# UK and EU financial institutions brace for new technology service provider regulations



Financial institutions in the UK and EU are set to undergo significant changes in their operational protocols as new regulatory frameworks concerning the oversight of third-party technology service providers (CTPs) come into effect. This move aims to bolster digital operational resilience following incidents such as the CrowdStrike outage in July 2024, which underscored the dependency of these institutions on external service providers and the associated risks.

From 17 January 2025, the newly introduced Digital Operational Resilience Act (DORA) will impose rigorous standards on EU regulated financial institutions regarding their information and communication technology (ICT) services. Under this legislation, critical ICT service providers will be subjected to a distinct oversight framework to ensure the effective management of ICT-related risks. Specifically, DORA mandates a comprehensive strategy focused on identifying, preventing, and responding to potential disruptions in technology services.

In the UK, a parallel regulatory framework has been put in place. It consists of a two-pronged strategy initiated with an operational resilience framework for regulated financial institutions introduced in March 2022, which sets a compliance deadline of 31 March 2025. This framework aims to highlight the importance of internal governance, requiring firms to identify key business services, set tolerances for service disruptions, and implement systems to adhere to these thresholds. Complementarily, a regime tailored for the oversight of technology service providers will commence on 1 January 2025. Although no CTPs have been designated under these regimes yet, it is anticipated that focus will initially be directed toward large cloud service providers and AI solutions.

Both DORA and the UK framework share common objectives, emphasising the necessity for financial institutions to prepare internal governance and control structures to manage risks effectively. The DORA regulations outline a requirement for risk management frameworks and digital operational resilience strategies, which are paralleled by the expectations under the UK's operational resilience rules. These include scenario testing to ensure important business services can withstand potential disruptions and prompt communication strategies to manage the fallout from these events.

Notably, DORA prescribes specific contractual obligations between EU regulated financial institutions and ICT service providers, establishing minimum requirements that encompass standardised provisions. Conversely, the UK’s operational resilience framework does not impose similar contractual stipulations, although it retains existing outsourcing regulations that may overlap.

In terms of oversight, designated ICT CTPs under DORA will be monitored by the European Supervisory Authorities, which will determine critical designations based on both qualitative and quantitative assessments. In the UK, regulators such as the Bank of England and the FCA will oversee CTPs, assessing the potential impact of service failures on financial stability in the UK. Both sets of regulations require CTPs to maintain robust risk management policies, testing programmes, and strategies for incident monitoring and reporting.

There are also several critical differences between the two regimes. Under DORA, the penalties for non-compliance are substantial, with the European Supervisory Authorities empowered to impose significant fines. The UK CTP regime, however, lacks similar punitive measures. Moreover, DORA extends its oversight to non-EU CTPs, necessitating the establishment of an EU subsidiary, while the UK does not impose location requirements for CTPs, allowing a more flexible approach without the need for physical presence.

As firms prepare for these seismic regulatory shifts, established financial institutions may find existing processes largely adequate under the new frameworks. However, the changes will necessitate substantial adaptations from technology providers designated as CTPs, marking their first exposure to direct supervision by financial regulators.

While the frameworks aim to mitigate systemic risks associated with technology providers and improve overall operational resilience, the effectiveness of these measures in preventing incidents similar to the CrowdStrike outage remains to be seen. Both jurisdictions reflect a growing recognition of the pivotal role technology plays in the financial sector and represent a proactive response to potential vulnerabilities emerging from third-party dependencies.

Source: [Noah Wire Services](https://www.noahwire.com)

## References

* <https://www.auditboard.com/blog/digital-operational-resilience-act-explained/> - This link explains the Digital Operational Resilience Act (DORA), including its key areas such as ICT risk management, incident reporting, digital operational resilience testing, and third-party risk management.
* <https://www.pymnts.com/connectedeconomy/2024/crowdstrike-aftermath-five-things-you-need-to-know/> - This article discusses the CrowdStrike outage in July 2024, its impact on financial institutions, and the broader implications for the financial sector's dependency on external service providers.
* <https://www.centralbank.ie/regulation/digital-operational-resilience-act-(dora)> - This link provides details on DORA, including its publication, application date, and the specific rules it introduces for ICT risk management, incident management, digital operational resilience testing, and third-party risk management.
* <https://orbograph.com/crowdstrike-outage-financial-institutions-experience-an-estimated-1-15b-loss/> - This article elaborates on the financial impact of the CrowdStrike outage on financial institutions and highlights the need for evaluating technology partners to mitigate disruption risks.
* <https://www.auditboard.com/blog/digital-operational-resilience-act-explained/> - This link explains the five pillars of DORA, which include ICT Risk Management, Incident Reporting, Digital Operational Resilience Testing, Third-Party Risk Management, and information sharing arrangements.
* <https://www.centralbank.ie/regulation/digital-operational-resilience-act-(dora)> - This link details the oversight framework for critical ICT third-party service providers under DORA and the role of European Supervisory Authorities in monitoring compliance.
* <https://www.centralbank.ie/regulation/digital-operational-resilience-act-(dora)> - This link explains that DORA applies to a wide range of financial entities regulated by the Central Bank of Ireland and will be fully applicable from January 2025.
* <https://www.auditboard.com/blog/digital-operational-resilience-act-explained/> - This article highlights the importance of governance and control measures under DORA, including clear role definitions and active involvement from senior management and boards in ICT risk management.
* <https://www.centralbank.ie/regulation/digital-operational-resilience-act-(dora)> - This link mentions the similarities between DORA requirements and existing Central Bank guidance on outsourcing, operational resilience, and IT & cybersecurity risks.
* <https://orbograph.com/crowdstrike-outage-financial-institutions-experience-an-estimated-1-15b-loss/> - This article emphasizes the need for financial institutions to evaluate all technology partners and solutions to ensure minimal disruptions and long-term success.