



Operational Resilience: Are You Ready and Seizing the Opportunities?

Financial services regulators have made it clear that operational resilience is now viewed with the same importance as prudential resilience. Financial services firms should be taking action to comply with new regulatory requirements relating to operational resilience. Are you doing enough to ensure compliance? Almost as importantly, are you maximising the opportunity to achieve a competitive advantage through operational resilience? If the answer to either of these questions is anything other than “yes”, there are steps you need to take now to change that.

Introduction

Operational resilience (“OR”) has been a key focus for global regulators in recent years. In the UK and European Union (“EU”), new OR regulations have been introduced. At the same time, regulators have readily applied sanctions to firms, and individuals, for failures in OR.¹ The deadlines for full implementation of the new UK and EU regulations regarding OR—March 2025 for the UK and January 2025 for the EU—are fast approaching. By then, firms must have fully tested their OR measures and embedded the people, processes and structures to operationalise them.

Experience suggests that, while many firms have taken steps towards compliance, the majority are not going far enough in building OR into the fabric of their company. Some may not have even fully met the existing requirements, for example, by defining key OR parameters to meet the UK requirements by March 2022.

This is concerning because operational disruptions harm consumers, firms and market integrity. Consumers

cannot access essential services. Firms cannot serve their customers. Trust in markets can be undermined.

What is more, sources of disruption to business operations are both proliferating and becoming more acute. While disruptive forces such as extreme weather, geopolitical events and pandemics are not new, today their impact has the potential to be far more severe because of climate change, globalisation and hyperconnectivity.

So why are some firms not yet taking OR seriously? Often, the problem is that they view it as a regulatory burden to be implemented through a “tick box” approach to compliance. This is bad business. It is far better to treat OR regulation as an opportunity to advance the interests of your customers and shareholders by avoiding disruptions, mitigating key risks and increasing process effectiveness.

¹ <https://www.dentons.com/en/insights/articles/2023/april/28/lessons-for-senior-managers-to-learn-from-tsb-it-migration-enforcement-action>

Key OR Regulations in the UK and EU

UK

In March 2021, following a consultation and review of proposals and feedback, the Financial Conduct Authority (“FCA”), in partnership with the Bank of England (“BoE”) and Prudential Regulation Authority (“PRA”), set out its final rules for OR in Policy Statement PS21/3.²

More recently, the Financial Services and Markets Act 2023 (“FSMA 2023”) granted His Majesty’s Treasury, the BoE, the PRA and the FCA powers to directly regulate critical third-party suppliers to financial services firms in order to further enhance OR. On 7 December 2023, a joint consultation was issued setting out the regulators’ proposals to implement these new powers, with more consultations promised in the near future.³

EU

On 16 January 2023, EU Regulation 2022/2554, or the Digital Operational Resilience Act (“DORA”), for the financial sector entered into force, providing a comprehensive framework aimed at strengthening the resilience of the financial sector against cyberattacks and other digital operational risks.

Scope

UK

The UK OR rules apply to a broad range of financial services firms, including those that fall under the enhanced-scope Senior Managers and Certification Regime, banks, designated investment firms, building societies, insurance firms (Solvency II firms), UK Recognised Investment Exchanges, electronic money institutions, payment institutions and recognised account information service providers.

FSMA 2023 also granted powers for the regulators to directly regulate critical third parties (see above).

EU

DORA applies to a wide range of authorised financial entities in the EU and, importantly, directly to information and communication technology (“ICT”) third-party service providers that provide services to financial entities in the EU and are deemed to be critical.

Key Requirements

UK

In the UK, firms are required to:

1. Identify important business services

“Important business services” refers to services provided by a firm that, if disrupted, could cause

intolerable levels of harm to one or more clients, or pose a risk to the soundness, stability or resilience of the UK financial system or orderly operation of financial markets. Internal services (e.g. legal or human resources) should not be classified as important business services unless they affect outcomes for, or services to, end users.

2. Set impact tolerances

For each identified important business service, firms must set an impact tolerance that is a maximum level of disruption reflecting the point at which further disruption could cause intolerable harm to one or more of the firm’s clients, or pose a risk to the soundness, stability or resilience of the UK financial system or orderly operation of financial markets.

3. Establish strategies, processes and systems

A firm must have in place sound, effective and comprehensive strategies, processes and systems to enable it to comply with its OR obligations.

4. Conduct mapping and scenario testing

Firms must identify and document the people, processes, technology, facilities and information necessary to deliver each important business service. The mapping should enable the firm to identify and remedy vulnerabilities.

