November 2020

adm
RISK, REGULATION & STRATEGY LTD.
INSIGHT

What should firms be thinking about when designing an operational resilience framework?

Palvinder Gill
Insight Regulatory Consulting

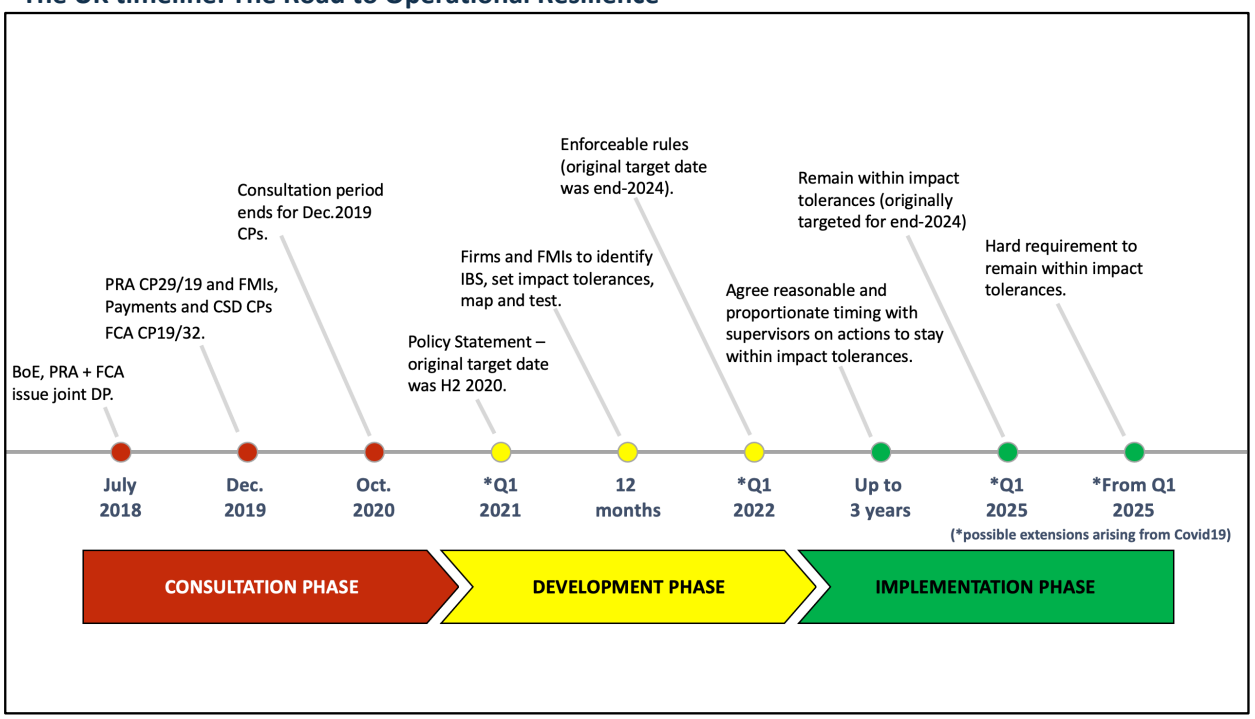
Anita Millar
ADM Risk, Regulatory & Strategy

Contents

Key messages

- **Don't delay.** While the UK is leading with a comprehensive and coherent regime on operational resilience, other jurisdictions will expect financial services firms (and particularly those of significant size) to adopt sound practices to strengthen their operational resilience to disruptions.
- **Get up to speed**. Educate board members, senior management and key individuals involved in delivering your operational resilience framework.
- **Choose and design your own tools wisely**. Before Covid-19, many jurisdictions focused on cyber threats to operational resilience, and this remains a key concern. Nonetheless, regulators are not endorsing, for example, any one cyber risk tool that a firm might deploy. Framework methodologies and metrics must be designed by the firm, and reflect its business and operational environment.
- **Coordination across multiple disciplines will be key, so choose your leader(s) wisely.** Regardless of jurisdiction, board and senior management accountability for operational resilience is a key theme. Under the UK regime, the PRA has suggested that the SMF 24 should lead.
- **Culture and people will be vital**. It will influence how a firm addresses issues ranging from leadership to its management of any unintended consequences that could emerge. Ultimately, firms will rely on their people to deliver operational resilience.
- **Avoid focusing on one source of disruption**. For example, firms focused on cyber risks or IT failure could overlook how other disruptions (no matter the source) could impact the promises they make to their end-clients (e.g. in terms of contracts, service levels and marketing) and promises they make to their regulator (in exchange for their license such as attestations). The focus should be on delivering services and keeping those promises.

