greyspark partners

ITRS GROUP

Operational Resilience Regulation

Why Multinationals Must Take a Group-wide Approach

Operational Resilience Regulation

Why Multinationals Must Take a Group-wide Approach

Since 2008, economic shock after shock focused regulators on initiatives to shore up the overall resilience of financial firms and reduce the impact of systemic interdependencies. Regulation dedicated to ensuring firms had sufficient capital requirements and were able to report their activities appropriately took much of the industry's attention. However, even prior to the onset of the Covid pandemic, regulators had begun to focus on the thorny issue of how to bolster firms' operational resilience. Regulators and standards setters in various regions began laying out what is expected of firms in respect to their operational resilience policies and processes, and significant progress has since been made over the last three years. While that progress is mostly consistent from region to region, divergence can be an issue for firms that operate across multiple regulatory jurisdictions. The significant degree of regulatory activity relating to operational resilience in the first half of 2022 is a call to action for firms to update – or create – their operational resilience practices and policies.

The globally integrated financial world with its cross-border service delivery interdependencies, means that the resilience of a firm's services in one jurisdiction may depend heavily on the supporting assets or processes located in other jurisdictions where regulation may differ. Assessing the feasibility of a multi-jurisdictional approach to operational resilience requires firms to understand the full extent of the demands that these emerging region-specific regulatory requirements will place on them and the consequential impact that the requirements will have on their strategies and business models.

Regulatory authorities in Australia, the EU, Hong Kong, Singapore, the UK and the US, as well as the Basel Committee on Banking Supervision (BCBS), have all published perspectives (see **Figure 1**) over the last three years. The good news for multi-jurisdictional firms is that perspectives from the Australian Securities and Investments Commission (ASIC), Monetary Authority of Singapore (MAS) and Hong Kong Monetary Authority (HKMA) guidelines and the UK are finalised, and they all demonstrate a convergence in the approach they are taking towards operational resilience; greatly benefiting firms building a globally consistent operational resilience framework. However, despite the overall convergence, regulation in key jurisdictions differs in the detail from region to region in important ways. This article explores the similarities and differences in operational resilience regulation to help firms navigate the challenges of building multi-jurisdictional operational resilience policies and processes.

Figure 1: Current & Next Steps for Key Operational Resilience Regulation / Standards Across Seven Key Jurisdictions

Source: BCBS, ASIC, EC, FCA, HKMA, OCC, MAS and GreySpark analysis

Jurisdiction	Regulating Entity	Relevant Documents	Current State	Next Steps
Global	Basel Committee on Banking Supervision (BCBS)	Principles for Operational Resilience[1] Published: March 2021	A 2021-22 work programme focused on the insights and supervisory approaches to operational resilience, with a particular focus on cyber security.	No further details have been provided yet.
Australia	Australian Securities and Investments Commission (ASIC)	ASIC's Consultation Paper 314: Market Integrity Rules for Technological and Operational Resilience[2] Published: June 2019	In March 2022, ASIC released a report that highlights the key issues that arose out of the submissions received on the Consultation Paper 314 and detail the regulators' response to those issues.	The new technological and operational resilience rules commence on 10 March 2023.
EU	European Commission (EC)	Proposal for a Regulation of the European Parliament and of the Council on Digital Operational Resilience for the Financial Sector and Amending Regulations (EC)[3] Published: September 2020	The finalisation of the EU's Digital Operational Resilience Act (DORA) is expected in the latter half of 2022. Negotiations on DORA are well underway, and the final shape of the legislation is becoming clearer.	The DORA rules are likely to be implemented over 24 months, after the finalisation of the revised DORA text.
HK	Hong Kong Monetary Authority (HKMA)	Supervisory Policy Manual OR-2 Operational Resilience V.1 - Consultation[4] Published: December 2021	The HKMA finalised its new Supervisory Policy Manual module on operational resilience and the revised version of its module on business continuity planning (BCP).	The HKMA expects every Authorized Institution (AI)[5] to have developed its operational resilience framework by May 2023.
Singapore	Monetary Authority of Singapore (MAS)	Guidelines on Business Continuity Management[6] Published: June 2022	In June 2022, the Monetary Authority of Singapore (MAS) issued revised guidelines on business continuity management for financial institutions.	No further details have been provided about the implementation of the guidelines taking place.
UK	• Bank of England (BoE) • Prudential Regulation Authority (PRA) • Financial Conduct Authority (FCA)	Building Operational Resilience: Feedback to CP19/32 and Final Rules Policy Statement PS21/3[7] Published: March 2021	The regulators noted that UK firms made meaningful progress in developing their operational resilience capabilities ahead of the first deadline in March 2022.	The deadline for the full implementation of all aspects of the policy is March 2025. By this date, firms must have proactively developed and progressed their approaches to mapping and testing.
US	• Federal Reserve Bank • Federal Deposit Insurance Corporation • Office of the Comptroller of the Currency	Sound Practices to Strengthen Operational Resilience[8] Published: October 2020	A joint agency paper published in 2020 sets out sound practices for operational resilience drawn from existing regulations, guidance and statements.	Although the timetable has not yet been decided, the paper requests continued public dialogue to help the agencies refine their approach.

