Fortifying Europe's Financial Future

A Deep Dive into the Digital Operational Resilience Act (DORA) and beyond the in-force date

Introduction

As cyber threats evolve, and financial institutions lean further into digital operations, Europe is taking bold steps to protect its financial ecosystem. The Digital Operational Resilience Act (DORA) stands at the forefront of this effort, aiming to secure the backbone of Europe's financial markets against increasingly sophisticated cyber risks.

In recent years, Europe's financial sector has faced an unprecedented wave of digital threats. The advent of digital banking, coupled with the reliance on cloud services and third-party providers, has exposed institutions to cyber risks that threaten not only individual firms but the stability of the entire financial system. A single breach can ripple through the interconnected web of global finance, impacting millions of consumers and shaking public confidence.

Enter the Digital Operational Resilience Act (DORA), a groundbreaking regulatory framework introduced by the European Union in December 2022. DORA is not merely a cybersecurity mandate; it is a holistic approach to operational resilience. It compels financial entities to proactively manage and secure their digital operations, ensuring continuity and safety for consumers, institutions, and the financial ecosystem as a whole.

In this article we endeavour to unpack the pillars of DORA, the regulatory documents that guide its implementation, and the roadmap for financial entities and ICT providers as they race toward the January 2025 compliance deadline. With DORA, Europe is setting a new standard for operational resilience in finance—a standard that could reshape the global regulatory landscape.

Why DORA – Addressing the Need for Digital Resilience in Finance

Financial markets are more interconnected than ever before. A cyberattack on one institution can cascade across borders, affecting businesses, governments, and individuals in unexpected ways. The rapid digitization of financial services has made the industry more efficient, but it has also created new vulnerabilities.

DORA is Europe's response to this changing landscape. It was developed to address three critical issues in the digital finance space:

1. ***Increased Risk from Digital Transformation***:
   As institutions digitize, they open new doors to cyber threats. Systems that are not adequately secured can be exploited, putting sensitive financial and customer data at risk.

2. ***Systemic Risk Due to Interconnected Systems:***
   Financial institutions rely on a web of third-party services, from cloud providers to payment processors. If one of these services fails or is compromised, the impact can quickly spread, disrupting operations across the sector.

3. ***Outsourcing and Third-Party Dependencies:***
   Many financial entities outsource critical functions to third-party ICT providers, including cloud infrastructure, data management, and cybersecurity solutions. However, this reliance introduces new risks, as the security of financial institutions is now partially dependent on their vendors.

DORA doesn't just ask financial institutions to secure themselves; it demands they ensure the resilience of their entire supply chain. It represents a paradigm shift from reactive cybersecurity measures to proactive, systemic resilience. In doing so, DORA aims to protect consumers, maintain financial stability, and promote trust in Europe's financial markets.

Unpacking the Regulatory Documents: A Comprehensive Overview

DORA's framework is underpinned by a series of regulatory documents, each of which outlines specific requirements and standards for different aspects of digital operational resilience. Together, they form a cohesive set of rules that financial institutions and ICT providers must follow. Let's take a closer look at these foundational documents.

1. *Regulatory Technical Standards (RTS) on ICT Risk Management Framework*

Published as EU Regulation 2024/1774 on March 13, 2024, this RTS lays the groundwork for the ICT risk management requirements under DORA. It mandates that financial entities develop a robust ICT security framework that addresses all aspects of digital risk, from data encryption to system availability. Key highlights of this RTS include:

- ***Data Security and Encryption***: Financial entities must use encryption to protect data at rest, in transit, and in use. This includes the use of cryptographic controls to ensure data integrity and confidentiality.
- ***Vulnerability and Patch Management***: Institutions are required to identify and address system vulnerabilities through a structured patch management process. This includes testing patches in a controlled environment before deployment to prevent operational disruptions.
- ***Incident Detection and Response***: DORA requires financial entities to establish mechanisms for early detection of cyber incidents, clear reporting lines, and rapid response strategies to minimize damage and recover swiftly.

