DORA & the UK Operational Resilience Framework Cybersecurity Implications

Navigating Operational Resilience in Financial Services

Operational Resilience in the Financial Sector

In the modern financial sector, operational resilience has emerged as a cornerstone of stability and security.

This concept, while not new, has gained unprecedented momentum in recent years, evolving into a critical focus area for financial institutions globally.

Operational resilience refers to the ability of financial organisations to withstand, adapt, and swiftly recover from operational disruptions, be they due to issues such as internal failures, or particularly external cyber threats.

The financial sector, inherently interconnected and reliant on complex IT infrastructures, faces a myriad of cybersecurity threats ranging from data breaches to sophisticated cyberattacks.

These threats not only jeopardise sensitive financial data but can also disrupt essential services, thereby eroding customer trust and potentially destabilising financial markets.

In this context, operational resilience goes beyond mere regulatory compliance; it is a strategic imperative that encompasses robust cybersecurity measures, effective risk management, and agile crisis response mechanisms.

The regulatory landscape surrounding operational resilience is rapidly evolving, with significant developments in both the European Union (EU) and the UK. The EU's Digital Operational Resilience Act (DORA) and the UK's Operational Resilience Framework stand out as pivotal regulatory milestones.

DORA, set to be enforced by January 17, 2025, specifically targets the digital operational resilience of the financial sector. It mandates financial entities to ensure that their IT infrastructures can withstand and recover from a wide array of digital disruptions.

Similarly, the Operational Resilience Framework in the UK, developed by the Financial Conduct Authority (FCA), the Prudential Regulation Authority (PRA), and the Bank of England, is focused on enhancing the ability of the financial sector to withstand and recover from a wide range of operational disruptions.

It mandates financial institutions to identify vital business services and set impact tolerances for disruptions, ensuring that they can continue delivering critical services, even during and after a crisis.

With these regulatory deadlines looming in the next year, the clock is ticking for financial institutions to align their strategies with these new requirements.

A proactive approach to resilience is no longer optional but a fundamental necessity. In the face of increasing cyber threats and technological interdependencies, financial institutions must fortify their defences, not just to comply with these emerging regulations but to safeguard their future in an increasingly digital and interconnected financial landscape.

The journey towards operational resilience is both challenging and complex, yet it presents an opportunity for financial entities to reimagine their approaches to risk, security, and crisis management.

This eBook aims to guide financial institutions through this journey, offering insights into regulatory expectations, best practices, and strategic imperatives for building a financial ecosystem that's secure against cyber threats.

Understanding DORA and the UK Operational Resilience Framework

Comparing DORA (Digital Operational Resilience Act) and the UK's Operational Resilience Framework reveals both similarities and differences, reflecting the distinct focuses and scopes.

In essence, while both DORA and the UK's Operational Resilience Framework aim to enhance the resilience of the financial sector, DORA has a more specific focus on digital and ICT aspects, whereas the UK's framework takes a broader approach.

DORA Overview

The Digital Operational Resilience Act (DORA) represents a significant regulatory step forward in the European Union's approach to digital operational resilience in the financial sector. It is a comprehensive framework that aims to consolidate and standardise the rules for digital operational resilience across the EU. The primary objectives of DORA are to:

Ensure Consistency:

Establish a unified set of standards for digital resilience, eliminating inconsistencies in how digital risks are managed.

Enhance Security and Resilience:

Mandate financial entities to fortify their IT infrastructures against a broad spectrum of digital disruptions, including cyber threats.

Improve Oversight:

Introduce a robust supervisory regime for third-party IT service providers, ensuring they adhere to stringent standards of security and resilience.

5 Pillars of DORA

The Digital Operational Resilience Act (DORA) outlines five key pillars to ensure the operational resilience of financial entities in the EU. These pillars provide a framework for financial institutions to enhance their digital operational resilience and ensure compliance with regulatory standards.

ICT Risk Management

Establishing comprehensive and robust risk management frameworks for information and communication technology (ICT) systems.

ICT-Related Incident Reporting:

Implementing mechanisms for timely reporting of significant ICT-related incidents.

Digital Operational Resilience Testing:

Mandating regular testing of digital systems to assess their resilience against disruptions.

Third-Party Service Provider Oversight:

Managing the risks associated with third-party ICT service providers, including cloud services.

Information Sharing:

Facilitating the sharing of cyber threat intelligence and best practices among financial entities.

UK Operational Resilience Framework Overview

The UK Operational Resilience Framework, developed jointly by the Financial Conduct Authority (FCA), the Prudential Regulation Authority (PRA), and the Bank of England, offers a broader approach to operational resilience. This framework focuses not only on digital resilience but also on the overall ability of financial institutions to withstand and recover from a wide range of operational disruptions. Key elements of this framework include:

Identification of Important Business Services:

Firms must identify services that are critical to their operation and the wider financial system.