[1] Basel Committee on Banking Supervision, 2021. *Principles for Operational Resilience.* [pdf] Available at: <https://www.bis.org/bcbs/publ/d516.pdf>.
[2] Australian Securities and Investments Commission, 2019. *Consultation Paper 314: Market Integrity Rules for Technological and Operational Resilience.* [pdf] Available at: <https://download.asic.gov.au/media/5169120/cp314-published-27-june-2019.pdf>.
[3] European Commission, 2020. *Proposal for a Regulation of the European Parliament and of the Council on Digital Operational Resilience for the Financial Sector and Amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014.* [pdf] Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0595&from=EN>.
[4] Hong Kong Monetary Authority, 2019. *Supervisory Policy Manual OR-2 Operational Resilience V.1 – Consultation.* [online] Available at: <https://www.hkma.gov.hk/media/SPM_module_OR-2_Consultation_(20211222).pdf>.
[5] An Authorized Institution (AI) is an institution authorised under the HKMA Banking Ordinance to carry on the business of taking deposits.
[6] Monetary Authority of Singapore, 2022. *Guidelines on Business Continuity Management.* [pdf] Available at: < https://www.mas.gov.sg/regulation/guidelines/guidelines-on-business-continuity-management>.
[7] Financial Conduct Authority, 2021. *Building Operational Resilience: Feedback to CP19/32 and Final Rules.* [pdf] Available at: <https://www.fca.org.uk/publication/policy/ps21-3-operational-resilience.pdf>.
[8] The Office of the Comptroller of the Currency, 2020. *Sound Practices to Strengthen Operational Resilience.* [pdf] Available at: <https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-144a.pdf>.

Operational Resilience Principles by Jurisdiction

The regulators, regardless of their specific supervisory requirements or definitions, are all aiming to create a financial services sector that is resilient to operational disruption. Rather than demonstrating divergence of intent, many differences arise from either how the regulation has evolved or is simply a manifestation of the way the jurisdiction has chosen to codify the concepts. The most fundamental differences arise in the definitions used by regulators and regional differences must be understood if firms are to develop successful cross-jurisdictional operational resilience frameworks. Evolving an informed understanding of whether a difference is minor or critical is key.[9] **Figure 2** compares the most recent publications on operational resilience for the seven regulatory jurisdictions (detailed in **Figure 1**) across five key concepts, highlighting areas of divergence.