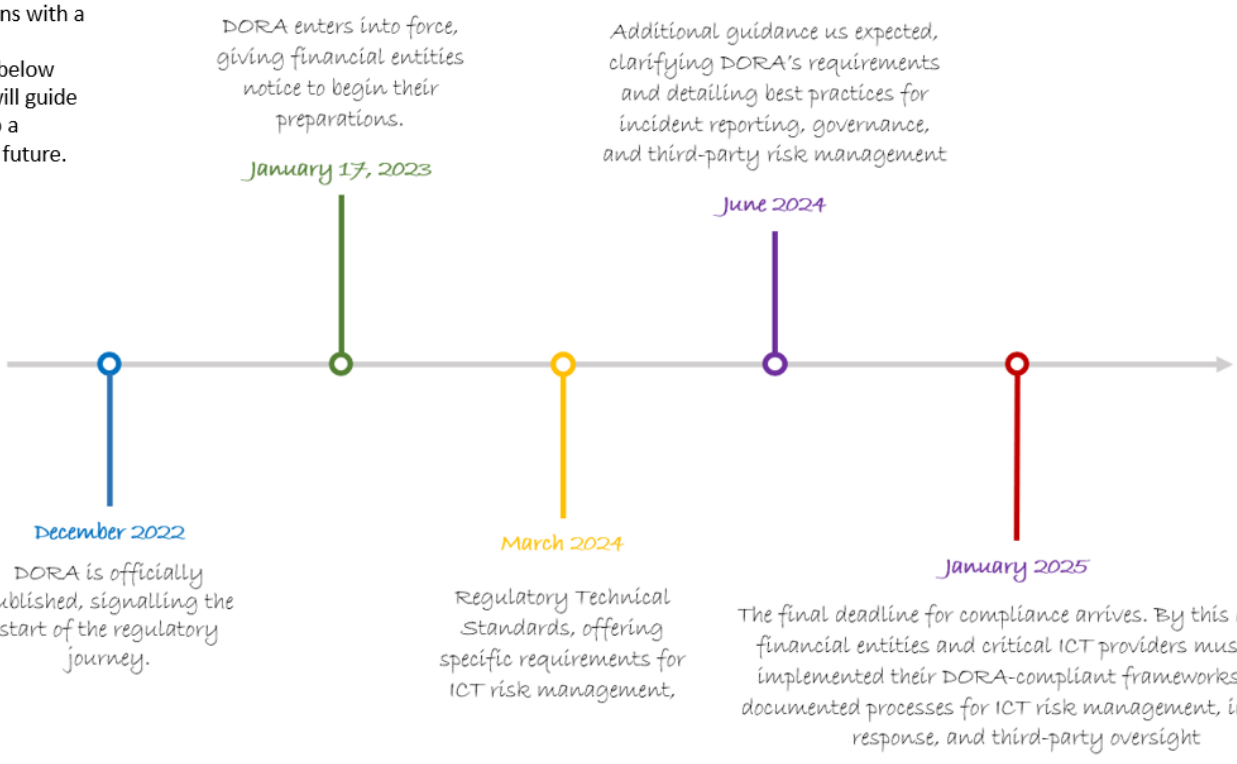
This RTS is designed to be flexible, recognizing that financial entities vary in size, complexity, and risk exposure. For example, while large institutions may require advanced tools and procedures, smaller entities may use simpler frameworks, provided they meet baseline resilience requirements.

2. *RTS on ICT Third-Party Criteria*

The importance of third-party ICT providers in today's financial services cannot be overstated. Regulation EU 2024/1773, also issued in March 2024, establishes clear criteria for managing these third-party relationships. It underscores that the financial sector's resilience is only as strong as the weakest link in its supply chain. Some of the key requirements include:

The Roadmap to Compliance: A Timeline for Financial Entities

DORA's rollout is designed to provide financial institutions with a clear, phased approach to compliance. The timeline below highlights key dates that will guide the industry's transition to a resilient, DORA-compliant future.