The UK timeline: The Road to Operational Resilience



Introduction

1. In November 2020, we were invited to present our summary and analysis of the incoming operational resilience regime first proposed by the Bank of England (BOE), Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) in July 2018 with the publication of a joint discussion paper Building the UK financial sector's operational resilience.

2. During these webinars participants asked several questions and/or made several observations that we explore in this article.

3. By way of background, the July 2018 discussion paper was followed by the December 2019 publication of three separate BOE consultations on the application of this new regime to Central Counterparties (CPPs), Central Securities Depositories (CSDs), Recognised Payment System Operators and Specified Service Providers. In parallel, the PRA and FCA issued one each, respectively CP29/19 and CP19/32.

4. Final policy statements from the BOE, PRA and FCA are now expected in Q1 2021. A time that, with the emergence of plausible Covid-19 vaccines, should coincide with boards and senior management emerging from the experience of managing their financial service firms through a pandemic and looking forward to an increasingly more certain and normal environment.

5. While some financial services firms might believe their response to Covid-19 has been successful and proof of their resilience, in a 6 November 2020 speech by Nick Strange the BOE warned that financial service firms should not rest on their Covid-19 laurels. In fact, the source of the next disruption might look very different from Covid-19, in the same way that Covid-19 is different to the disruptions that preceded it. Hence, the case for UK financial services firms to implement operational resilience frameworks that:
    - Actively anticipate a disruption crystallising;
    - Identifies important business services in terms of the statutory objectives of all three regulators;
    - Considers the impact of a disruption to an important business service on end-users (retail and wholesale) in terms of its duration and when it becomes intolerable to end-users; and
    - Requires firms to actively think about how they respond to and recover from disruptions.

6. The questions and observations that emerged over the webinar were broadly concerned with:
    - Regulatory motivations and the UK's proposed regime versus those in other jurisdictions;
    - The organisational challenges from "who leads" to the potential "skills gap";
    - The tools, methodologies and approaches available; and
    - Unintended consequences for decentralised models/networks and small suppliers.

7. Whilst we don't have all the answers to these questions, we take this opportunity to provide further context and comments with: (i) a view to promoting an open discussion; and (ii) understanding that these may be overtaken by the upcoming BOE/PRA/FCA policy statements.

Regulatory motivations and the UK's proposed regime versus those in other jurisdictions

8. First, many regulators were looking at the question of the operational resilience of financial services firms before Covid-19. Much of this work was focused on the challenges presented by the adoption of new technologies in banking along with increased cyber and technology risks. Examples of this include the:
    - Financial Stability Board consultation paper *Effective Practices for Cyber Incidence Response and Recovery* (Apr 2020); and *Cyber Incidence Response and Recovery: Overview of Responses to the Public Consultation* (Oct 2020);
    - European Central Bank guidance *Cyber resilience oversight expectations for financial market infrastructures* (Dec 2018);
    - European Banking Authority *Guidelines on ICT and security risk management* (consultation December 2018 and final rules Nov 2019); and,
    - Monetary Authority of Singapore consultations on *Proposed Revisions to Guidelines on Business Continuity Management* (Mar 2019) and *Technology Risk Management Guidelines* (Mar 2019).
9. In comparison, the breadth and depth of the proposed UK regime is ambitious — owing to the UK experience with events such as the TSB 2018 disruption as documented in the UK Parliamentary 2019-20 report on IT failures. It is clear that UK regulators have been thinking about operational resilience for a while and elements of the UK regime appear to have influenced recent policy developments outside the UK.
10. Two recent publications of note are the Basel Committee on Banking Supervisions (BCBS) consultation on *Principles for operational resilience* (Aug 2020) and the (Oct 2020) US interagency paper on *Sound Practices to Strengthen Operational Resilience* (as prepared by the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation).
11. The following table provides an overview of how the UK regime compares to that proposed by the BCBS and the US interagency paper.