Figure 2: Differences and Similarities in the Approach Taken by the UK to Operational Resilience Principles

Source: BCBS, ASIC, EC, HKMA, MAS, FCA, OCC and GreySpark analysis

Principles	Similarities in Jurisdictional Approach to UK						Divergence / Convergence
	Global (BCBS)	Australia	EU	Hong Kong	Singapore	US	
Prioritisation of Services					✓		Critical divergence
Impact Tolerances				✓			Critical divergence
Mapping	✓	✓	✓	✓	✓	✓	Convergence
Testing	✓	✓	✓	✓	✓	✓	Convergence
Governance & Oversight	✓	✓	✓	✓	✓	✓	Minor divergence

The five operational concepts shown in **Figure 2** are common across all seven jurisdictions, but they are not uniformly interpreted in the regulatory documentation, and the subtle nuances are vitally important for multi-jurisdictional firms. The following is an assessment of each of these five broad concepts:

- **Prioritisation of Services**
  Although, most of the regulatory jurisdictions take the prioritisation of services into account, there is a *critical difference* in the way regulators define an 'important business service.' Whilst the UK and Singapore explicitly factor in the customer into their definitions, the BCBS, HKMA and US agencies do not, which leaves a material gap in their operational resilience regulatory frameworks. The EU and Australia, on the other hand, mainly focus on the identification of technology systems rather than business services. GreySpark Partners has observed that many UK financial institutions are already well into the conceptual phase of building a customer-centric resilience plan to help them address future issues before the impacts are felt and customers experience disruption to services.

- **Impact Tolerances**
  There is a *critical difference* in the approach taken regarding impact tolerances between the regulatory jurisdictions. The BCBS and US agencies avoid the concept of 'impact tolerances' and instead rely on firms adapting their existing risk appetite and their 'tolerance for disruption.' However, the UK agencies and HKMA view impact tolerances as a cornerstone of their approach and stress that impact tolerances are not the same as risk appetite metrics. ASIC and MAS offer no guidelines for 'impact tolerances,' however MAS does define a similar concept, 'Service Recovery Time Objective,' which is a metric to assess the amount of time a business has to restore its services to an acceptable level after a disruption. There is a very real risk of getting lost in the detail, however, and many firms are struggling with the calibrations and approach to the setting of impact tolerances. In GreySpark's view, firms should focus on developing impact tolerance statements that compare current and baseline data to support scenario stress testing and to identify operational gaps. Impact tolerance statements are a useful way of articulating clearly and concisely to boards and the regulators how firms have reached their impact tolerance conclusions.

[9] A *'critical difference'* is a significant gap identified in a specific regulatory policy that is already addressed in other regulatory standards. A *'minor difference'* is a subtle variation that is specifically mandated by the regulator for that jurisdiction, although the regulators share a common approach.

- **Mapping**
  The regulators in all seven jurisdictions require specific mapping of supporting resources. GreySpark has observed progress in this area, with many firms maintaining close to real-time mapping and are quickly reflecting any changes in how important business services are delivered. This is helping to highlight vulnerabilities in critical functions such as single points of failure, concentration and limited substitutability of resources.

- **Testing**
  The regulators in all seven jurisdictions agree on the value of testing to ensure that firms demonstrate the level of preparedness to not only remain within impact tolerances, but also to withstand and recover from operational disruptions. GreySpark is aware of many firms working on a testing programme and monitoring regime that can provide them with ongoing assurance that they are able to remain within impact tolerances.

