



Impact of FCA's Updated Operational Resilience Deadline on UK Compliance with DORA

UK Financial Institutions: Accelerated FCA Operational Resilience Deadline

Since 2017, the FCA has been preparing for the UK Operational Resilience Act, originally set for a March 2025 implementation. However, the deadline has been advanced to January 2025, surpassing the European Digital Operational Resilience Act (DORA) timeline.

STRENGTHENING STABILITY AND MITIGATING THIRD-PARTY RISKS

The Act aims to mitigate systemic risks posed by Critical Third Parties (CTPs) to the UK financial sector. It establishes stringent requirements to bolster the stability of financial institutions and safeguard against escalating cyber threats and other risks, ensuring third parties cannot undermine the sector's resilience.

DORA VS. FCA: KEY FOCUS AREAS

DORA prioritises ICT risk management, harmonising digital resilience and addressing cyber threats, IT failures, and incident reporting, particularly related to third parties. In contrast, the FCA's framework adopts a broader scope, covering both digital and non-digital disruptions, such as supply chain issues or extreme weather.



Key Requirements of the FCA Operational Resilience Act

- | | |
|--|---|
| <p>✔ IDENTIFY IMPORTANT BUSINESS SERVICES (IBS)</p> <p>Identify services whose disruption could harm consumers or market integrity.</p> | <p>✔ THIRD-PARTY RISK MANAGEMENT</p> <p>Assess and manage risks from outsourcing and third parties to ensure their resilience meets the firm's requirements.</p> |
| <p>✔ SET IMPACT TOLERANCES</p> <p>Define the maximum tolerable disruption level for each IBS, based on duration or other metrics (e.g., transaction volume).</p> | <p>✔ GOVERNANCE AND ACCOUNTABILITY</p> <p>Hold senior management and boards accountable for embedding operational resilience in the firm's strategy and oversight.</p> |
| <p>✔ MAPPING AND DEPENDENCIES</p> <p>Map processes, systems, people, and third parties supporting each IBS to identify dependencies and potential failure points.</p> | <p>✔ COMMUNICATION AND TRANSPARENCY</p> <p>Create a communication plan for disruptions to minimise harm and provide timely updates.</p> |
| <p>✔ SCENARIO TESTING</p> <p>Regularly test extreme scenarios, including cyberattacks, IT failures, and third-party outages, to assess impact tolerance.</p> | <p>✔ REGULAR REVIEWS AND UPDATES</p> <p>Continuously improve resilience with annual reviews of IBS, impact tolerances, and testing results.</p> |

Confusion or Alignment?

How DORA Implementation Is Impacted

The areas of alignment include:



Shared focus on resilience:

Both the UK Operational Resilience Act and DORA aim to strengthen financial institutions' resilience, helping firms streamline and monitor compliance.



Overlap in key practises:

Scenario testing, impact tolerances, and third-party risk management are central to both the FCA and DORA, creating a unified approach.



Timelines that are harmonised:

With the FCA deadline moved from March to January, there is now a harmonised approach to compliance with both.



Automation is key:

Continuous monitoring is a key focus of both the UK Operational Resilience Act and DORA, urging financial institutions to adopt shared tools and processes for compliance.

Confusion or Alignment?

How DORA Implementation Is Impacted

The areas of confusion include:



DORA has one scope, the FCA has another:

DORA focuses on ICT risk management, while the FCA covers broader operational disruptions, requiring separate approaches from financial institutions.



3rd party oversight:

Both regulations focus on third-party risk, but DORA requires direct monitoring of critical ICT providers, while the FCA holds financial institutions accountable for third-party risk.



Prescriptive vs principle:

DORA is prescriptive in ICT resilience, while the FCA takes a more flexible approach, allowing firms to interpret guidelines.



Resource allocation:

The FCA and DORA will compete for resources, posing challenges for teams managing both.

Meeting Both FCA and DORA Requirements

Proactive Steps for Meeting Aligned Deadlines

1

CONDUCT A GAP ANALYSIS NOW IF YOU HAVEN'T ALREADY.

2

DEFINE YOUR IMPORTANT BUSINESS SERVICES (IBS).

3

SET AND VALIDATE IMPACT TOLERANCES.

4

REVIEW YOUR THIRD-PARTY RISK MANAGEMENT.

5

IMPLEMENT CONTINUOUS MONITORING.

6

CONDUCT SCENARIO TESTING.

7

ENHANCE INCIDENT RESPONSE PLANS.

8

TRACK REGULATORY UPDATES.



The background of the slide features a dark teal color with a faint, light blue graphic. The graphic includes a target with an arrow hitting the bullseye, positioned above a bar chart with several bars of increasing height. A green horizontal line is drawn across the middle of the target.

Should you need support
with the implementation of
DORA and the FCA's UK
Operational Resilience Act,
visit our website

[QUODORBIS.COM](https://quodorbis.com)