Firms must also develop, and keep up to date, testing plans to appropriately detail how they will gain assurance that they can remain within impact tolerances set for important business services. Firms have to carry out testing to assess the ability to remain within impact tolerances for each important business service in the event of a severe but plausible disruption. For this purpose, they need to identify an appropriate range of adverse circumstances, considering the risks in those circumstances. Following scenario testing or in the event of operational disruption, firms must also conduct a “lessons learned” exercise to identify weaknesses and make the necessary improvements to address them.

5. Complete self-assessment, governance and communication

Firms must make, and keep up to date, written records of their compliance assessments and ensure that their governing bodies regularly review and approve these self-assessment records. Firms are also expected to maintain an internal and external communication strategy so that they can act quickly and effectively to reduce anticipated harm caused by operational disruptions.

² www.fca.org.uk/publication/policy/ps21-3-operational-resilience.pdf

³ <https://www.bankofengland.co.uk/prudential-regulation/publication/2023/december/operational-resilience-critical-third-parties-to-the-uk-financial-sector>

EU

DORA has requirements similar to the UK OR rules but is focused on ICT risks rather than broader OR risks, and in many places, it is more prescriptive with its requirements. It aims to establish a universal framework across EU member states. DORA separates digital OR into five categories:

1. ICT risk management

Financial entities must establish and maintain a risk management framework to identify, classify and mitigate ICT risks. This will include governance, policies, controls, risk assessments and mapping activities.

2. ICT incident management and reporting

Financial entities must establish a mechanism to detect and report significant ICT-related incidents to the relevant supervisory authority. The scope of this requirement goes beyond personal data breaches, which would be covered by the General Data Protection Regulation (“GDPR”).

3. Digital OR testing

Financial entities are expected to regularly test their ICT systems and processes to ensure resilience against disruptions. This testing must include vulnerability assessments and penetration testing.

4. Third-party risk management

Financial entities must manage and monitor their ICT third-party risk, including that from providers of cloud services and other critical services, ensuring they do not compromise the entity’s OR. This may require changes to the contracts in place with third-party technology providers and will extend beyond pure outsourcing, which would be covered by the European Banking Authority Outsourcing Guidelines.

5. Information sharing

The regulation encourages the sharing of cyber-threat information and intelligence among financial entities to improve collective resilience against cyber threats. In addition, DORA will establish an oversight framework for critical ICT third-party service providers, including the ability for relevant authorities to directly supervise these providers.



Operational resilience (“OR”) has been a key focus for global regulators in recent years.

Timing

UK

By 31 March 2022, firms should have identified important business services, set impact tolerances, and started mapping and scenario testing to identify OR vulnerabilities.

By 31 March 2025, mapping and testing should be completed, as should the planning of, investment in and execution of operational changes required to remain within set impact tolerances in the event of disruptions.

Firms must not wait for the hard deadline at the end of the transitional period to start preparing to remain within impact tolerances; the regulators expect that firms make reasonable effort to do so during the transitional period to avoid being in breach of the rules.

EU

DORA entered into force on 16 January 2023. Enforcement of DORA will commence on 17 January 2025.

How to Effectively Design and Integrate OR

With one year to go, time is now running short for firms to implement comprehensive compliance programmes to meet these requirements. So, what are the practical steps you can take now?

Define Accountability, Responsibility and Governance for OR

Firms should establish clear accountability and responsibility for operational resilience. OR oversight should be structured in the most effective way for their business, using existing committees and roles or establishing new ones if necessary. Among the most important stakeholders is the person responsible for the firm's OR policy implementation and reporting to the board, typically the chief operating officer for UK regulation⁴, the chief information officer may be more suitable to meet the EU regulation. This individual's role is pivotal in steering the organisation towards resilience and ensuring that OR policy not only is implemented but also becomes a part of the firm's DNA.

Also vital are the business leaders in charge of the activities that deliver important business services. They should be made aware of their responsibilities for establishing and maintaining the resilience of their activities. Their engagement is crucial in making OR a shared responsibility across the organisation.

Collectively, these stakeholders need to be able to demonstrate to the board that an integrated approach to OR is in place, that in each area there is effective business ownership, and that for each required activity,

an appropriate level of resources is maintained. This collaborative approach is essential for creating a resilient organisation where every stakeholder understands their role and responsibilities in maintaining OR.

It is vital to have effective governance and accurate and timely data to support and control OR, from establishing initial measures to steady state management and event-driven adaptation.

Optimise Your OR Organisational Model

A key element of effective ongoing OR is embedding the structures that promote good practice into business as usual ("BAU"). This means ensuring that there is sufficient capacity to execute all OR activities, not forgetting the need to maintain the approach, standardise measures across the organisation and monitor that activities are completed. This may require a reorganisation to allocate appropriate resources and hiring additional resources where there are any gaps in skills and expertise.