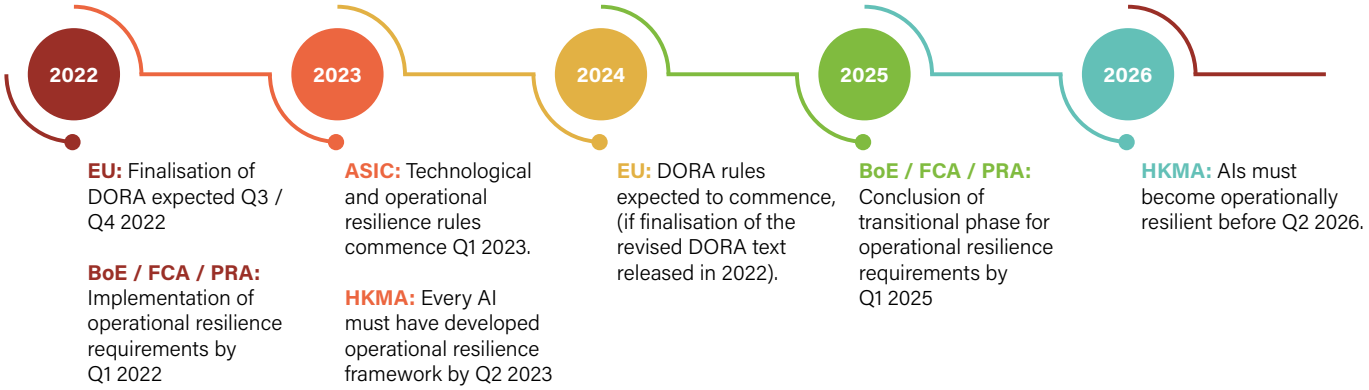
- **Governance & Oversight**
  The regulators in all seven jurisdictions place significant responsibility for operational resilience with the Board of Directors. However, there is a *minor difference* when it comes to the UK, because they place specific responsibility on the shoulders of the Chief Operations Function for the implementation of operational resilience policies. Although the other six jurisdictions have adopted, or are looking closely at, broad-based accountability frameworks, firms are starting to look to the use of clearer roles and responsibilities as a supervisory tool.

GreySpark believes that while there has been notable convergence in the concepts and principles being adopted in consultations and guidance released since 2019, not all regulatory fragmentation will be eliminated and important differences between jurisdictions will remain. Understanding the differences will make them more manageable for multi-jurisdictional firms and, after adjusting for the variation, firms will be able to take a global group-wide approach to operational resilience.

Although the regulatory work on operational resilience is complete in Australia, Hong Kong, Singapore and the UK, the industry is still awaiting the final views from the EU and the US, which may throw a last-minute spanner in the metaphorical works for the multi-jurisdictional approaches taken by early adopters. **Figure 3** shows regulatory milestones and deadlines relating to operational resilience over the next five years.

Figure 3: Deadlines for Operational Resilience Regulatory Milestones Across the Seven

Source: EC, ASIC, HKMA, FCA, GreySpark analysis



The Role of Technology in Operational Resilience Enhancement

While every firm with an 'important business service', as defined in operational resilience regulation, has an underlying IT component, there is a potential lack of focus on IT (it is treated as an 'internal service') in UK, Hong Kong, Singapore and the US regulation which could be problematic. The EU's DORA and ASIC's Consultation Paper on the other hand place greater emphasis on the role and impact of a firm's technology on its operational resiliency. GreySpark believes that for a firm to be operationally resilient its technology enterprise must be fit for purpose and able to provide real-time data to support business processes. However, this is certainly not the case in many instances.

Operational silos are one of the most well-known and common challenges that firms face in 2022. Typically resulting from legacy technology, business structure and jurisdictional expansion through acquisition, firms struggle to put in place cohesive policies and processes that can ensure the operational resilience of the business as a whole. The need for technological investment is vital in breaking operational disjointedness. Analysing cross-silo client usage patterns can help identify operational vulnerabilities and ensure uninterrupted service delivery when the firm experiences an internal or external crisis.

Achieving Group-wide Operational Resiliency

Financial institutions are more resilient to unexpected operational threats when they take a consistent group-wide approach based on an internationally agreed best practice. However, large operational burdens from overlapping or duplicative requirements put forward by different regulators, add significant complexity and hinder a successful outcome. For example, as noted by the European Commission, incident reporting requirements are insufficiently streamlined and use different terminology and timeframes across different regulatory jurisdictions and require different levels of detail. Consequently, there is a very real risk that internationally active firms will struggle to achieve 'resilience-by-design' and substitutability in their service provision. Given the cross-border service delivery interdependencies for financial firms today, the resilience of a firm's services in one jurisdiction will often depend on the supporting assets or processes located in other jurisdictions. Taking a group-wide approach to planning for operational resilience will give firms more opportunities to 'plug the gaps' between jurisdictional approaches and reconcile inconsistencies in a way that boosts operational efficiency and reduces costs. Cross-border firms should, therefore, consider adopting an international group-wide practice to assess the firm's policies and practices, even if local regulators only require some of their units to do so.