Regulatory motivations and the UK's proposed regime versus those in other jurisdictions

Overview of Policy Frameworks addressing Operational Resilience			
Key elements	**UK proposal**	**Basel Committee proposal**	**US summary**
Definition of Operational Resilience	The ability of firms and the financial sector as a whole to prevent, adapt, respond to, recover, and learn from operational disruptions.	The ability of a bank to deliver critical operations through disruption. This ability enables a bank to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from disruptive events in order to minimise their impact on the delivery of critical operations through disruption. In considering its operational resilience, a bank should take into account its overall risk appetite, risk capacity and risk profile.	The ability to deliver operations, including critical operations and core business lines, through a disruption from any hazard. It is the outcome of effective operational risk management combined with sufficient financial and operational resources to prepare, adapt, withstand, and recover from disruptions.
Relevant business focus	The **Important Business Services** (IBSs) delivered to external users (retail and wholesale) of the service. Each IBS is to be viewed through the chain of activities that make it up (from the taking up of the service to those part of the chain critical to its delivery). The level of granularity at which IBSs are defined should support the remaining elements of a resilience framework.	**Critical operations** is based on the Joint Forum's 2006 high-level principles for business continuity. It encompasses the **critical functions** as defined by the FSB as "activities performed for third parties where failure would lead to the disruption of services that are vital for the functioning of the real economy and for financial stability due to the banking group's size or market share, external or internal interconnectedness, complexity and cross-border activities".	**Critical operations** (including associated services, functions, and support) the failure or discontinuance of which could pose a threat to the financial stability of the USA. **Core business lines** (including associated operations, services, functions, and support) that in the view of the firm, upon failure would result in a material loss of revenue, profit, or franchise value.
Reference to relevant regulator's statutory objectives	The statutory objectives (of all three UK financial services regulators) are pivotal to identifying important business: **financial stability, safety & soundness of firms, secure insurance protection, consumer protection, market integrity, and effective competition**.	**Financial stability** is a linked to critical functions (which are encompassed by critical operations).	With the US regime aimed at the largest and most complex financial services firms, **financial stability** is the statutory objective driving the identification of critical functions.

Regulatory motivations and the UK's proposed regime versus those in other jurisdictions

Overview of Policy Frameworks addressing Operational Resilience			
Key elements	**UK proposal**	**Basel Committee proposal**	**US summary**
Key metrics	**Impact tolerance** assumes a **disruption crystallises** and is primarily a **duration metric**. It assesses the amount of time for which a single disruption to an important business service is tolerable to a financial services firm's end-clients.	**Risk tolerance for disruption** taking into consideration risk appetite, risk capacity and risk profile.	In setting the firm's risk appetite, the board of directors articulates the firm's **tolerance for disruption** considering its risk profile and capabilities of its supporting operational environment.
Relationship to related internal frameworks, capabilities, mapping and testing	**Operational risk management, business continuity and outsourcing / third party risk management** are treated as capabilities. However, the UK regime does not appear to exclude other capabilities — such as the Operational Continuity in Resolution (OCIR) — and the need to harmonise them. **Mapping** of the resources used to deliver an IBS. **Sensitivity analysis and scenario analysis** are required, based on severe and plausible scenarios.	Banks are expected to "leverage their respective functions for the **management of operational risk**". It is also expected that **business continuity planning** aids the identification of critical operations and key dependencies in the assessment of risks and the potential impact of various disruption scenarios. Business continuity and contingency planning are also to be considered in relation to the **failure or disruption at a third-party provider** that impacts the bank's critical functions. Information and communications technology (ICT) and cyber security are also covered. **Mapping** of relevant internal and external interconnections and interdependencies needed to deliver critical operations (including those dependent on third parties). **Testing** of the bank's ability to deliver critical operations through disruptions. **Severe but plausible disruptions to be considered**.	**Operational risk and business continuity management** anchor the sound practices, informed by **rigorous scenario analysis** and consideration of third-party risks (particularly in relation to outsourcing). **Scenario analysis** to help firms develop, calibrate and validate their tolerance for disruption. Firms may integrate their analysis with disaster recovery and business continuity management. Includes an **annex on sound practices for cyber risk.**
Governance and leadership	The Board and senior management have explicit responsibilities. The PRA singles out the **Senior Management Function (SMF) 24** (i.e. Chief Operations role) or similar should hold overall responsibility for implementing operational resilience policies and reporting to the Board.	The Board and senior management have explicit responsibilities.	The Board and senior management have explicit responsibilities.

Regulatory motivations and the UK's proposed regime versus those in other jurisdictions

12. While the US interagency paper brings together rules and guidance already in existence for various US financial institutions, its aim is clearly to promote a comprehensive approach to operational resilience, particularly in relation to critical operations and core business lines. What is unclear is the speed at which US supervisors will enforce these rules and promote the development of operational resilience frameworks.

13. Like the BCBS proposal, the US paper looks at identifying "critical operations" (as well as "core business lines") through the lens of the threat a disruption might pose to financial stability.

