changes.

Firms should not wait until the end of the 3-year transitional period to be able to remain within their impact tolerances, but rather remain within them as soon as reasonably practicable within the 3-year period. The 3-year period is a hard deadline. However a firm that is not making reasonable effort to remain within its impact tolerances during the 3-year period would be in breach of our rules.

Operational resilience over the last year

We appreciate that the last 12 months have been challenging for many firms with the impact of the coronavirus pandemic and ongoing Brexit preparations.

Over the last year, operational resilience has become even more important. There has not been a spike in incidents reported to the FCA. But firms and third parties have experienced an increase in hackers attempting to use the pandemic to extract information (for example, through phishing emails). Most firms have also had to quickly adapt to high numbers of their workforce working from home which can bring additional security risks.

While many firms have successfully adapted in the face of the pandemic, we would emphasise that being operationally resilient is an iterative and evolving process. As we have seen with the pandemic, disruption can happen at any time and we should assume that it will occur.

Approach for newly-authorised firms

We expect firms authorised within the 3-year transitional period to March 2025, to use the time up to the 3-year deadline to show they can remain within their impact tolerances. For example, a firm authorised 18 months into the 3-year transitional period will then have up to a maximum of 18 months to show it can remain within its impact tolerances. All firms subject to the policy, included those newly-authorised, will have to meet all other requirements of the policy as soon as the rules take effect on 31 March 2022.

Approach for enhanced-scope SMCR firms

We expect firms changing their status from 'core' to 'enhanced-scope' SMCR, and so bringing themselves into scope of this policy, to approach implementation in the same way as other enhanced firms.

5 Mapping and scenario testing

5.1 In this chapter, we summarise the feedback received on our proposals for firms to map the resources that support their important business services and test their ability to remain within their impact tolerances through a range of severe but plausible disruption scenarios. We also set out our response to this feedback.

CP proposals

5.2 To enable firms to have a complete view of their resilience, we proposed they should identify and document the people, processes, technology, facilities and information (resources) necessary to deliver each of a firm's important business services. This process of mapping will enable firms to identify and address vulnerabilities, and gain assurance that an important business service can remain within the impact tolerance as set.

5.3 We also proposed firms should test their ability to remain within their impact tolerances for each of their important business services in the event of a range of adverse scenarios, including severe but plausible disruption of its operations. This will enable them to gain assurance of the resilience of their important business services and identify where they might need to act to increase their operational resilience.

5.4 We asked 2 questions on mapping and scenario testing, as follows:

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.***

Feedback and responses

5.5 We received 54 responses to question 7 and 60 responses to question 8.

Mapping

Granularity and proportionality

5.6 Several respondents to question 7 asked us to clarify the depth of granularity they should go to when identifying and documenting the people, processes, technology, facilities and information that support their important business services (mapping). Respondents also wanted to understand whether all components of an important business service should feature in the mapping exercise and if the exercise should extend to capture business processes.

5.7 Three respondents asked if we could, now or in the future, provide templates for them to use for the mapping exercise.

5.8 One respondent asked us to clarify how firms should determine when a change is material enough to warrant a review of mapping exercise (eg when a key person leaves).

5.9 Two respondents asked us to clarify our expectations of the level that mapping should be signed off at. One of these respondents asked if it might be possible for a Board/ equivalent management committee to delegate approval of the mapping exercise to an individual, if they considered it appropriate.

Our response

Granularity of the mapping exercise
The level of granularity necessary for mapping important business services will vary between firms. In the CP we proposed that firms should map these proportionately, with the following outcomes in mind:

- identify vulnerabilities and remedy these as appropriate
- enable firms to conduct scenario testing

In response to consultation feedback and to make it easier for firms to implement the mapping requirements, and to a sufficient level of detail, we have changed the final requirements in this area. We have included a transitional provision at SYSC TP 10 setting out our expectation that firms only need to carry out mapping, by 31 March 2022, to a level of sophistication necessary to identify important business services, set impact tolerances and identify any vulnerabilities in their operational resilience. Firms will then have until 31 March 2025, at the latest, to continue performing mapping with a view to being able to remain within impact tolerances for each important business service.

Given mapping is integral to identifying and addressing vulnerabilities that impact its ability to remain within impact tolerances, firms should endeavour to carry out full mapping to meet this policy outcome as soon as reasonably practicable. This is essential to ensure firms consistently remain within impact tolerances by 31 March 2025 at the latest.

We expect firms' mapping exercises to develop and evolve over time. Firms will ultimately need to map to a level of granularity that is sufficient to identify the people, processes, technology, facilities and information that support the operation of their important business services. 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. If the mapping exercise does not provide this outcome, it is likely that the methodology used does not align with the firm's business, size, scale or complexity.

Additional mapping guidance
To help firms with their mapping exercise, we have provided further guidance below on what we mean by the people, processes, technology, facilities and information that support the operation of important business services:

- **People** – People that support the provision of the important business service. Firms need to understand which people are responsible for processes, technology and implementing and monitoring controls. As well as understanding overall senior management accountability

this could include individuals responsible for specific capabilities, the size and strength of their teams, training/education and wider organisational people challenges such as HR controls, employee attrition, hiring practices and key personnel succession planning.
- **Processes** – A process is a structured set of activities designed to produce a specific output. The ability to define what processes are responsible for delivering outputs in an organisation is a key element of an organisations approach to technology.
- **Technology** – Underlying systems and architecture to support the provision of the service.
- **Facilities** – Office locations, printing facilities, mailing, credit card production / statements / client communications.
- **Information** – Any data, feeds or material that is required by a firm to deliver a service.

Mapping templates
Firms mapping exercises will vary greatly depending on the firm's business, size, scale and complexity. We have considered if it is appropriate to develop mapping templates. For mapping templates to be useful for firms and effective for our regulatory purposes, multiple templates would need to be developed and maintained and even these may not reflect the specifics of a firm's business operations.

Updates to the mapping exercise
Firms should update their mapping exercise:

- if there is a material change to the firm's business, the important business services identified in line with SYSC 15A.2.1R or impact tolerances set in line with SYSC 15A.2.5R
- in any event, no later than 1 year after it last carried out the relevant assessment

Governance and sign-off
We do not consider it appropriate for approval of the mapping exercise to be delegated to someone that is not on the Board or equivalent management body. Senior management is accountable for their firm's operational resilience and should have improved oversight. However, as we outlined in the CP, members of the Board or equivalent management body responsible for the mapping exercise should still discuss the detail of the firm's operational resilience with other colleagues who have more technical expertise to satisfy themselves of its adequacy.

Firms in scope of the SM&CR should continue to refer to paragraphs 7.8 to 7.12 of the CP where we set out our expectations for senior managers (and in particular, those performing the SMF24 function (Chief Operations Function)). 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 changing this approach for the oversight of operational resilience. If firms do not have an individual performing the SMF24 function under the SM&CR, they must determine the most appropriate individual within the firm who is accountable for operational resilience.

It is also likely that firms will identify, through the mapping exercise, individuals fulfilling key roles. Firms should ensure they have plans in place for these key people being unavailable. This has been demonstrated particularly throughout the coronavirus pandemic where key people have been unavailable for a number of reasons such as being unwell/self-isolating and taking time off work to fulfil caring responsibilities.

