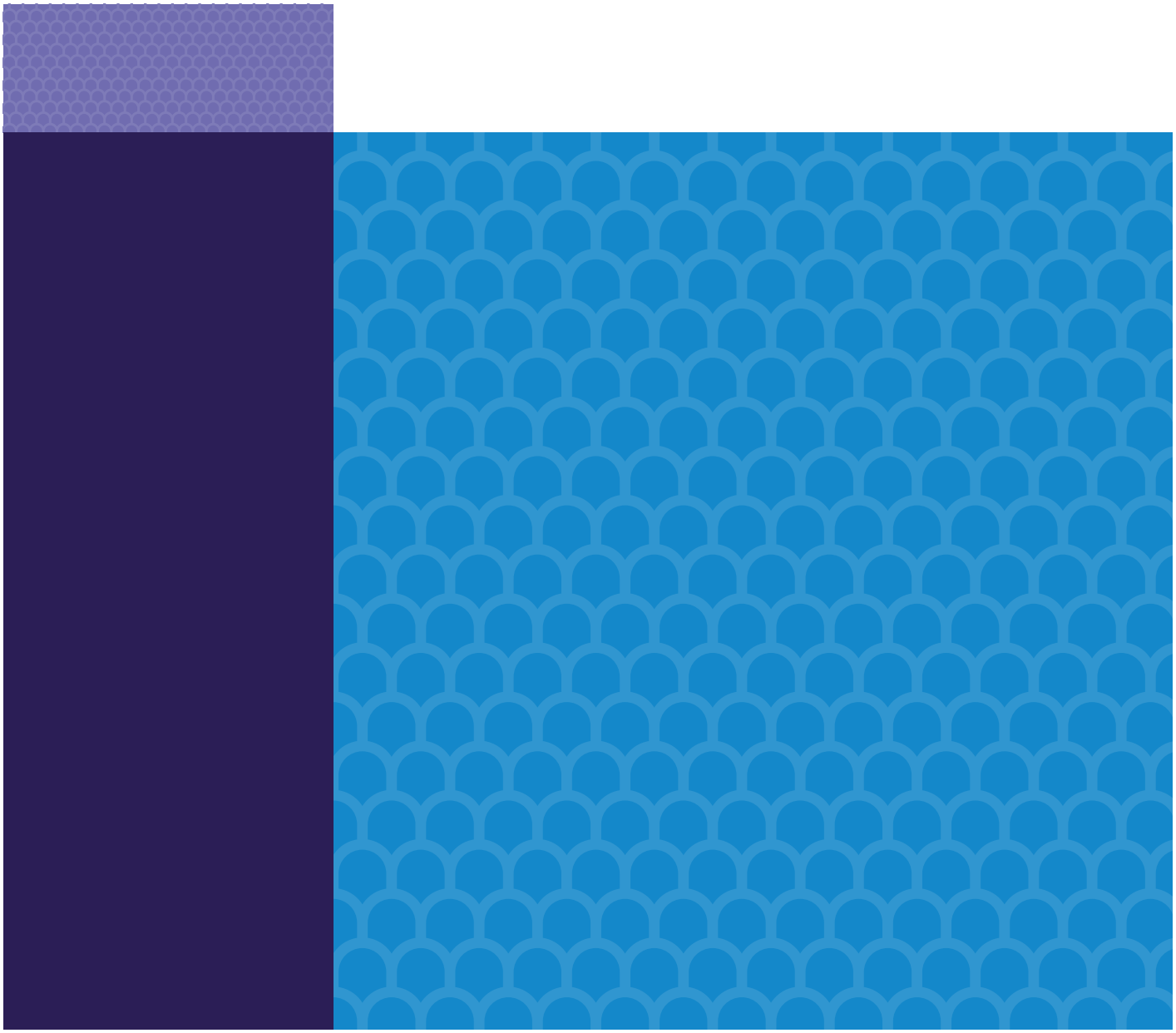
BANK OF ENGLAND

Financial Market Infrastructure

Policy Statement

Operational Resilience: Recognised Payment System Operators and Specified Service Providers

March 2021



BANK OF ENGLAND

Policy Statement

Operational Resilience: Recognised Payment System Operators and Specified Service Providers

March 2021

1 Overview

1.1 This Bank of England (the Bank) Policy Statement (PS) provides feedback to responses to the Consultation Paper Operational Resilience: Recognised Payment System Operators and Specified Service Providers. It also contains the Bank's final policy, as follows:

- Operational resilience section to the Code of Practice ("the Code"); and
- Final Supervisory Statement (SS).

1.2 This PS is relevant to the operators of payments systems recognised (RPSOs) under section 184 of the Banking Act 2009 (the Act) and specified service providers (SSPs) under section 206A of the Act.

Background

1.3 A key priority for the Bank, Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) ('the authorities') is to put in place a stronger regulatory framework to promote the operational resilience of firms and financial market infrastructures firms (FMIs). To this end, we published a joint Discussion Paper on Operational Resilience in 2018 setting out an approach to operational resilience. Following this, the authorities published a suite of consultation papers[1] (CPs) in December 2019 to consult on the policy approach.

1.4 The authorities sought views on a number of proposals which are designed to improve the operational resilience of firms and FMIs, and protect the wider financial sector and UK economy from the impact of operational disruptions. The proposals related to the identification of important business services, setting impact tolerances, and for ensuring firms' and FMIs' services can remain within impact tolerances in extreme but plausible scenarios.