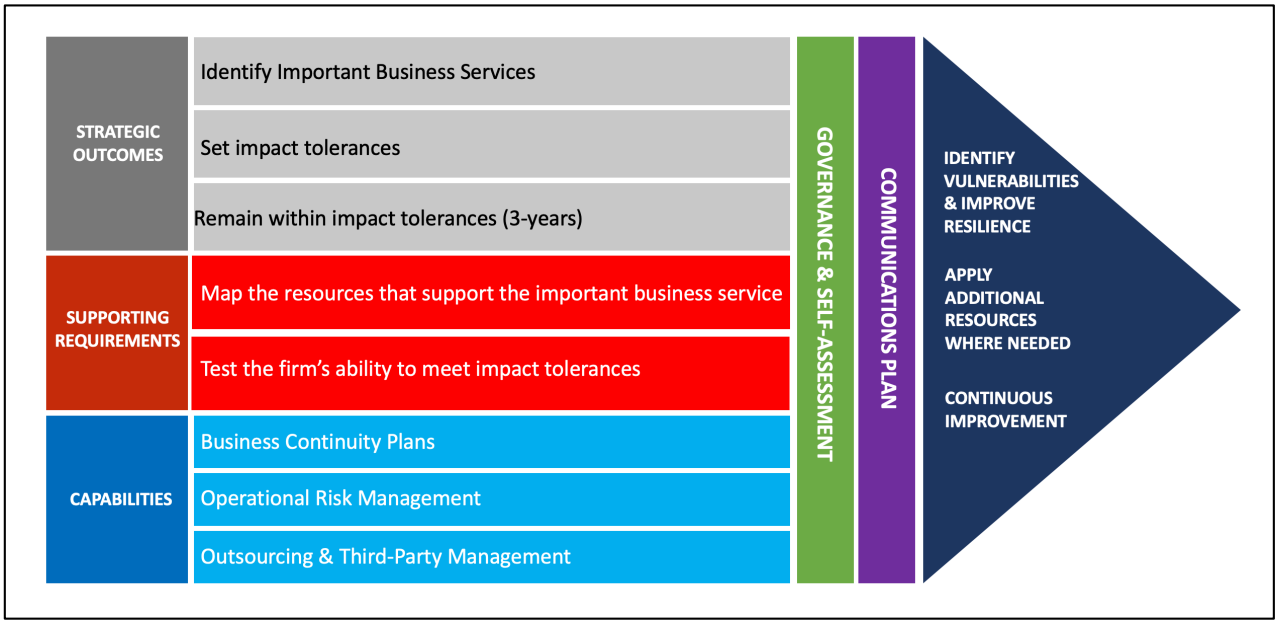
14. This sits in contrast to the UK regime which looks over a wider set of statutory objectives (including those of the FCA and PRA as well as the BOE) and links these to the impact of a disruption to a firm's services to consumers, financial markets and the UK financial system. The identification of which business services are important is the cornerstone of the regime, as is the setting of impact tolerances, which if exceeded, identify when a duration of a disruption is intolerable to the firm's external users (retail or wholesale). In essence, the UK regime aims to shift the UK financial services industry's focus from commercial interests to one informed by the public interest. It also shifts the focus away from individual systems and resources, so away from silos to the business services that cross and connect with these systems and resources.

15. Neither the proposed BCBS standard nor the US interagency report go as far as the UK's proposals. It is not just a question of language, both remain focused on the firm's financial interests and have not fully differentiated operational resilience from operational risk. Moreover, a "risk tolerance" normally varies both with the likelihood of an event occurring and its possible impact. In contrast, an "impact tolerance" is independent of likelihood and assumes an event occurs.

16. Nonetheless, the BCBS proposal has not been finalised and the US rules and guidance may evolve with the proposed BCBS standard and developments in the UK and elsewhere. Moreover, despite their differences, the direction of all these regulatory initiatives is the same: **supervisors will be expecting firms to be able to discuss, in a coherent and structured fashion, how they respond and recover from operational disruptions on an ongoing basis**.

17. Anecdotally, the results of an informal poll taken during the zyen/FS Club webinar indicates that webinar participants, directly affected by the UK regime, have understood this and started to think about the new requirements, to assess key metrics and appoint a team and senior manager.

Key Elements of the UK Operational Resilience Framework



The organisational challenges from "who leads" to the potential "skills gap"

18. A firm's operational resilience framework will clearly have multiple dimensions. Firms must map the resources used to deliver important business services. These are to be viewed as a chain of activities which, to varying degrees, intersect with risks, controls and processes instigated, monitored and assessed by multiple internal functions.