The organisational structures typically deployed for OR sit on a continuum of centralised, decentralised and hybrid models.

A **centralised model** puts the onus of almost all OR activity on a single function, typically in operations. This model can be attractive due to its simplicity; however, it can complicate the application of a firm-wide lens due to the complexity of co-ordinating specialisms that often operate in silos. It often leads to a focus on complying with minimum regulations (a "tick box" exercise) and may fail to maximise the long term stability of OR measures or business benefits (a "point-in-time" exercise). This model can severely complicate the coordination of the relevant resilience disciplines, such as cybersecurity, business continuity, technology and change management, and physical security.

A **decentralised model** may be more successful. It is possible, for example, to move all OR activity to the functional business teams with oversight and standards provided by the second line of defence. This approach encourages engagement from management and business units but risks OR practices diverging across an organisation, and complicating communication. It can impose additional administration and workload on often already stretched staff—an extra burden that may impact business performance and make it harder to demonstrate to the regulator that sufficient "horsepower" is available.

Often, an optimum solution lies in a **hybrid model** that combines the centralised and decentralised approaches and is carefully designed to suit the individual business and its established capabilities,

⁴ <https://www.bankofengland.co.uk/prudential-regulation/publication/2021/march/operational-resilience-impact-tolerances-for-important-business-services-ss>

capacity, systems and reporting structures. For example, business teams may execute some OR activities, e.g. IBS assessments, while a centralised team actively co-ordinates and/or assists to ensure effective execution and, potentially, informs the oversight activities of the second line. This hybrid approach can safeguard control, ownership and groupwide standardisation while still embedding OR into BAU. It provides a balance between centralised oversight and decentralised execution, ensuring that OR is both efficient and effective. This approach does, however, require formal governance and board support to incentivise the component parts to work together effectively.

Whatever structure your organisation selects, the objective should be to curate a culture in which OR is driven by executive leadership, understood and actively managed, as opposed to just ticking boxes to comply with the regulation.

Align OR to Your Other Risk and Regulatory Frameworks

To maximise business benefits and efficiencies in BAU, there should be a high level of interaction between OR and teams such as business continuity and disaster recovery planning, cybersecurity, third-party risk management, operational risk management and change management. This interaction should be underpinned by design of the OR framework to use and align to existing artefacts and frameworks.

For instance, OR scenario testing should be conducted and reported on by the team leading OR (e.g. Operations), but results and outcomes should be recorded in the operational risk register maintained by risk and thus inform associated risk function monitoring and reporting

of the company's risk profile. OR testing should also be coordinated with other related testing, e.g. crisis plan and recovery and resolution testing (where applicable). Finally, outputs of OR scenario testing should ideally form a vital input set to operational risk capital calculations being performed by the company's risk and capital modelling teams.

By designing OR frameworks to align with existing risk and capital frameworks, organisations can ensure a more streamlined and unified approach to risk management, avoiding silos, reducing rework and cost and enhancing overall risk awareness and response.

Optimise Your Change Capability

Effective OR requires both the ability to manage and monitor the steady state and the ability to adapt processes to changing external and internal circumstances. Organisations should be able to continuously adapt resources, processes, systems and frameworks, and the organisational structures used to manage and maintain OR.

Firms should build the capability to use change and operational excellence methodologies to implement and embed OR. Proactive management of the impacts of, for example, resource constraints, cultural shifts and evolving regulatory landscapes, is essential.

Continuous improvement is also vital. Long-term success depends on regular reviews and adaptations based on lessons learned from testing, as well as on industry best practices. This approach ensures that your organisation remains agile and responsive to change, maintaining its resilience in the face of evolving challenges and opportunities.



Maximising Business Benefits from OR

By adopting the approach to OR described above, firms can realise business benefits that go far beyond mere compliance – for example:



Cost savings: Service outages are very expensive. In addition to possible regulatory fines, contractual payments to customers may be required. Large sums may also be spent on a wide range of experts, including IT and reputation management consultants, and on legal fees. Effective OR minimises the cost of disruption to the firm and its customers, delivering substantial savings.



Resource optimisation: Aligned to cost savings arising from operational continuity, OR enables the effective prioritisation and allocation of resources, both financial and human. By adopting an OR-driven approach, resource deployment can be laser focused on where it is most needed to realise resilience uplifts.



Customer confidence: Disruptions reduce customer confidence and lead to higher levels of customer attrition. Customer acquisition is expensive and difficult. OR can improve customer retention, building stable revenue growth.



