Teleport

Digital Operational Resilience Act (DORA): Navigating Compliance with Teleport

Contents

The stakes for operational resilience and regulatory compliance have never been higher — and governments around the world are responding accordingly.

In the European Union (EU), the Digital Operational Resilience Act (DORA) aims to fortify financial institutions and their critical third-party technology service providers against the ever-growing threat of ICT-related incidents. Disruptions can no longer be viewed as isolated events — they're inevitable. Your organization is now tasked with increasing its survivability and mitigating the potential for damage.

This white paper will delve into the intricacies of DORA, unpacking why these frameworks are vital and how the correct solutions can simplify the journey towards compliance with the controls defined by the regulation. We'll explore how Teleport's suite of secure infrastructure access solutions can support your organization in meeting these mandates effectively.

Let's start with an in-depth look at the DORA framework.

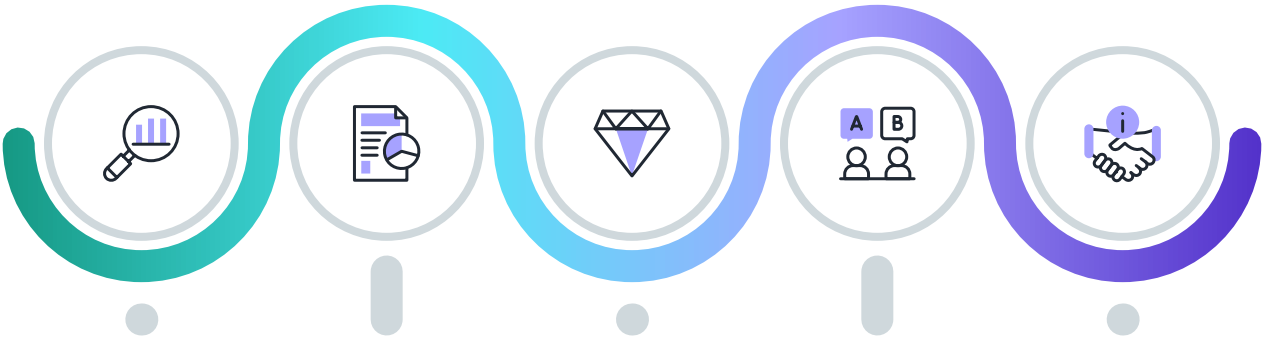
Understanding the DORA Framework

The Digital Operational Resilience Act framework is a regulatory initiative introduced by the EU to increase the financial sector's resilience to ICT-related events. It applies to banks, investment firms, insurance companies, and payment institutions, among others. DORA has also been expanded to include essential third-party technology service providers, such as cloud service providers, data analytics service providers, and software vendors.

The Five Key Pillars of DORA

The regulation includes a five pillar structure that addresses critical security and ICT components that organizations must focus on, including:

1. **ICT Risk Management and Governance:** Financial institutions must implement robust information and communication technology (ICT) risk management frameworks to effectively identify, assess, and mitigate ICT risks.
2. **ICT-Related Incident Reporting:** All ICT-related incidents, no matter how big or small, must be reported to the appropriate officials. This includes anything that had a small to major impact.
3. **Digital Operational Resilience Testing:** This calls for testing ICT incident responses on a regular basis to mimic different situations, such as hacking, natural disasters, and human mistakes.
4. **ICT Third-Party Risk:** This focuses on handling the risks that come with important third-party technology service providers. It requires due diligence, performance tracking, and planning for what to do if something goes wrong.
5. **Information Sharing:** Encourages financial institutions and officials to share information about threats and incidents linked to ICT.



ICT Risk Management and Governance

Implement robust ICT risk management frameworks to effectively identify, assess, and mitigate ICT risks

ICT-Related Incident Reporting

Report all ICT-related incidents to DORA regulators

Digital Operational Resilience Testing

Test ICT incident responses on a regular basis to mimic different situations, such as hacking, natural disasters, and human mistakes

ICT Third-Party Risk

Test the resilience of critical third-part technology service providers and implement backup services for outages

ICT Risk Management and Governance

Financial entities must share information about ICT threats and incidents with DORA regulators

DORA Prerequisites

The road to achieving DORA compliance is daunting – organizations only have until January 17, 2025 to prepare. This timeline has allowed EU regulators to build a robust infrastructure of technical rules, assessment frameworks, and operational processes to guide financial services entities along their compliance journey.

While none of these structures exist in full measure today, their ongoing development is critical to ensuring organizations not only meet baseline DORA requirements, but can continuously adapt to address evolving ICT risks. Looking towards the future, the major tasks ahead include harmonizing ICT risk management, creating incident reporting mechanisms, and identifying critical third-party service providers.

Harmonizing ICT Risk Management

At the heart of DORA is the desire to harmonize ICT risk management across all EU Member States. Articles like 8 and 15 mandate regulators to fold ICT risk into the EU's Single Rulebook, which already governs other areas of financial risk. This is achieved by setting up technical security requirements and standardizing evaluation processes under the DORA framework. Once in place, this uniform approach will help financial institutions streamline compliance and reduce friction when operating across borders.

Establishing a Comprehensive Incident Reporting System

Another key priority is the creation of an incident sharing and reporting process. Under Articles 19-23, financial entities are required to report significant ICT-related incidents to relevant authorities, who will then assess the incident's severity and potential cross-border impact. Establishing this system will be a major focus during the pre-compliance period, and will ensure that organizations can react swiftly to cyber incidents, reducing potential fallout and helping to protect the broader financial ecosystem of the EU and beyond.

Managing Third-Party Risk: Identifying Critical ICT Service Providers

A substantial portion of DORA focuses on mitigating the risks associated with third-party ICT service providers. In fact, a full quarter of the framework is strictly dedicated to assessing and designating providers that are deemed critical for financial institutions.

Article 31 tasks regulators with creating a formal process for identifying and evaluating these service providers. This is akin to the U.S. federal government's cloud.gov initiative, which centralizes approved third-party cloud services. By the 2025 deadline, regulators will need to have a clear system in place for monitoring and managing the risks posed by these critical providers.

Penalties for Non-Compliance: A Financial Wake-Up Call

For entities that fail to comply with DORA, the consequences can be significant. Article 50 outlines administrative and remedial penalties, while Article 35 hits third-party providers with a specific monetary penalty for non-compliance.

Providers could face daily fines of up to 1% of their average global turnover (revenue), making it clear that DORA takes compliance seriously. The financial stakes are high, and organizations that delay in meeting DORA's requirements will not only face legal repercussions but risk significant damage to their reputation and bottom line.

Overcoming DORA Compliance Challenges

While DORA's objectives are clear, the path to compliance presents several challenges:

- **Managing Third-Party Risk:** As financial institutions become increasingly reliant on third-party services, ensuring the resilience of these providers can be a complex and resource-intensive process.
- **Evolving Cyber Threats:** The cybersecurity landscape is in constant flux, and organizations must adopt a proactive approach, continuously monitoring and updating their defenses to keep pace with new threats
- **Resource Constraints:** Meeting DORA's stringent requirements may require significant investment in resources — whether through new security controls, regular risk assessments, or staying ahead of regulatory updates.

Ultimately, the Digital Operational Resilience Act is more than a cut-and-dry compliance requirement — it's a strategic tool that empowers organizations to strengthen their ICT resilience and enhance their competitive position. By addressing these challenges head-on, organizations can not only achieve compliance with DORA but also strengthen their overall cybersecurity and competitive posture, making them better equipped to thrive in the digital age.

Teleport

Want to view more? Unlock the full PDF.

Fill out the form to unlock the full PDF.