Third-parties and supply chains

5.10 Twenty-four respondents had comments about the mapping exercise and third-party providers and supply chains. Respondents asked for clarity on if, and if so how, they should map 4th/5th party providers, used by a known third-party provider, which may not be visible to the primary firm. Respondents also had comments on the circumstances in which they would need to map third-party provision, including whether Appointed Representatives (ARs) should be included in a firm's mapping exercise.

Our response

Mapping external providers

We expect firms in scope to be responsible for accurately mapping any relationship outsourced to an external third party. If a firm outsources to a third party (including an AR, or for payments firms, agents providing payment services on behalf of the firm, for example), it still needs to be able to understand the potential vulnerabilities by mapping where those vulnerabilities occur, whether they sit with the third party or beyond. If firms are unable to obtain sufficient information from the third party to satisfy them that they can operate within tolerance, then they should review and where necessary change their arrangements.

By actively capturing and maintaining relationships with third-party providers we expect firms in scope of this policy to satisfy themselves of that third party's resilience. Ultimately, if a third-party provider supplying an important business service to a firm fails to remain within impact tolerances, that failure is the responsibility of the firm.

Links to existing/proposed requirements

5.11 Some respondents also commented on how our policy proposals interact with outsourcing requirements, namely those proposed by the European Banking Authority (EBA) and in the EC's Digital Finance Strategy.

Our response

For further information on the interaction between our proposals and relevant EBA Guidelines and the EC's Digital Finance Strategy, including DORA, please see Annex 2.

Data handling

5.12 One respondent was concerned about how firms' mapping information would be handled by the regulator and asked us to consider this data-handling to avoid unintended consequences. The respondent highlighted that firms must also consider the data risk associated with sharing information externally.

Our response

Any data provided to us is, and will continue to be, handled with the utmost care. The FCA is subject to the onshored General Data Protection Regulation (GDPR) and complies with these requirements. We are also subject to confidentiality under section 348 FSMA. For firms sharing data with external parties, firms should comply with existing requirements on data handling. Payments firms are subject to s.348 FSMA as applied and modified by the EMRs 2011 / PSRs 2017 as applicable.

How our example firms may approach the mapping exercise

Firm A

Firm A conducts a mapping exercise to fully outline the underlying systems, technology and people, including material third party suppliers, and their interdependencies that enable its mobile platform app.

From its mapping, Firm A concludes that its proprietary software engineering procedures and code enhancement (a core dependency) ensures resiliency by design including advance monitoring tools for early detection of availability and performance anomalies. Firm A also engages with critical third-party suppliers including data centre providers (Cloud Provisioning) where mobile app servers are hosted to understand their risk controls and agree a compatible service level agreement.

Firm A leveraged an existing map used for its annual business impact analysis during its mapping exercise.

Firm B

Firm B undertakes a mapping exercise of the resources that support the delivery of claims handling process. Firm B's mapping reflects that it employs 180 contact centre agents (inbound call handlers) who work across two 7-hour shifts during office hours in their main office location, and have the appropriate technology to work from home if required.

Firm B has identified most of the technology infrastructure including the online portal are hosted in the cloud provided by an external cloud service provider. The contact centre is located at the same location as the main office, and its technology and infrastructure are outsourced to a major telecom company where a service level agreement is in place.

Firm C

Firm C's mapping exercise is complex due to the number of interconnecting systems and technologies it relies on and because many of them are outsourced to, or delivered by, third-party providers. Customisation of services and tools and the way that they are often integrated with consumers and counterparties increase this complexity further.

Technical services and components are mapped through developed process and governance function but Firm C does not have a complete view for all business and operational services including their underlying dependencies. However, Firm C considers that is has sufficiently undertaken the mapping exercise, liaising where necessary with its third-party providers, to identify vulnerabilities and next steps to remedy these.

Testing

Testing expectations for firms

5.13 Twenty-two respondents asked us to further clarify our proposal that firms test their ability to remain with their impact tolerance. Respondents suggested this could be achieved through:

- the prescription of industry-wide tests
- firm and sector-level testing
- examples of real-life or hypothetical 'severe but plausible' scenarios
- information on types of testing methods to be used
- effective collaboration across firms/industry

5.14 One respondent asked if firms should test for worst case scenarios which are unlikely, or concentrate on testing for more likely/probable scenarios but which may cause less harm.

5.15 Three respondents considered that we should review the language used in the CP to focus more on preventative measures than mitigating disruption once it has already occurred.

Our response

We appreciate respondent's comments on the ways in which we could make our testing expectations clearer. We have set out in this PS, through our example firm scenarios, how different firms might go about scenario testing. We have also included in these examples 'severe but plausible' scenarios firms might test against.

Industry-wide tests

While we agree that the introduction of industry-wide tests could be helpful for some firms, and particularly smaller firms, this needs to be balanced against the cost and resources to develop and maintain these tests. Such tests could also encourage some firms to adopt a 'tick-box' approach to testing, where they simply strive to ensure the requirements of the prescribed tests were met. We will, however, consider if industry-wide tests could be developed over the longer term as part of our supervisory approach.

Testing methods
The most appropriate testing method to use will depend on several factors. These include the firm's:

- size, scale, complexity
- business (considering the sector, products, services)

Testing methods will also vary depending on the 'severe but plausible' scenarios identified by the firm in question. While the methodologies may vary from firm to firm, we would expect each firm to approach scenario testing in a consistent manner to ensure accurate results.

Testing in a range of severe but plausible scenarios is intended to help firms identify areas where further resilience needs to be built. In carrying out testing and remediating any vulnerabilities, firms should in turn be better prepared for potential real-life disruption and reduce the number of such disruptions which could cause intolerable harm to consumers and/or risk to market integrity. Testing is a preventative measure against real-life disruption.

Firms should also continue to consider the scenario factors and testing plan considerations included in paragraphs 6.15 – 6.16 of the CP.

Frequency of testing

5.16 Five respondents had comments on the frequency of testing. Four suggested that re-testing only be done when the environment has materially changed, or sufficient time has passed. One respondent noted the difference between the FCA's requirement to test 'annually' and the PRA's requirement to test 'regularly'.

Our response

We have made some changes to our scenario testing requirements to provide firms with some additional flexibility.

First, we have clarified (through a transitional provision at SYSC TP 10) our expectation that firms only need to carry out scenario testing, by 31 March 2022, to a level of sophistication necessary to identify important business services, set impact tolerances and identify any vulnerabilities in their operational resilience. Firms will then have until 31 March 2025, at the latest, to continue performing scenario testing with a view to being able to remain within impact tolerances for each important business service. Firms have the flexibility to implement scenario testing proportionately through this initial phase. In practice this means that firms may decide to focus during the first year (from publication of this PS to 31 March 2022) on scenario testing only some of their important business services.

Given scenario testing is crucial to meeting the requirement of consistently remaining within impact tolerances by 31 March 2025, at the

latest, firms should continue to test as effectively as possible during the transition period.