- ***Contractual Provisions:*** All contracts with third-party providers must include clauses on data protection, incident response, and compliance with DORA standards. This ensures that both the institution and provider are aligned on risk management expectations.
- ***Ongoing Monitoring:*** Once a provider is engaged, institutions must continuously monitor their performance and compliance. Regular assessments are required to ensure providers maintain high standards, particularly those involved in critical functions.

3. Delegated Regulation on Designation Criteria for Critical ICT Third-Party Providers (CTPPs)

Not all third-party providers carry the same level of risk. Some are deemed "critical" due to the essential services they provide. The Delegated Regulation on CTPP Designation specifies the criteria for identifying these providers, focusing on factors such as systemic impact, importance of supported functions, and the difficulty of replacing the provider.

This regulation also empowers the European Supervisory Authorities (ESAs) to designate certain providers as critical and oversee their compliance. Designated CTPPs face enhanced scrutiny, with mandatory annual audits and continuous monitoring by ESAs. This ensures that crucial services remain resilient and secure, minimizing the risk of disruptions that could impact financial stability.

4. Delegated Regulation on DORA Oversight Fees

To fund the oversight of critical ICT providers, DORA includes a fee structure outlined in this regulation. Fees are calculated based on the provider's turnover, ensuring that larger, high-revenue providers contribute proportionally to the costs of their oversight. This revenue funds regular audits, assessments, and any additional compliance activities led by ESAs, allowing for a sustainable model of regulation and enforcement.

Navigating DORA Compliance: A Step-by-Step Guide for Financial Institutions

Achieving DORA compliance is a complex process, especially for large financial institutions with extensive digital operations. Here's a detailed guide to help institutions meet DORA's standards.

1. Conduct an Initial Gap Analysis

The first step in any compliance journey is understanding where your organization stands. Conduct a thorough gap analysis to identify where current ICT practices fall short of DORA's requirements. Focus areas should include risk management, incident response, and resilience testing capabilities.

2. Develop a Detailed Compliance Roadmap

Based on the findings from the gap analysis, create a compliance roadmap with clear goals, deadlines, and responsibilities. Prioritize high-risk areas that could impact your organization's ability to deliver critical services during a cyber incident.

3. Strengthen the ICT Risk Management Framework

Update your security policies to align with DORA's standards. This includes introducing or enhancing data encryption, capacity management, and patch management. Ensure that your framework is adaptable, allowing you to respond to emerging threats effectively.

4. Establish Incident Response and Reporting Mechanisms

Develop a comprehensive incident response plan. This should include staff training on incident detection, predefined escalation paths, and regular reporting to senior management and regulatory authorities.

5. Implement Regular Resilience Testing

DORA mandates that institutions perform resilience tests regularly. These include penetration tests, vulnerability assessments, and simulation exercises to prepare the organization for potential disruptions. By testing systems under various scenarios, you can identify weaknesses and improve your defences.

6. Manage Third-Party Risks Rigorously

Third-party providers are integral to modern financial operations, but they also pose risks. Establish a rigorous third-party management program, ensuring that all ICT providers are compliant with DORA. For critical providers, conduct additional due diligence and enforce regular performance monitoring.

7. Strengthen Governance and Oversight

Create a governance structure that clearly assigns roles and responsibilities related to DORA compliance. Regularly report progress to senior management, providing insights into risk management, incident response, and third-party assessments.

8. Keep Detailed Records of All Compliance Activities

Documentation is a cornerstone of DORA compliance. Maintain comprehensive records of all ICT incidents, resilience tests, and third-party evaluations. This will be

essential for audits and regulatory inspections, and it demonstrates a commitment to transparency.

9. Engage with Regulatory Authorities

Maintain open communication channels with regulatory bodies and keep stakeholders informed of your compliance efforts. This ensures alignment with regulatory expectations and allows for any adjustments needed based on evolving DORA guidance.

10. Embrace Continuous Improvement

DORA is not a one-time compliance exercise. It mandates continuous improvement, requiring institutions to update their ICT frameworks in response to new risks, technological changes, and regulatory updates. By building a culture of continuous improvement, institutions can stay ahead of future compliance challenges.