Investor confidence: Disruptions can reduce shareholder value. Investors will want management to evidence that everything possible was done to avoid and mitigate the disruption. Where investors lose confidence in a company's ability to avoid foreseeable disruptions, management will be held accountable.



Competitive advantage: Firms with robust OR can differentiate themselves in the market, especially in industries where customers value reliability and uninterrupted service. Higher service levels, reflecting a proven record, can become a key business development tool. Customers may also accept more relaxed contractual terms, with weaker remedies, when they have commercial confidence in the reputation of the counterparty. This helps to lower overall business risks.



Brand enhancement: Reliability and stability are key to enhancing the value of the goodwill in a business. Market recognition that a firm has effective OR can make it possible to charge a premium on business sales. Conversely, reputational damage from poorly handled disruptions can be immediate and permanent.

Next Steps

OR has emerged as a critical ingredient for a successful business strategy, transcending its roots in risk management.

Effective OR is not just about surviving; it is about thriving in the face of adversity. By embracing OR, firms can enhance their service continuity, protect their reputation, maintain customer trust and ultimately gain a competitive edge.

Preparing to tackle OR in this new way requires clear vision from the board and a concerted effort across all levels of an organisation. With a year to go before the OR regulations are fully enforced by regulators, business leaders, lawyers and compliance professionals urgently need to take a proactive role in ensuring their OR programme is on track and empowered to deliver the maximum business benefits.

Leadership commitment combined with a strategic, integrated approach will be key to transforming OR from a regulatory requirement into a core business strength.



SEBASTIAN SPRIGGS

FTI Consulting
Director
UK
sebastian.spriggs@fticonsulting.com



TRISTAN JONCKHEER

Dentons
Partner
UK
tristan.jonckheer@dentons.com

How Dentons and FTI Consulting Can Help

Dentons and FTI Consulting offer a range of services and tools that can help you develop your organisation's capability to meet the OR challenge. We use our host of frameworks, established methodologies and accelerators to quickly and effectively deliver your OR programme while transferring knowledge and capabilities to client teams. In particular, we can deliver:

- **Reviews:** We can review your third-party contracts, policies and procedures to deliver OR requirements and benefits.
- **Templates:** We can provide template documents which can be adapted and used in your OR programme.
- **Governance:** We can advise on how to implement governance arrangements that will be most effective at delivering OR throughout your organisation.
- **Audit/diagnostic:** We can assess your organisation to identify gaps in compliance and provide a scorecard of compliance with OR requirements.
- **Project management:** We can provide specialist project managers who can help deliver your OR programme on time and on budget.
- **Business transformation:** Our experts can support your organisation with the required transformation efforts needed to achieve desired OR outcomes. Our resilience specialists and deep subject matter experts can assist with closing the gap between current state and full compliance.

Together, Dentons and FTI Consulting can help you to achieve compliance with OR requirements quickly and efficiently, while at the same time delivering a tangible competitive advantage for your business.

© 2024 Dentons. Dentons is a global legal practice providing client services worldwide through its member firms and affiliates. This document has been provided to you for information purposes only and you may not rely on this document. This publication is not designed to provide legal or other advice or give rise to a solicitor/client relationship and you should not take, or refrain from taking, action based on its content. Dentons does not have any duty, liability or responsibility whatsoever to you of any sort, whether in contract, tort (including negligence) or otherwise in respect of this document and Dentons does not accept any such duty, liability or responsibility. Specialist legal advice should be taken in relation to specific circumstances. You agree not to make any claim of any sort against Dentons in connection with this document. This information is provided to you on the basis you agree to keep it confidential. Dentons UK and Middle East LLP is a limited liability partnership registered in England and Wales under no. OC322045. It is authorised and regulated by the Solicitors Regulation Authority and the Law Society of Scotland. A list of its members is open for inspection at its registered office: One Fleet Place, London EC4M 7WS. Any reference to a "partner" means a person who is a partner, member, consultant or employee with equivalent standing and qualifications in one of Dentons' affiliates. Please see [dentons.com](https://www.dentons.com) for Legal Notices.

The views expressed herein are those of the author(s) and not necessarily the views of FTI Consulting, Inc., its management, its subsidiaries, its affiliates, or its other professionals. FTI Consulting, Inc., including its subsidiaries and affiliates, is a consulting firm and is not a certified public accounting firm or a law firm.

FTI Consulting is an independent global business advisory firm dedicated to helping organisations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centres throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities. © 2024 FTI Consulting, Inc. All rights reserved. [fticonsulting.com](https://www.fticonsulting.com)

© 2024 Dentons and FTI Consulting LLP. All rights reserved.