Second, we have changed the frequency of testing requirement at SYSC 15A.5.7R. Our final rules do not require testing to be undertaken at least every year as proposed. Instead, firms are required to scenario test when:

- there is a material change to the firm's business, the important business services identified in line with SYSC 15A.2.1R or impact tolerances set in line with SYSC 15A.2.5R
- following improvements made by the firm in response to a previous test
- in any event, on a regular basis.

This approach recognises the benefits of providing firms greater flexibility to tailor the frequency of testing to the characteristics of the important business service concerned. We expect firms to set the frequency of their scenario testing prudently and in a way that meets the ultimate goals of the policy. We have also removed 'any' from 'following any improvements made by the firm in response to a previous test' to clarify that firms can be proportionate about the improvements they need to make in this situation.

Business as usual and testing requirements

5.17 Eleven respondents asked us to consider how testing requirements will impact on business-as-usual operational needs. Respondents suggested that firms take a risk-based and proportionate approach to testing. Some respondents noted that testing schedules and priorities will need to be established and maintained as it may not be feasible to test all scenarios at the same time.

Our response

We understand that there may be occasions where the scenario testing schedule could affect business-as-usual operations. This could be, for example, because people resource required for testing takes resource away from other required tasks. Firms should consider such issues when organising their testing schedule and consider how best to minimise disruption to other activities while still meeting our requirements.

Third parties and effective testing

5.18 Some respondents asked us to clarify whether, and if so how, firms should work with third parties to ensure effective testing. One such respondent highlighted that third and fourth parties may become overburdened by testing requests and could either refuse or charge to carry out testing or only test on a periodic basis.

Our response

Working with third parties on testing

Firms should approach testing with third parties in the same way as they approach the mapping exercise, working as effectively as possible with third parties to facilitate testing. This could mean that either the firm or the third party carries out testing. Firms in scope of the policy will need to satisfy themselves, if the third party is going to carry out any testing, of the methodologies, scenarios and considerations of the third party in doing so. The firm is ultimately responsible for the quality and accuracy of any testing carried out, be that by themselves or by an external party.

How our example firms may conduct scenario testing

Firm A

Firm A conducts regular reviews of resources that enable the delivery of its business services as part of its annual business impact analysis. It designs severe but plausible scenarios, considering the potential impact of loss of third-party provision, and engages third parties to test the enablers of its e-wallet account provision for users. These tests indicate some residual risks and resilience gaps when faced with a severe but plausible scenario including those associated with channel of service delivery and cloud service provisioning by third parties.

Following a review of lessons learned, Firm A provides a web channel as an additional service delivery channel to users as a back-up solution, and as an alternative in all eventualities. Among other actions, the firm also conducts a benchmarking exercise to identify alternate cloud providers with dispersed data centres across broader geographical spread where servers can be hosted to enable seamless continuity of service in all eventualities. It sets in motion plans to refresh its data protection policy to recognise cross-jurisdictional legal and regulatory requirements and develops a communication plan to advise users about alternative ways to access services and updates for service resumption.

Firm B

Firm B works with its cloud and contact centre infrastructure providers to design and test severe but plausible scenarios, considering the potential impact of cloud disruption, to ensure it can remain within its impact tolerance.

During testing, Firm B has identified challenges with its contact centre provider, where there were significant dependencies on the provider's sub-contractor based in a different country, and due to resource stretch and poor change management practices, the sub-contractor was unable to bring Firm B's contact centre systems back online within the 2-day time frame.

Firm B has also identified there was a significant backlog of cases after a disruption, and its current call handling resourcing plans were inadequate to deal with the backlog of cases.

Firm B initiated a review to improve its controls over the monitoring and oversight of the contact centre provider. It also revisited its contractual terms and service level agreement (including the use of sub-contractors) with the provider, to ensure appropriate service and support can be provided to enable Firm B to remain within tolerance.

Firm B also updated its resourcing plans to allow additional call handlers to be brought in and trained up straight after an outage to minimise the backlog of cases.

Firm C

Firm C scans the operating environment to understand changing risks and events that could affect parts of its business eg cyber security, political, environmental, social, technology and market changes. It engages with its business counterparties to enhance the validity of these tests. This includes carrying out end-to-end tests for individual processes involving all relevant parties (internal and external) and including an independent third party to verify the testing methodology.

Firm C carries out 'severe but plausible' scenario testing on investment execution including the order management systems to ensure procedures for execution and allocation of client orders are robust. The firm carried out a test whereby an inaccurate order was created during a period of high market volatility. Modelling the remediation required in simulated market conditions showed that a real-world occurrence of a similar event would have resulted in significant losses to the firm. It was identified that lack of resources to pick up the error and use of multiple platforms within the firm exacerbated the problem. Firm C has responded by both improving its trade monitoring and reducing the number of platforms used to order and execute trades.

6 Communications, governance and self-assessment and responses to our cost benefit analysis

6.1 In this chapter, we summarise the feedback received on our proposals on firms' communications plans and a self-assessment document, along with our response. We also address feedback received to our cost benefit analysis.

CP proposals

6.2 We proposed firms should have internal and external communication strategies in place to respond quickly and effectively to reduce the harm caused by operational disruptions. For their internal communications strategies, we proposed firms should also include the escalations paths they would use to manage communications during an incident, and identify the appropriate decision makers. As part of their external communications strategy, we proposed firms consider how they would provide important warnings or advice to consumers and other stakeholders, including where there is no direct line of communication.

6.3 We also proposed that firms should compile a self-assessment document which shows how they meet our operational resilience requirements. The document will not need to be submitted to us, but it should be made available on request. Boards, or the firm's management body, should review and approve the self-assessment document regularly.

6.4 We asked 2 questions on communications plans and the self-assessment document:

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

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

Feedback and responses

6.5 We received 45 responses to question 9 and 55 responses to question 10.

Communication plans

6.6 All respondents agreed with our approach to communications plans. However, several respondents asked us to clarify specific areas. These included:

- the high-level nature of our proposed SYSC 15A.8 provisions on communications and how these interact with Principle 7
- if existing communications plans can be repurposed rather than developing new ones
- how our proposals for communication plans interact with the treatment of vulnerable consumers

- if the regulators could review the resilience and interdependencies of major central systems, such as CHAPS, to define what communication paths need to be reaffirmed and/or established, when faced with national or sector wide incidents
- if the regulators could play more of a role in coordinating communications responses, for example in the event of systemic disruption

6.7 Three respondents commented on the interaction of our proposals for communications plans with existing requirements such as Supervisory Review and Evaluation Process (SREP), Internal Capital Adequacy and Risk Assessment (ICARA), operational risk and K-factors. Two of these respondents raised concerns with how the proposals would interact in future with those of the BCBS.

Our response

Existing requirements
Our proposed Handbook section on communications, SYSC 15A.8, aims to provide high-level requirements and guidance for firms. This approach aims to ensure that our provisions give firms the flexibility to apply our framework in a proportionate manner. We have also reviewed the interaction between SYSC 15A.8.3R and Principle 7 (Communications with clients). We consider that these 2 provisions complement each other. Given that Principle 7 applies to all the firms we regulate, any firm subject to operational resilience proposals is also subject to this Principle. In practice, this means for the purposes of operational resilience communications, a firm must 'pay due regard to the information needs of its clients' and provide 'clear, timely and relevant communications to stakeholders in the event of operational disruption'. Firms should ensure, in line with Principle 7, that such communications are also 'fair, clear and not misleading'.