The Long-Term Impact of DORA: A New Standard for Financial Resilience

DORA's effects will extend far beyond the 2025 compliance deadline. By establishing a high standard for ICT risk management, DORA will elevate cybersecurity across the financial sector. Some of the long-term impacts include:

- ***Increased Customer Confidence***: As institutions adopt stringent security measures, consumers can trust that their financial data is protected. This trust is crucial for the ongoing success of digital finance.

- ***Stronger Market Integrity***: By ensuring that critical ICT providers are also resilient, DORA reduces the risk of systemic shocks caused by third-party disruptions.

- ***Enhanced Operational Efficiency***: The focus on resilience and risk management will prompt institutions to optimize their digital operations, improving service delivery and reducing costly disruptions.

- ***A Model for Global Financial Regulation***: DORA sets a high standard that could influence regulatory bodies outside Europe. As cyber risks grow globally, other regions may look to DORA as a model for their own digital resilience frameworks.

Minimum Requirements for January 2025 Compliance under DORA

When DORA enters into force in January 2025, financial institutions and ICT providers need to have essential operational and compliance measures established. As a minimum, insinuations will be required to have in place:

- ***ICT Risk Management Framework***: A robust and adaptive ICT risk management framework must be operational. This framework should cover areas such as:
    - *Data Security and Encryption*: All sensitive data, both in transit and at rest, must be encrypted. Institutions should use encryption standards that meet or exceed regulatory requirements to protect consumer data and operational information.
    - *Incident Detection and Response*: Mechanisms should be in place to detect, report, and respond to incidents promptly. This includes defining escalation paths for incidents and ensuring that staff members understand response protocols.
    - *Vulnerability Management and Patch Updating*: Institutions need a structured approach for identifying and remediating vulnerabilities. Regular patch management ensures systems are updated to resist new threats.

- ***Third-Party Risk Management***: Given DORA's emphasis on third-party dependencies, financial entities must have formalized controls for managing third-party risks, including:
    - *Contractual Obligations*: Contracts with third-party ICT providers should include clauses on data protection, incident response, and alignment with DORA standards.
    - *Ongoing Monitoring*: Financial entities must actively monitor third-party providers' performance, focusing especially on critical providers who could impact operational resilience.

- ***Resilience Testing Capabilities***: Regular resilience testing, such as penetration testing, must be an integral part of ICT risk management to ensure systems are prepared for potential disruptions. These tests help institutions identify weaknesses and implement effective controls.

- ***Governance and Reporting Structures***: Organizations should establish a clear governance structure for DORA compliance, including defined roles and responsibilities for compliance oversight, regular reporting to senior management, and escalation protocols for DORA-related issues.

These elements represent a minimum standard for readiness. Each institution may need additional measures depending on its complexity, third-party dependencies, and risk profile.

zeb's support: performing Gap Analysis – Current status vs. DORA Requirements

A gap analysis is essential to evaluate where an institution currently stands compared to DORA's requirements, especially as January 2025 approaches rapidly. zeb has expertise in supporting clients to analyse the gap with the regulatory reequipments by performing:

- ***Comprehensive Review of Existing ICT Frameworks***: zeb will perform a thorough assessment of the institution's ICT risk management frameworks, examining data security practices, incident response procedures, and resilience testing capabilities. The goal is to compare these existing practices against DORA's standards and highlight any deficiencies.

- ***Third-Party Dependency Analysis***: As institutions often rely heavily on third-party providers, the analysis can also include a review of contracts, monitoring protocols, and critical providers' resilience. zeb can assist in identifying high-risk areas where third-party compliance may fall short of DORA's standards.

- ***Development of a Compliance Roadmap***: Based on the gap analysis findings, zeb can support in creating a detailed roadmap toward full DORA compliance. This roadmap can include specific actions, priorities, and timelines to address identified gaps. For example, high-risk gaps in areas like incident response would be prioritized, while lower-risk gaps may be scheduled for a later phase.