Setting Impact Tolerances:

Establishing thresholds for maximum tolerable disruption for each critical service.

Scenario Testing:

Conducting tests to assess the firm's ability to operate within these impact tolerances under a range of severe but plausible disruption scenarios.

Self-Assessment and Reporting:

Firms must regularly assess their compliance with the framework's requirements and report to regulators.

DORA vs the UK's Operational Resilience Framework:

Scope and Focus:

DORA

DORA, an EU regulation, specifically targets digital operational resilience, emphasising the technological aspect of operational integrity in financial entities.

It applies to a wide range of EU-regulated financial entities, including banks, payment institutions, investment firms, and others.

UK's Operational Resilience Framework

The UK's framework, developed by the FCA, PRA, and the Bank of England, broadly addresses operational resilience beyond just the technological perspective.

It focuses on the overall ability of firms, financial market infrastructures, and the financial sector to prevent, adapt to, respond to, recover from, and learn from operational disruptions.

DORA vs the UK’s Operational Resilience Framework:

Methodology and Requirements:

DORA

DORA mandates the creation of an ICT risk management framework and includes requirements for governance and control, ICT-related incident reporting, and digital operational resilience testing.

It emphasises the need for firms to establish their risk tolerance level for ICT risk and to analyse the impact tolerance of ICT disruptions.

UK’s Operational Resilience Framework

The UK's framework requires firms to identify their "important business services" and set an impact tolerance for each based on the maximum tolerable level of disruption.

The UK approach involves assessing factors like client base, financial losses, and impact on the firm's reputation and the financial system.

DORA vs the UK’s Operational Resilience Framework:

Implementation and Compliance:

DORA

DORA's compliance expectation is slightly less granular compared to the UK's framework.

While it requires firms to address ICT risk and attain specific objectives by analysing the impact tolerance for ICT disruptions, it does not require firms to set impact tolerances for each critical function or service as the UK rules do.

UK’s Operational Resilience Framework

The UK's operational resilience rules became effective on March 31, 2022, with a timeline set for firms to comply fully by March 31, 2025.

This involves identifying important business services, setting impact tolerances, and making necessary investments to operate within these tolerances.

DORA vs the UK's Operational Resilience Framework:

Likelihood vs. Impact of Disruption:

DORA

The UK framework represents a shift in thinking, focusing more on the impact of disruption rather than the likelihood of its occurrence.

It requires firms to consider various factors, including client impact and potential financial losses, when setting impact tolerances.

UK's Operational Resilience Framework

DORA, similarly, does not generally require firms to consider the likelihood of a disruption occurring, except in relation to critical ICT third-party service providers.

It places more emphasis on assessing contractual arrangements with these providers to identify risks.

Preparing for DORA Compliance

Compliance with the Digital Operational Resilience Act (DORA) is crucial for financial institutions operating within the European Union.

This chapter provides a step-by-step guide for preparing for DORA compliance, highlights the role of Security Operations Centres (SOCs) in meeting these requirements, and offers actionable strategies.

On the next page, you'll find a compliance checklist. that gives you a step by step guide to prepare for DORA compliance

DigitalXRAID
CYBER SECURITY EXPERTS

Step by Step Guide to Prepare for DORA Compliance

Steps	Actions	Completed
Understand DORA Requirements	Begin by comprehensively understanding the scope and requirements of DORA. This includes ICT risk management, incident reporting, testing, and third-party service provider oversight.	
Assess Current Compliance Level	Evaluate your current IT infrastructure, policies, and procedures against DORA requirements. Identify areas that need enhancement or overhaul.	
Develop an ICT Risk Management Framework	Establish a robust framework for managing ICT risks, including policies for risk assessment, mitigation, and ongoing monitoring.	
Implement Incident Management Processes	Set up efficient processes for ICT-related incident detection, reporting, and response. Ensure these processes align with DORA's requirements for timeliness and comprehensiveness.	
Regular Testing and Auditing	Incorporate regular testing of your digital resilience, such as penetration testing and scenario analysis. Regular audits will help ensure continuous compliance and identify areas for improvement.	
Third-Party Risk Management	If you rely on third-party ICT service providers, assess and manage the risks associated with them. Ensure they comply with DORA's standards for operational resilience.	
Training and Awareness	Educate staff about DORA requirements and the importance of digital operational resilience. Regular training will help to build a culture of resilience and compliance.	
Documentation and Reporting	Maintain thorough documentation of your compliance efforts, including risk assessments, incident reports, and mitigation measures. This documentation is crucial for regulatory reporting and audits.	