Treatment of vulnerable consumers
We agree with feedback received that firms should consider the communication needs of vulnerable consumers. In the CP, at SYSC 15A.8.2G, we proposed firms consider how they 'would provide important warnings or advice quickly to consumers and other stakeholders, including where there is no direct line of communication'.

To address how firms should treat vulnerable consumers in the context of our policy, we have added guidance at SYSC 15A.8.2G(3). This new sub-paragraph aims to clarify that firms should be mindful of consumer/stakeholder access to different channels when identifying communications methods.

We also recommend firms consult our finalised guidance on the fair treatment of vulnerable customers for further information.

Repurposing existing communications plans/strategies
We have considered respondents' feedback about repurposing existing communications plans or strategies. We consider this to be appropriate, if firms continue to maintain the original plans to meet other existing requirements.

Resilience and interdependencies of major central systems
We appreciate the feedback about us reviewing the resilience and interdependencies of major central systems. Our focus is to improve operational resilience in aggregate by focusing on individual firms although we expect firms to understand their dependencies on third parties and have capabilities in place to ensure that any disruption to services is minimised. Trade bodies and industry groups, which coordinate industry and sector-wide views and information, may be able to help firms in identifying links between major central systems.

Cross-firm/systemic disruption
We can see how it could be beneficial for firms to be notified of cross-firm/systemic disruption. We expect firms to consider, in line with SYSC 15A.8.2G(1), how communications strategies can be used to notify consumers and other stakeholders in the event of disruption. This guidance includes where the customer is another regulated firm and so could be a valuable tool for cross-firm coordination.

It will not be possible for us to coordinate communications for firms in the event of cross-firm/systemic disruptions. While we understand there may sometimes be disruptions which affect multiple services across a range of firms simultaneously, it would be challenging for the FCA, given reporting mechanisms and data sharing processes, to provide this oversight function to firms. In addition, communication needs will vary depending on a number of factors (such as the firm/sector/important business service affected/customer base). So firms remain best placed to identify how best to prepare communications for, and respond to, disruption.

Existing requirements
We have considered the feedback about the interaction of our proposals for communications plans with existing requirements such as Supervisory Review and Evaluation Process (SREP), Internal Capital Adequacy and Risk Assessment (ICARA), operational risk and K-factors. Annex 2 contains further detail.

Self-assessment document

6.8 Respondents broadly agreed with our proposed requirement for a self-assessment document. Some respondents asked us for clarification in some areas, and requested for additional guidance.

Templates

6.9 Seventeen respondents asked if we could provide templates for the self-assessment document, or if we could provide further information on the format the document should take. Respondents considered that templates would ensure consistency of approach across firms and sectors.

Our response

We appreciate why some respondents felt a template for the self-assessment document would help meet the rules for their business. However, as with the mapping exercise, for templates to be useful for firms they would need to be sufficiently detailed to meet the range of firms in scope. We consider that any template may end up being too high-level to be of value to firms, or risk not sufficiently catering to their individual circumstances. We are also concerned that the introduction of templates could promote a 'tick-box' approach to complying with the policy when we want firms to implement it in a proportionate manner.

Similar firms may wish to share best practice through working groups, which we are happy to engage with.

Self-assessment document content/purpose

6.10 Three respondents had general comments on the content/purpose of the self-assessment document. Areas where further clarity were requested included:

- our intentions for 'the methodologies used to undertake the activities' as set out in paragraph 7.16 of the CP
- how the document would show a firm's resilience journey
- if the document could be published on firms' websites

6.11 One respondent asked if it would be possible to include additional documentation as part of their self-assessment document, for example internal or external audit reports. The respondent considered that the inclusion of such reports would help show the extent to which Boards or senior management are across issues.

6.12 Seven respondents commented on how often the self-assessment document needs to be reviewed, the earliest date it could be requested and whether it could be submitted in a staged approach through the transition period. One other respondent commented whether maintaining a self-assessment document which may never be requested by the FCA could be too resource intensive. They also observed that the resource effort put into reviewing and maintaining the document could vary across firms.

Our response

What to include in your self-assessment document

Our proposal for firms to prepare a self-assessment document, like many of the rules introduced through this policy, is intended to allow firms to apply the proposals proportionately and in a way which best suits their business. We set out, in SYSC 15A.6.1R, our proposal for what firms must include written record of in their self-assessment document. The rule also states that the list is 'not limited'. Firms have discretion to include additional information in their self-assessment document as they see fit. Firms may wish to include internal or external audit reports, or parts thereof, in the document.

With reference to the 'methodologies' set out in SYSC 15A.6.1R(9), firms should develop their own methodology to best fit their business, and to document their activities 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.

Format

Firms should prepare their self-assessment document in a format which is clear and well-structured. This could be in the form of a text document, slide-deck or spreadsheet. A firm's self-assessment document may also be presented in the form of multiple files of different types. The format of the documentation is not important, but ensuring it is clear and accurately reflects the operational resilience of the firm is.

Self-assessment and the resilience journey

We consider that the self-assessment document will show a firm's resilience journey. When firms include in the document the required information as required by SYSC 15A.6.1R, and the methodologies used to fulfil the activities set out in sub-paragraphs (1) to (8), they will in turn show the steps they have taken over time to comply with the policy. The document will not show the firm's resilience journey pre-introduction of the policy but it will show how the firm has endeavoured to meet its requirements.

Firms can publish their self-assessment documents on their websites if they wish to, but this is not something we require.

Submission expectations

We remind firms that their self-assessment documents do not need to be submitted to us periodically. They need only be provided to us on request or made available for inspection as part of firm engagement. The earliest date that we would formally request the completed self-assessment document will be no earlier than 31 March 2022. This is because we consider that firms will need to have fully operationalised the policy before the document can be completed.

We agree that different firms may allocate differing levels of resource to create and maintain the self-assessment document. Preparation of this document has a range of benefits beyond provision to the FCA. For example, compiling a self-assessment document helps firms assure themselves of their own compliance, provide the basis to take necessary action to address weaknesses in their resilience and to provide necessary information for senior management.

Review process

Firms should review and update their self-assessment document regularly. Firms are best placed to decide how regularly this review needs to be depending on their business. As set out in the CP, where changes occur that may have a clear impact on the firm's operational resilience, such as 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.

Data handling

6.13 One respondent asked us to clarify how we plan to receive and store data submitted to us as part of the self-assessment document.

Our response

We can assure firms that any data provided to us is, and will continue to be, handled with the utmost care. Self-assessment documents, as with other sensitive material submitted to the FCA, will be stored securely.

Response to our cost benefit analysis

6.14 We received 32 responses to our cost benefit analysis. Most respondents agreed with our cost benefit analysis but several respondents considered that some of the cost estimates appeared too low. Of these, 2 provided their own cost estimates. Both estimates set the expected costs at a higher level than estimated in our CBA.