- ***Ongoing Support and Documentation***: Beyond the initial analysis, zeb can support documentation efforts that will be essential for audits and inspections. Comprehensive records demonstrating the steps taken to address gaps show regulators that the institution is committed to achieving and maintaining compliance.

Importance of External Gap Assessment and Support in Closing Identified Gaps

An external gap assessment offers an objective view of an institution's DORA readiness and can uncover areas that may not be apparent through internal reviews. zeb can support clients in closing gaps by performing:

- ***Independent Verification of Compliance***: Regulators and stakeholders place higher trust in assessments conducted by an external party, as it removes potential biases and ensures an unbiased approach to identifying compliance gaps.

- ***Uncovering Less Obvious Vulnerabilities***: zeb can leverage internal experiences and industry best practices in compliance to conduct a meticulous review, often identifying hidden vulnerabilities that internal teams may overlook. This is especially valuable in complex ICT environments with multiple interdependencies, where subtle gaps may still lead to significant operational risks.

- ***Assistance in Prioritizing and Addressing Gaps***: After completing the assessment, zeb can work with clients to prioritize the identified gaps based on risk levels, potential operational impact, and regulatory urgency. This approach helps clients allocate resources efficiently, focusing on the most critical gaps first.

- ***Support in Implementing Solutions***: zeb can provide practical support for closing gaps, from helping adjust existing policies and controls to implementing new procedures that align with DORA's standards. zeb's approach is hands-on and solution-oriented, ensuring that each step taken directly addresses the compliance requirement.

DORA as a Continuous Compliance Journey

The EU's Digital Operational Resilience Act is a landmark regulation that reshapes how Europe's financial sector manages digital risk. With DORA, Europe is building a financial ecosystem prepared not just to survive in a world of cyber threats but to thrive in it. By 2025, financial institutions and ICT providers are expected to have transformed their operations to meet this new standard, ushering in an era of resilience, security, and consumer trust. For financial entities, DORA compliance is a journey that demands attention, investment, and commitment, but it is a journey that will fortify the sector against the challenges of the digital age.

Compliance with DORA is not a one-time event; it requires an ongoing commitment to maintaining operational resilience and adapting to new threats and regulatory updates. Post-2025, financial institutions must integrate DORA's requirements into their daily operations and are expected to have in place:

- ***Annual Risk and Compliance Monitoring***: Control functions within organizations should conduct regular reviews to assess alignment with DORA. This involves:
    - *Annual Risk and Compliance Plans*: Organizations should develop annually plans that outline specific risk management and compliance activities. These plans must consider any new threats, emerging technologies, and updates to regulatory requirements.
    - *Testing and Audits*: Regular audits and resilience tests should be integrated into the annual risk assessment process, ensuring systems and procedures remain effective in mitigating risks.
- ***Board Reporting and Accountability***: Institutions should establish mechanisms for regularly updating the board on DORA compliance, operational risks, and resilience. Reports should include:
    - *Status Updates on Compliance Activities:* Boards must be kept informed about compliance initiatives, any incidents that have occurred, and steps taken to mitigate risks.
    - *Progress on Closing Identified Gaps:* Gaps identified in previous assessments or incidents should be monitored closely, with updates on progress provided to the board as part of its oversight function.
- ***Embracing Continuous Improvement***: DORA mandates a proactive approach to cybersecurity and resilience, requiring organizations to adapt policies and frameworks as new threats emerge. This continuous improvement approach includes:
    - *Periodic Updates to Policies and Controls:* Organizations should routinely review and update their policies in response to new regulations, technological advancements, and changes in the threat landscape.
    - *Building a Resilience-Focused Culture:* By fostering a culture of resilience, institutions can ensure that staff at all levels understand the importance of compliance and are trained to identify and respond to risks effectively.

This ongoing compliance journey is critical, as cyber threats continuously evolve. By integrating DORA's principles into the organization's culture and daily operations, institutions can stay ahead of potential disruptions and build trust with regulators, clients, and stakeholders.

Joseph Jawahiri
Manager – Governance, Risk and Compliance
zeb Nordics