5 Pillars of DORA
The Role of a Security Operations Centre (SOC)

SOC services are well-positioned to help organisations address the five pillars of DORA:

ICT Risk Management

SOC services offer continuous monitoring and threat detection, aligning with DORA's requirement for active management of an institution's security posture.

ICT-Related Incident Reporting:

SOC services provide real-time alerts and incident reporting capabilities, ensuring that organisations can quickly and effectively respond to any security incidents.

Digital Operational Resilience Testing:

Regular security assessments and penetration testing can evaluate the resilience of ICT systems, helping organisations meet DORA's requirements for operational resilience testing.

Third-Party Service Provider Oversight:

SOC services can extend to monitoring third-party risks, ensuring that organisations don't put all their eggs in one basket, as DORA advises against concentration of risk.

Information Sharing:

Threat intelligence capabilities can help organisations stay ahead of emerging threats, aligning with DORA's focus on intelligence sharing.

Actionable Strategies

- Conduct a Risk Assessment: Regularly assess ICT risks and update risk management strategies using frameworks such as NIST.
- Implement a Partnership with Expert Providers: Collaborate with expert service providers, including SOC services, for specialised support in ICT risk management and incident response.

SOC Services as a Solution for Operational Resilience

Outsourcing to expert Security Operations Centre (SOC) service providers is increasingly recognised as a strategic solution for enhancing operational resilience in financial institutions, particularly in managing cybersecurity threats. SOCs play a crucial role in the real-time monitoring, detection, and response to cybersecurity threats, providing a comprehensive and dynamic defense mechanism against cyberattacks.

As financial institutions navigate towards compliance with regulations like DORA and the UK Operational Resilience Framework, partnering with a SOC provider can be a pivotal step in bolstering their cybersecurity defenses and operational robustness.

Best Practices in Risk Management

Real-Time Monitoring and Threat Detection:

SOCs utilise advanced tools and technologies to continuously monitor network traffic, system activities, and other indicators of compromise. This real-time surveillance enables early detection of potential security incidents, reducing the time between breach occurrence and detection.

Expertise in Threat Intelligence and Analysis:

SOC teams are comprised of cybersecurity experts, skilled in threat intelligence and adept at interpreting complex security data and can identify subtle patterns indicative of cyber threats, which might be missed by non-specialist staff.

Rapid Incident Response:

Upon detecting a threat, SOC teams swiftly execute response protocols. This rapid response capability is vital in mitigating the impact of cyberattacks, ensuring that operational disruptions are minimised.

Continuous Security Updates and Adaptation:

Cyber threats are constantly evolving. SOCs continuously update their security practices, tools, and knowledge to stay ahead of emerging threats, ensuring that the financial institution's defenses are always up to date.

Why Outsource Your SOC?

Access to Expertise:

Building and maintaining an in-house SOC requires significant investment in skilled personnel and advanced technologies. Outsourcing to a SOC service provider gives financial institutions access to top-tier cybersecurity expertise without the overhead of developing and maintaining it in-house.

Cost-Effectiveness:

Outsourcing can be more cost-effective than maintaining an in-house SOC. It reduces the need for significant capital expenditure in security infrastructure and training while providing access to high-quality services.

Scalability and Flexibility:

SOC service providers offer scalability to adapt to the changing size and complexity of the financial institution's operations. They can scale up or down their services based on the institution's evolving needs.

Focus on Core Business Activities:

Outsourcing cybersecurity operations allows financial institutions to focus on their core business activities. It alleviates the burden of continuous security monitoring and management, enabling them to allocate resources more effectively towards growth and innovation.

Regulatory Compliance:

SOC providers are typically well-versed in regulatory requirements. They can ensure that the institution's cybersecurity practices are compliant with relevant laws and regulations, including DORA and the UK Operational Resilience Framework.

Enhanced Incident Recovery and Business Continuity:

In the event of a security incident, SOC providers offer robust incident recovery services. Their expertise in managing and mitigating cyber threats is crucial for maintaining business continuity and safeguarding the institution's reputation.

The Future of Operational Resilience in Financial Services

Operational resilience in financial services is at a critical juncture, poised for transformative growth.

Operational resilience requires a comprehensive approach, encompassing not just technology and cybersecurity but also organisational culture, governance, and third-party risk management.

As financial institutions navigate the complexities of compliance, cybersecurity, and technological advancements, the role of expert SOC service providers becomes increasingly vital.

Looking ahead, the focus will be on embracing innovation, fostering collaboration, and continually enhancing resilience strategies to safeguard the financial sector's integrity and stability in an ever-changing digital world.

DigitalXRAID

CYBER SECURITY EXPERTS

Need the Best Defence
Against Cyber Threats?
Call us now on 0800 090 3734

---

info@digitalxraid.com digitalxraid.com