6.15 Respondents commented more generally on the following areas of the CBA:

- **The sample of firms used.** Some respondents considered that the sample size itself was too small, or not representative of all the firms which would be in scope of the policy.
- **Costs missed/underestimated.** Some respondents believed we should have included costs for firms using service providers. Others considered that the CBA underestimated costs associated with people and resources, IT costs, testing implementation, and costs for firms 'opting up' to enhanced SM&CR status.
- **The proportionality implications of our proposals.** Several respondents considered that we should have greater regard to how the costs could be more proportionate to the size of the firm and the systems and processes they may or may not have already in place. In particular, respondents were concerned that the costs may be higher for smaller firms. One respondent commented that the costs borne by medium and small firms may ultimately result in increased costs for customers. In addition, the respondent considered that such costs could pose a barrier to entry for smaller firms as they are more easily borne by the largest or more established firms.

6.16 One respondent asked us to provide our suggested methodology for assessing 'appropriate' level of resilience effort/investment based on the nature, scale and complexity of the firm's activities.

6.17 Another respondent asked us to clarify how respondents to the industry survey (and the FCA) can assess the additional benefits that the proposed operational resilience framework may deliver over the existing/baseline regulatory compliance framework. The respondent stated this was unclear when some components of the baseline framework only started to apply in the last 12 months.

6.18 One respondent requested we consider the economic and financial impacts caused by the current pandemic in setting out cost estimations.

6.19 A couple of respondents asked us to clarify how the proposals will be beneficial to/ improve efficiency of firms in the long term. One of these respondents evidenced that

in paragraph 81 of the CBA we only stated that 'our proposals will be net beneficial in the short to medium term'.

6.20 Some respondents noted the differences in costs estimated by the FCA and PRA. One of these respondents questioned how it should interpret the regulators' analysis. For example, whether it should sum the PRA and FCA figures, take the higher value or take an average.

6.21 A few respondents commented on the cost implications of implementing our proposals alongside existing frameworks. One such respondent considered that tooling and data enrichment could be needed to effectively implement our policy. The respondent considered that further changes to pre-existing frameworks, such as the Operational Risk Framework (ORF), would also be needed to ensure alignment across the business. Another respondent considered that firms may need to make changes to their operating models to implement our policy alongside existing legislative requirements. For example, to ensure that business continuity teams can take on the additional work and be appropriately supported on governance measures.

Our response

We thank respondents for their comments on our CBA. When we undertook the data gathering exercise for the CBA we ensured that a range of firms across the scope of the policy were captured. We sent surveys to 1,562 firms, and received responses from 146 firms. We considered this level of engagement to be representative of the general firm population within scope. Our CBA costs used the costs estimated by these 146 firms as their basis. We set out in paragraph 35 of Annex 2 to the CP known limitations with our approach and, where possible, what action we had taken to remediate these limitations. For example, knowing that a small sample size in sub-groups can reduce the reliability of conclusions that can be drawn from the data, we stratified responses by size to make the sample as representative as possible of firms in scope.

We did not include any costs associated with outsourcing (including the use of third-party service providers) in our CBA as we are not introducing any new requirements in this area. So such costs are out of scope. As the CBA was based on costs estimated by firms themselves, to accurately revisit any costs, we would need to ask firms for their input again. We do not consider this to be necessary given most respondents to question 11 of the CP agreed with our analysis, and we are not making any substantive changes to the policy. Detail on the specific costs considered can be found at paragraphs 49 to 63 of Annex 2 to the CP.

We have engaged directly with the 2 firms who provided cost estimates reflecting costs greater than those set out in our CBA in their consultation responses. The discussion allowed us to understand the firms' feedback and ensure our CBA estimates are accurate.

One of the firms went on to complete the survey on which we originally based our CBA. We considered this would allow us to more accurately compare their estimated costs to others previously received from similar

firms. We have compared the estimated costs against the submissions of other firms of a similar size and complexity. Following this analysis, while we welcome the breadth and rigour of the firm's approach to operational resilience in general, we do not believe the size and scale of the programme envisaged is representative of the costs likely to be experienced by other similarly sized firms to meet the new requirements of the policy. As with another similar firm who responded to the original survey, and whose estimate we excluded in on the same basis from our CBA estimates, the firm projected implementation costs of an order of magnitude higher than its other peers who participated. We do not therefore consider it necessary to add the firm's estimated costs to our CBA estimate of average costs.

The other firm who we had a discussion with advised that its estimated costs were intended only to give an indication of the likely magnitude of the costs. Their methodology made use of a number of general assumptions including on the number of services and estimated market rates for certain activities the firm was undertaking to implement the framework (improvements to existing IT systems, for example). On this basis, we have not amended our original CBA estimates to include them. This is because we do not consider all of their costs necessary to implement the policy requirements to an instructive level of accuracy.

Reflecting this, and the fact most respondents agreed with our detailed analysis, we are satisfied the CBA estimates remain accurate. And reflects the final rules being implemented. We are only making one substantive change to the policy - to provide firms with more flexibility and time to perform mapping and scenario testing. We consider this will have a positive impact on costs for firms, although, correspondingly, it is likely to delay the delivery of benefits.

If a firm chooses to 'opt-up' to enhanced scope SM&CR status to bring itself within scope of the policy, it should consider the associated costs and benefits as set out in Annex 2 to the CP. We did not expressly include costs for such firms in the CBA as we considered that firms identifying as enhanced scope SM&CR firms would fall within the existing large/ medium firm size brackets, for which costs are included.

The rules set out in this PS, are designed to give firms the flexibility to apply these proportionately to reflect their business. This means that, for example, for a smaller firm with a limited number of important business services, costs will be significantly lower than for a medium-sized firm with a high number of important business services. However, we recognise that smaller firms may have limited resources. But we are only applying the rules to the firms which we consider carry the highest levels of systemic risk and/or intolerable levels of harm to their consumers and/or risk to market integrity in the event of disruption. These are firms we consider are generally equipped to implement the rules within the 4-year period.

The rules are also designed to be targeted, limiting the extent of application for firms who would be out of scope but for their PSRs 2017/EMRs 2011 permission. Where these payments firms have other permissions to carry on activities which do not meet the relevant FSMA thresholds, they only have to apply the policy to their payments activities.

We are aware that the impact of the coronavirus pandemic will have placed some firms under increased financial pressure. Withstanding operational challenges throughout the pandemic has also highlighted the importance and the benefits of strengthening firms' operational resilience. While we do not consider it necessary to revisit our cost benefit analysis in light of coronavirus, we understand that some firms may face greater implementation and financial pressures at the present time. We consider that the costs and benefits remain substantively the same now as originally estimated in the CP.

It is not possible to quantify with certainty when the policy will be net beneficial. This would depend on the number and scale of disruptive incidents firms might have faced in the future without our intervention, and the benefits to firms, customers and the wider economy from the mitigating effects of this policy. Keeping these limitations in mind, we set out in the CP (see Annex 2, paragraphs 77 to 80) how we expected the costs to be net beneficial.

We do this by comparing 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 our proposals to be net beneficial. We expect that the benefits will be delivered in several ways; from the reduction of avoidable costs such as fines and operational disruptions to other unquantifiable benefits such as avoided psychological stress and wider benefits to the stability of the financial system and wider economy. Our assessment was that intervention would become net beneficial within the short to medium term, so that it is also net beneficial in the longer term.