19. Leading this complexity will be a significant task and require individuals with an understanding of the firm's business, its operations and how it connects to the wider market infrastructure — from central clearing, to custodial services, to payments. The firm will also need to develop an internal and external communications strategy, a self-assessment methodology, along with mapping and testing capabilities.

20. The UK regulators have suggested that the senior management function (SMF) 24, i.e. the head of operations/chief operations officer (COO), should have overall responsibility for implementing operational resilience policies and reporting to the board. Where this function is split between two or more individuals, it is expected that it accurately reflects the firm's organisational structure and that comprehensive responsibility for operations and technology is not undermined. Where the SMF24 function is split, the PRA does not expect it to be split among more than three individuals.

21. Even where the SMF24 function is split, developing and implementing a firm's operational resilience framework will require individuals with an array of skills that can work together to, for example, identify important business services, determine impact tolerances and develop testing methodologies. Bringing together and developing these skills means that there is likely to be a skills gap, at least in the first instance, including at the most senior levels.

22. Anecdotally, the results of a second poll taken during the zyen/FS Club webinar indicates that webinar participants, directly affected by the UK regime, more frequently appoint the COO (or similar) over heads of finance, business continuity or operational risk.

23. Operational resilience is dynamic and will change with the operational challenges faced by firms. Consequently, the skills required to support the framework will evolve with the framework and the dataset that supports it.

24. This question of a possible skills gap, and whether it might be related to technology, leadership or other attributes, was one of the issues raised during one of the webinars we held in November 2020. No doubt where firms are lacking these skills, regulators will require that they be addressed.

25. The knowledge to implement an operational resilience framework exists in different areas of a firm. In order to be successful, firms will need to ensure that they identify internal expertise and successfully deploy it alongside any external experts.

The available tools, methodologies and approaches

26. In relation to questions concerning the tools available to firms, firms will inevitably seek to leverage the tools, methodologies and approaches already on hand, such as Risk & Control Self-Assessment (RCSA) processes, business continuity and cyber-resilience. For instance, during the course of the webinars we were asked about the applicability of the US Department of Commerce National Institute for Standards and Technology (NIST) framework for Cyber risk; or the possible use of Banking Industry Architecture Network (BIAN) as a starting point for identifying important business services. The answer to these questions depends on the firm, the nature of its business, and its operating environment. These approaches are already being used in some firms; so the key questions are whether they are effective, and how they might need to be modified for the purposes of a firm's operational resilience framework.

27. In regard to cyber risk management (a capability in the parlance of the UK regime), NIST is mentioned as one of several tools identified in Appendix A of the US interagency paper on operational resilience. While we cannot comment on the possible applicability of BIAN, it is possible to respond to the question of standardised taxonomies for the identification of important business services. The UK regulators are keen for firms to identify these services for themselves. As such, important business services should reflect the intersection of promises a firm makes to its end-clients and those it makes to its regulator(s) in exchange for its license.

28. Nonetheless, industry requests for guidance and some standardisation is likely to continue. It is not inconceivable that some of the industry trade associations may act as a forum where firms might discuss whether any standardisation is possible. However, the most resilient firms will have a competitive advantage and firms may not wish to invest time in such an effort without knowing how industry standardisation efforts might be received.

Unintended consequences for decentralised models/networks

29. The final set of questions and observations raised over the webinars concerned the unintended consequences of the new regime. These included whether this regime could prompt financial services firms to:
    - Scale back unprofitable business services;
    - Curtail direct relationships with newer/smaller technology providers; and
    - Build centralised systems that undermine the resilience associated with decentralised self-reliant and independent self-sufficiency (e.g. where big ships have many small life boats).
30. These concerns and observations all have merit. How firms address them will be reflected in the design of their operational resilience frameworks, the nature of their business, and the culture of the firm.
31. For instance, a firm that values coordination and decentralisation may be able to build a highly functional resilient framework that allows business to operate in a decentralised fashion. The culture of the firm will also help to determine how it approaches unprofitable business services, in view of the customers it serves, and manages its relationship with technology providers.

What to do now?

32. The UK regulators will publish their policy statements in Q1 2021, which will trigger the requirement for all firms in scope to design their operational resilience frameworks over the course of the following 12-months.
33. It is important that firms educate themselves and agree internally what operational resilience means for them. This will allow firms to identify the key people who will then deliver the framework.
34. Getting these foundations right will help to ensure successful project design and implementation.

Get in touch

Anita.Millar@ADMADVISORY.com
+ 44 (0)7770-844226

Palvinder.Gill@Insight-Regulatory.com
+44 (0)7811-371884