Summary of Consultation Responses

1.5 The Bank has had regard to the representations made to the proposals set out in the Consultation Paper Operational Resilience: Recognised Payment System Operators and Specified Service Providers. There was an excellent level of engagement with the consultation. Overall, respondents were supportive of the policy and the approach to operational resilience, although there were some requests for additional clarity in any final policy. In developing the Bank's final approach, we have drawn upon these responses. The feedback received is summarised below:

i. **Disruption to multiple important business services** – A number of respondents stated that a disruption to an individual important business service may be unlikely to impact the authorities' objectives. Rather, disruptions that could impact multiple important business services simultaneously are more likely to pose a meaningful threat. We acknowledge these views and have amended the policy to include an expectation for RPOs and SSPs to consider that multiple important business services could be simultaneously impacted in the event of a disruption when setting their impact tolerances.

ii. **Third Party Outsourcing** – Respondents raised concerns over third party suppliers which may be reluctant to share information necessary for mapping and testing. The final policy does not prescribe that third party suppliers must disclose all (and sometimes sensitive) information to

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

RPSOs and SSPs, but RPSOs and SSPs will need to cooperate with their third party suppliers to assure themselves that they can remain within impact tolerances. The Bank will retain its approach to third party outsourcing and take a proportionate approach. For testing, evidence that RPSOs and SSPs have satisfied themselves that a third party has undertaken testing may be sufficient. While we recognise that some RPSOs and SSPs may struggle to negotiate mapping and testing arrangements with more significant third parties, the Bank considers that this clarification of RPSOs' and SSPs' expectations from suppliers will help suppliers understand the constraints they are operating under when agreeing contract terms, and thus improve the negotiations for RPSOs and SSPs.

iii. **Implementation timeline** – Respondents asked for greater clarity and consistency on the implementation timeline and suggest setting dates for implementing the new policy. Some respondents also inquired as to whether there would be flexibility within the timelines for implementation. Having considered the responses regarding the proposed implementation timeline, the Bank has decided to maintain it as proposed in the CP. The Bank considers it is critical that progress is made on operational resilience and for RPSOs and SSPs to prioritise their operational resilience as soon as reasonably possible. The Code comes into force on 31 March 2022 and requires RPSOs and SSPs to identify important business services, set appropriate impact tolerances and regularly test their ability to meet tolerances with due regard to the mapping of dependencies. RPSOs and SSPs would then, within a reasonable time but in any event no later than 31 March 2025, take all reasonable action to ensure they remain within impact tolerance for each important business service in the event of an extreme but plausible disruption.

iv. **Impact Tolerance** - Respondents commented that focusing on a single time-based metric for impact tolerance and requiring RPSOs and SSPs to stay within the time frame may not be possible and it may have an undesirable effect especially in circumstances of uncontrollable events such as a severe cyber-attack. The proposed policy is that RPSOs and SSPs consider a range of possible measures by which to judge the appropriate impact tolerance for a given important business service. Accordingly, the Bank does not consider it necessary to make changes to the proposed policy in this regard. The actions of RPSOs and SSPs in the event that an uncontrollable disruption occurs will depend on the circumstances.

v. **Defining extreme but plausible scenarios -** Respondents asked for greater clarity on the definition of 'extreme but plausible' scenarios, including a set of defined scenarios to support the development of effective testing and harmonised scenario planning programmes across the sector. The Bank expects RPSOs and SSPs to undertake an assessment of the operational risks that are relevant to their important business services and incorporate those risks in the design of disruption scenarios for the purpose of testing. The nature and severity of scenarios for RPSOs and SSPs to use may vary according to the risks and vulnerabilities identified. As such, the Bank does not consider that it would be helpful to provide a set of defined scenarios. The policy further provides a non-exhaustive list of the risks that RPSOs and SSPs may consider in designing their scenarios.

vi. **Documentation** - Respondents questioned the proportionality of requiring RPSOs and SSPs to prepare and regularly update a written record of the assessments they have undertaken to demonstrate how they met the operational resilience requirements. The Bank maintains that such a requirement helps RPSOs and SSPs assure themselves of their own compliance, provides the basis for them to take the necessary action(s) to address identified weaknesses in their resilience, and provides the necessary management information for senior management. RPSOs and SSPs should decide the appropriate frequency with which written records of assessments are updated.

vii. **Industry collaboration** - Respondents commented that the Financial Market Infrastructure sector should be encouraged to collaborate with other financial institutions and authorities in addressing issues such as industry preparedness for market-wide scenarios, approaches to setting and managing important business services, and the overall resilience of the UK financial sector. The Bank strongly agrees that this collaboration would be beneficial in establishing good practice for enhancing operational resilience and has emphasised this since the Discussion Paper.

Changes to draft policy

1.6 Financial stability is more likely to be impacted by a mass outage affecting multiple important business services, rather than individual important business service outages. The current drafting of the Code and SS requiring RPSOs and SSPs to set an impact tolerance for each important business service may be interpreted narrowly such that RPSOs and SSPs primarily focus on the disruption of single important business services and fail to consider their impact tolerance if multiple important business services are disrupted simultaneously. In the final Code and SS, we clarify that we expect RPSOs and SSPs to consider the implications for their impact tolerances should more than one important business service be disrupted at the same time.

1.7 The Bank has also taken the opportunity to make some typographical changes to the SS and the Code to improve readability.

1.8 The Bank considers that the above changes are not significant, and benefit RPSOs and SSPs by providing further clarity on the original proposals.

1.9 Prior to consultation, the Bank considered the way in which the Code and SS advances its statutory obligations and objectives. The Bank's findings on these issues are unchanged following consultation and consideration of the feedback received.

1.10 Appendix 1 contains a link to the final Supervisory Statement and the Code.

Appendix 1

1 **Supervisory Statement 'Operational Resilience: Recognised Payment Systems and Specified Service Providers' and the Operational resilience section to the Code of Practice**