Our rules are designed to help firms implement the rules in a proportionate way, that reflects their business. For the same reason, we do not consider it appropriate to suggest a methodology for firms to assess what is an appropriate level of resilience effort. We expect smaller and less complex firms to have fewer important business services, and fewer staff, systems and processes to map, test and stay within tolerance for. Firms may wish to work together alongside trade associations and industry groups to discuss the framework and share knowledge.

One respondent indicated a potential additional need for tooling and data-enrichment processes. However, different firms might require different solutions/tooling to comply. In our CBA we provided average values for this type of cost across all firms in scope.

We recognise it can be challenging to measure the benefits the new framework may deliver over the existing regulatory framework when some of those baseline requirements have only taken effect recently. From a regulatory perspective, we will be assessing the benefits of the new framework throughout the policy implementation and transition periods and beyond.

For dual-regulated firms, we ensured that costs set out by the FCA did not constitute additional costs on top of those set out by the PRA. Differences in costs reflect the different firms within scope of each regulator's proposals; for example, 'small' and 'large' firms for the PRA's purposes are different to 'medium' and 'large' referenced by the FCA. But both the FCA and PRA estimates used the same survey from the same firms. The FCA and PRA's costs are not cumulative, but reflect an estimate of the cost each firm will incur in implementing, and complying with, each authority's policy. Many aspects of the authority's policies align and overlap.

Annex 1
List of non-confidential respondents

Legal & General

Incillation Ltd

BGL Group

St James' Place Wealth Management

IPSX UK Limited

Citi

The Institute of International Finance (IIF) and Global Financial Markets Association (GFMA)

European Venues & Intermediaries Association (EVIA)

Electronic Money Association (EMA)

IBM

Bank Policy Institute (BPI)

Investment & Life Assurance Group (ILAG)

AXA UK Group

Association of British Credit Unions Limited (ABCUL)

TheCityUK

London Stock Exchange Group (LSEG)

Association of Mortgage Intermediaries (AMI) and the Association of Finance Brokers (AFB)

London Metal Exchange (LME)

Standard Life Aberdeen plc

JP Morgan

HSBC

Building Societies Association (BSA)

Pavel Burkov

UK Finance

The Association of British Insurers (ABI)

Depository Trust & Clearing Company (DTCC)

Ernst & Young LLP (EY)

World Federation of Exchanges (WFE)

Lloyd's/Lloyd's Market Association (LMA)

Accenture

Bud

Association of Foreign Banks (AFB)

London & International Insurance Brokers' Association (LIIBA)

Deutsche Bank

Japanese Bankers Association (JBA)

Zurich Insurance

The TA Forum

The Investment Association

Personal Investment Management & Financial Advice Association (PIMFA)

PwC

Nationwide Building Society

Nottingham Building Society

Ashmore Group

The England and Wales Chapter of the Institute of Operational Risk

Aldbury International Ltd

The Society of Pension Professionals (SPP)

West Bromwich Building Society

Computershare Investor Services (CIS) plc

Experian

Cboe Global Markets

The Investing and Saving Alliance (TISA)

Annex 2
Examples of relevant existing FCA requirements

1. In this annex, we summarise the feedback received on the examples of existing legislation.

2. We received 35 responses to this question. Of these 35, 17 had no comments on, and/or agreed with, our examples provided in Annex 4 to the CP.

Feedback and responses

Interaction with existing/proposed requirements

3. Nine respondents had comments relating to how our proposals will interact with existing or proposed requirements. Respondents had a strong preference for regulatory alignment across jurisdictions, where possible. The existing or proposed requirements where respondents asked for information on interaction with our new proposals included:

- the EBA Guidelines on ICT and security risk management (EBA/GL/2019/04) and the EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02)
- the Basel Committee for Banking Supervision's (BCBS's) proposed Principles for Operational Resilience and the European Commission's proposed Digital Operational Resilience Act (DORA)
- Recovery and Resolution Planning (RRP), Operational Continuity in Resolution (OCIR), Resolvability Assessment Framework (RAF) and business continuity planning (BCP), and
- the International Organization of Securities Commission's (IOSCO's) Principles on Outsourcing.

Regulatory obligations for firms operating internationally

4. Several respondents expressed some concern that our proposed requirements could overcomplicate their regulatory obligations, particularly where the firm operates at the international level and must comply with multiple frameworks from different jurisdictions. In this context, 4 respondents considered that the introduction of our new operational resilience framework could create a fragmented approach to operational resilience. One such respondent considered that there were already many different approaches to the implementation of existing regimes across jurisdictions. Further, it considered that introducing a new operational resilience framework which was not fully aligned at the international level would compound existing challenges for global firms and undermine the objective to strengthen operational resilience.

Our response

As we explained in the CP, our intention with the introduction of this policy is not to create overlaps or conflicts with existing requirements. When developing our policy, we considered, and we continue to consider, the interaction of our framework with existing requirements.

We recognise that there are some areas where the requirements are similar, and that it could be harder for firms to identify action they need to take to comply. We also appreciate the challenges for global firms in complying with cross-jurisdictional requirements.

In introducing a framework which is flexible and proportionate, firms will have autonomy to implement and comply without the existing regulatory landscape becoming fragmented. We have reviewed Annex 4 to the CP and consider that all the information provided is still relevant. Firms should therefore continue to use this as a resource.

EBA Guidelines

We committed in paragraph 1.12 of the CP to further clarify the links between the EBA Guidelines on ICT and security risk management (EBA/GL/2019/04) and our operational resilience policy.

In summary, 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.

We consider our operational resilience framework can be distinguished from the Guidelines in the following key ways:

- 'business function' is a very common term in traditional risk management approach and is broadly understood in a similar way. We consider such business functions would cover the same services that we call 'important business services', but can also be broader by covering support functions, which of course we don't capture in our definition of 'important business services' (e.g. the HR function). An easy way to understand the difference is by viewing the concepts in the following ways: Important Business Service = Business Function + Assessment of 'Importance'.
- The Guidelines establish requirements for firms to mitigate and manage their ICT and security risks. While these requirements cover topics such as sound internal governance, information security requirements, ICT operations, project and change management and business continuity management, (and so can contribute towards a firm's overall resilience), they are not setting requirements around operational resilience. Furthermore, while the guidelines are focused on ICT and security risks, our focus is on operational resilience more broadly (covering ICT and security, but not limited to just ICT and security risks).

In relation to the EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02), because of our focus on responding to the pandemic, we have so far been unable to undertake any formal policy work in the area of outsourcing and third-party service providers. Firms should continue to comply with existing requirements in this area and have regard to ESMA's Final report: Guidelines on outsourcing to cloud service providers and EIOPA's Guidelines on outsourcing to cloud service providers. We are working closely with colleagues at the PRA to input into its outsourcing work and are monitoring whether there is a need for us to take additional action.

Firms should continue to apply the EBA Guidelines in line with our Brexit: Our approach to EU non-legislative materials document.

Other international developments

We have been monitoring, and contributing to, international operational resilience proposals. We consider that the BCBS's proposals are broadly aligned to our framework in terms of outcomes. For example, while the BCBS refer to 'critical operations' and us to 'important business services', we consider the identification of such operations and services by firms would result in better operational oversight, increased protection for consumers and market integrity and overall, improved resilience. As the EC's DORA is in draft form and could be subject to further change post-consultation, we will continue to monitor its progression.

Links with business continuity planning

Firms should continue to refer to Annex 4 of the CP for detailed information on business continuity planning (BCP). Operational Continuity in Resolution (OCIR) requirements are the responsibility of the PRA. The PRA has recently consulted on updated requirements in this area to improve firms' resolvability and support the Bank of England's approach to resolution as set out in the Statement of Policy 'The Bank of England's approach to assessing resolvability'. The PRA expect to publish final policy in H1 2021, with the changes taking effect on 1 January 2022. For further information on Recovery and Resolution Planning (RRP) and the Resolvability Assessment Framework (RAF), please see the PRA's website.

Operational resilience builds upon the concepts of preparedness and recovery by focusing on how businesses can prevent, adapt, respond to, recover and learn from operational disruptions. Key to this is firms positioning themselves to be able to continue to provide the important business services relied upon by customers and markets from the perspective that disruption is inevitable, including from unexpected disasters. This is distinct from business continuity planning which focuses on how firms manage operational risks in respect of their ability to continue operating or recover their internal and external business processes if something goes wrong with an eye to the firm's own commercial interests.

Operational resilience and the Temporary Permissions Regime

5. One respondent asked us to clarify the applicability of the operational resilience framework requirements to EEA firms that enter the Temporary Permissions Regime (TPR), post-Brexit.

Our response

We stated in the CP that the policy would not apply to EEA firms (see paragraph 1.5). This includes previously incoming EEA firms who have now entered the Temporary Permissions Regime (TPR) or Financial Services Contracts Regime (FSCR). We have also added provisions to the rules (see SYSC 15A.1.4R and SYSC 15A.1.9R) to clarify that overseas firms are not in scope. This is consistent with the PRA's approach.

Links between operational risk and operational/cyber resilience

6. One respondent asked us to clarify the interaction between operational risk and operational resilience, specifically around when probability plays a role in decision making. Similarly, we also received a request for clarity from another respondent around the interrelationship between operational resilience and cyber resilience. The respondent considered that, with the focus of cyber resilience being protecting high risk data and infrastructure that pervades across a firm and not just through important business services, it may be challenging for cyber resilience teams to identify priorities.

Our response

Operational risk broadly refers to the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. Operational risk is an integral part of any risk management framework and is addressed in multiple regulatory requirements including Operational Continuity in Resolution, Business Continuity, ICAAPs, ILAAPs, Wind Down Plans, Recovery and Resolution Plans. Operational risk management supports both operational resilience and financial resilience but is managed in relation to a firm's risk appetite, ie the maximum amount a risk a firm is prepared to take. Our experience is that operational risk management has not been sufficient to ensure adequate operational resilience on its own because disruptions are inevitable. To be resilient, firms need to plan to be able to continue providing the services most relied on by customers and markets (important business services) during severe but plausible scenarios from the perspective that these disruptions have already happened (impact tolerance).

We consider that cyber resilience is complementary to operational resilience outcomes. Our operational resilience framework requires firms to take a holistic approach to their overall resilience. Teams which currently focus on cyber resilience may need to work with the relevant SMF to input into the firm's operational resilience program and identify priority areas. We understand that in some cases this could present a challenge for firms given existing infrastructure but consider that as their resilience program progresses firms should be able to identify how to align resources and collaborate across the two areas.

Use/handling of sensitive/personal data

7. As with the feedback relating to the need for important business service users to be 'identifiable', one respondent asked for clarity on how the application of 'sensitive' data fits with GDPR definitions of personal data or sensitive personal data and if we see any potential confusion or conflict for firms in applying the requirements.

Our response

As we stated in paragraph 2.21, firms should be able to recognise which of their consumer base use a certain important business service. This does not require the firm to identify individual consumers by name, or change existing requirements concerning the handling of customer data. We do not therefore consider that our definition of 'sensitive' data conflicts with the GDPR or DPA definitions.

Scope of the policy

8. One respondent reported that some firms had difficulty in interpreting scope of application based on different wording in the FCA/PRA CPs. For example, on third country branches, CP19/32: paragraph 1.4 does not refer to them explicitly and nor does the draft instrument (see SYSC 15A.1.1R), yet the CBA does. The respondent added that PRA CP29/19 Draft Supervisory Statement does not explicitly state third country branches are in scope.

Our response

We recognise that we should have been clearer in the CP, as to whether third country branches are in scope of these rules. They are not. However, in-scope UK firms operating third country branches may wish to voluntarily apply some or all of the requirements to these branches to ensure consistency of approach across the firm's operations. Moreover, certain FCA and PRA rules relevant to operational resilience apply to third country branches and did so even prior to publication of the CP. For example, the outsourcing rules in SYSC 8.

Consistency within our own rules

9. One respondent had some minor drafting suggestions to ensure consistency in the draft legislation regarding when firms must consider compliance. The respondent pointed out that our proposed SYSC 15A.2.2R(1) refers to a 'relevant' change, whereas SYSC 15A.4.1R(1) refers to a 'material' change. The respondent believed 'material' should be used throughout the rules. In relation to SYSC 15A.5.7R, the respondent suggested the word 'materially' be included before 'operational disruption'.

Our response

We agree with the drafting suggestions as set out in paragraph 9 above. We have changed both SYSC 15A.2.2R(1) and SYSC 15A.2.6R(1) to refer to a 'material' change in the context of important business services and the knock-on impact on the mapping exercise.

We consider that adding 'materially' ahead of 'operational disruption' at SYSC 15A.5.8R would limit the sort of disruptions captured by this rule. All operational disruptions impacting the firm in a similar way to those tested (severe but plausible scenarios) should be followed up with a lessons-learned exercise that allows the firm to identify weakness and act to improve its ability to effectively respond to, and recover from, future disruptions.

Annex 3
Abbreviations used in this paper

Abbreviation	Description
AR	appointed representative
BAU	Business as Usual
BCBS	Basel Committee on Banking Supervision
BCP	Business Continuity Planning
CBA	Cost Benefit Analysis
CEF	Critical Economic Functions
CP	Consultation Paper
DORA draft	Digital Operational Resilience Act
DP	Discussion Paper
DPA	Data Protection Act
EBA	European Banking Authority
EC	European Commission
EEA	European Economic Area
EMRs 2011	Electronic Money Regulations 2011
FCA	Financial Conduct Authority
FMI	Financial Market Infrastructure
FSMA	Financial Services and Markets Act 2000
GDPR	General Data Protection Regulation
ICAAP	Internal Capital Adequacy Assessment Process
ICARA	Internal Capital Adequacy and Risk Assessment
ILAAP	Internal Liquidity Adequacy Assessment Process

Abbreviation	Description
IOSCO	International Organization of Securities Commissions
OCIR	Operational Continuity in Resolution
PRA	Prudential Regulation Authority
PRIN	Principles for Businesses
PS	Policy Statement
PSD 2	Revised Payment Services Directive
PSRs 2017	Payments Services Regulations 2017
RIE	Recognised Investment Exchange
RRP	Recovery & Resolution Planning
SM&CR	Senior Managers & Certification Regime
SMF	Senior Management Function
SREP	Supervisory Review and Evaluation Process
SSB	Standard Setting Body
SYSC	Senior Management Arrangements, Systems and Controls (Handbook)
UK	United Kingdom

Appendix 1
Made rules (legal instrument)

OPERATIONAL RESILIENCE INSTRUMENT 2021

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);

(2) the following sections of the Act:

(a) section 139A (Guidance);
(b) section 247 (Trust scheme rules);
(c) section 261I (Contractual scheme rules); and

(3) regulation 6 of the Open-Ended Investment Company Regulations 2001 (SI 2001/1228);

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

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

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

(7) 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 31 March 2022.

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).

(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 2021.

By order of the Board
25 March 2021

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: (1) cause intolerable levels of harm to any one or more of the *firm's clients*; or (2) pose a 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 in addition to any other relevant metrics, reflecting the point at which any further disruption to the *important business service* could cause intolerable harm to any one or more of the *firm's clients* or pose a 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 and striking through indicates deleted 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) a *UK RIE*.

as set out in the text of that chapter.

…

1.4.1B G Apart from *SYSC* 12, *SYSC* 19A, *SYSC* 19D, *SYSC* 20 and *SYSC* 21 which are disapplied by *SYSC* 1.4.1AR, the other chapters of *SYSC* 11

to *SYSC* ~~17~~ 14 do not apply in relation to a *firm's* carrying on of *auction regulation bidding* because they only apply to an *insurer*. *SYSC* 18 provides guidance on the Public Interest Disclosure Act.

Actions for damages

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*; and

(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 This chapter does not apply to a *TP firm*, a *TA PI firm*, *TA RAISP firm* or a *TA EMI firm*.

15A.1.4 R This chapter does not apply to a *firm* which has its registered office (or, if it has no registered office, its head office) outside the *United Kingdom*.

15A.1.5 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.1.6 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*; and

(2) an investor in an *AIF*.

15A.1.7 R The requirements in this chapter apply with respect to:

(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 activities connected to the provision of *payment services* and to the issuing of *electronic money* (whether or not the activity of issuing *electronic money* is specified in article 9B of the *Regulated Activities Order*); and

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

15A.1.8 R Notwithstanding *SYSC* 15A.1.7R, where the requirements in this chapter apply to a *firm* only as a result of *SYSC* 15A.1.1R(3), the requirements only apply to the provision of *payment services* and the issuance of *electronic money* by the *firm*, and activities connected to the provision of *payment services* and to the issuing of *electronic money* (whether or not the activity of issuing *electronic money* is specified in article 9B of the *Regulated Activities Order*).

15A.1.9 R There is no territorial limitation on the application of this chapter.

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 material 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 any vulnerabilities that would make the *person* more susceptible to harm from a disruption;

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

(3) the time criticality for *clients* receiving the service;

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

(5) the 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 clients* or pose a risk to the soundness, stability or resilience of the *UK financial system* or the orderly operation of the financial markets;

(9) the potential to cause reputational damage to the *firm*, where this could harm the *firm's clients* 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) the 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 material 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 nature of the *client* base, including any vulnerabilities that would make the *person* more susceptible to harm from a disruption;

(2) the number of *clients* that may be adversely impacted and the nature of the impact;

(3) the potential financial loss to *clients*;

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

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

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

(8) the potential loss of functionality or access for *clients*;

(9) any potential loss of confidentiality, integrity or availability of data;

(10) the potential aggregate impact of disruptions to multiple *important business services*, in particular where such services rely on common operational resources as identified by the *firm's* mapping exercise under *SYSC* 15A.4.1R.

15A.2.8 G When setting its *impact tolerance*, a *firm* should 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 should generally not do so if this would put the *firm* in breach of another 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. Under certain circumstances, a *firm* may wish to resume a degraded service. This is usually only appropriate if having regard to the interest of the *firm's clients*, the soundness, stability and resilience of the *UK financial system* and the orderly operation of the financial markets, the benefits of resuming a degraded service outweigh the negatives of keeping the service unavailable until the issues have been fully remediated and the service is able to be fully restored to its pre-disruption levels.

15A.2.11 G Under *Principle* 11 (Relations with regulators), 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 strategies, processes 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.

15A.4.2 G Where a *firm* relies on a third party for the delivery of an *important business* service, we would expect the *firm* to have sufficient understanding of the people, processes, technology, facilities, and information that support the provision by the third party of its services to or on behalf of the *firm* so as to allow the *firm* to comply with its obligations under *SYSC* 15A.4.1R.

15A.4.3 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, to assess 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, 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 Where a *firm* relies on a third party for the delivery of its *important business services*, we would expect the *firm* to work with the third party to ensure the validity of the *firm's* scenario testing under *SYSC* 15A.5.3R. To the extent that the *firm* relies on the third party to carry out testing of the services provided by the third party to or on behalf of the *firm*, the *firm* should ensure the suitability of the methodologies, scenarios and considerations adopted by the third party in carrying out testing. The *firm* is ultimately responsible for the quality and accuracy of any testing carried out, whether by the *firm* or by a third party.

15A.5.6 G In carrying out the scenario testing, 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.5.7 R A *firm* must carry out the scenario testing:

(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 improvements made by the *firm* in response to a previous test; and

(3) in any event, on a regular basis.

Lessons learned

15A.5.8 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.5.9 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; and

(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.5.8R;

(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 *clients* 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; and

(3) ensure that their choice of communication method takes account of the circumstances, needs and vulnerabilities of their *clients* and other stakeholders.

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 10, after SYSC TP 9 (Updates to reflect CRD V). The text is not underlined.

TP 10 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
10.1	*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 31 March 2022, and in any event no later than 31 March 2025, it can remain within its *impact tolerance* for each *important business service* in the event of a severe but plausible disruption to its operations.	From 31 March 2022 to 31 March 2025	31 March 2022
10.2	*SYSC* 15A.4.1 and 15A.5.3	R	A *firm* is not required to have performed the mapping and testing exercises as required by the	From 31 March 2022 to 31 March 2025	31 March 2022

			provisions in column (2) to the full extent of sophistication by 31 March 2022. A *firm* is required to have carried out the mapping and testing exercises as required by the provisions in column (2) by 31 March 2022 to the extent necessary to identify important business services, set impact tolerances and to identify any vulnerabilities in its operational resilience. After that date, a *firm* must continue the mapping and testing exercises so that it is able to remain within its *impact tolerance* for each *important business service* as soon as reasonably practicable, and in any event no later than 31 March 2025.		

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	*SYSC* 15A (Operational resilience) sets out further provisions which are 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 Recognition requirements

…

2.5 Systems and controls, algorithmic trading and conflicts

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

Paragraph 3 – Systems and controls	
(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: 007562

12 Endeavour Square London E20 1JN
Telephone: +44 (0)20 7066 1000
Website: www.fca.org.uk