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.

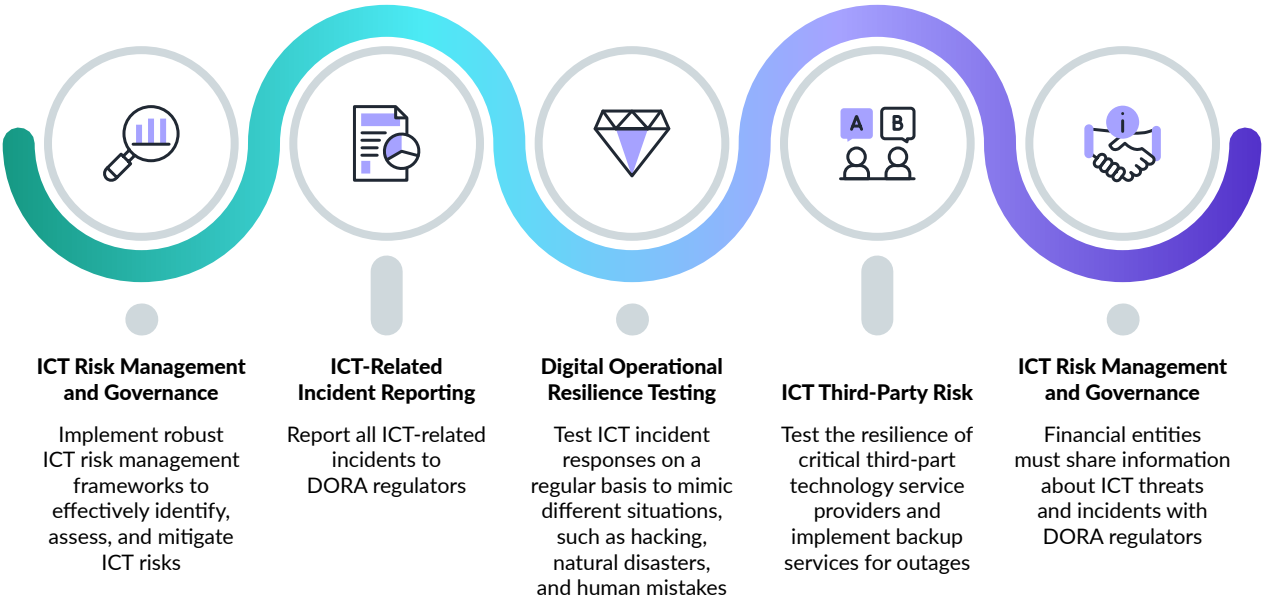
Understanding the DORA Framework

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.



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.

How Teleport Addresses DORA Requirements

As we've covered, the EU's Digital Operational Resilience Act mandates a robust cybersecurity framework that encompasses risk management, secure access controls, incident response, and ongoing monitoring. Teleport's suite of secure infrastructure access solutions — including Teleport Zero Trust Access, Teleport Identity Governance, Teleport Identity Security, and Teleport Machine & Workload Identity — is well-positioned to help organizations meet stringent requirements while enhancing operational efficiency and security.

Teleport Zero Trust Access

Eliminate credentials and standing privileges

On-demand, least privileged access on a foundation of cryptographic identity & zero trust

Teleport Identity Governance

Protect against identity-based attacks

Harden your infrastructure with identity governance and security

Teleport Identity Security

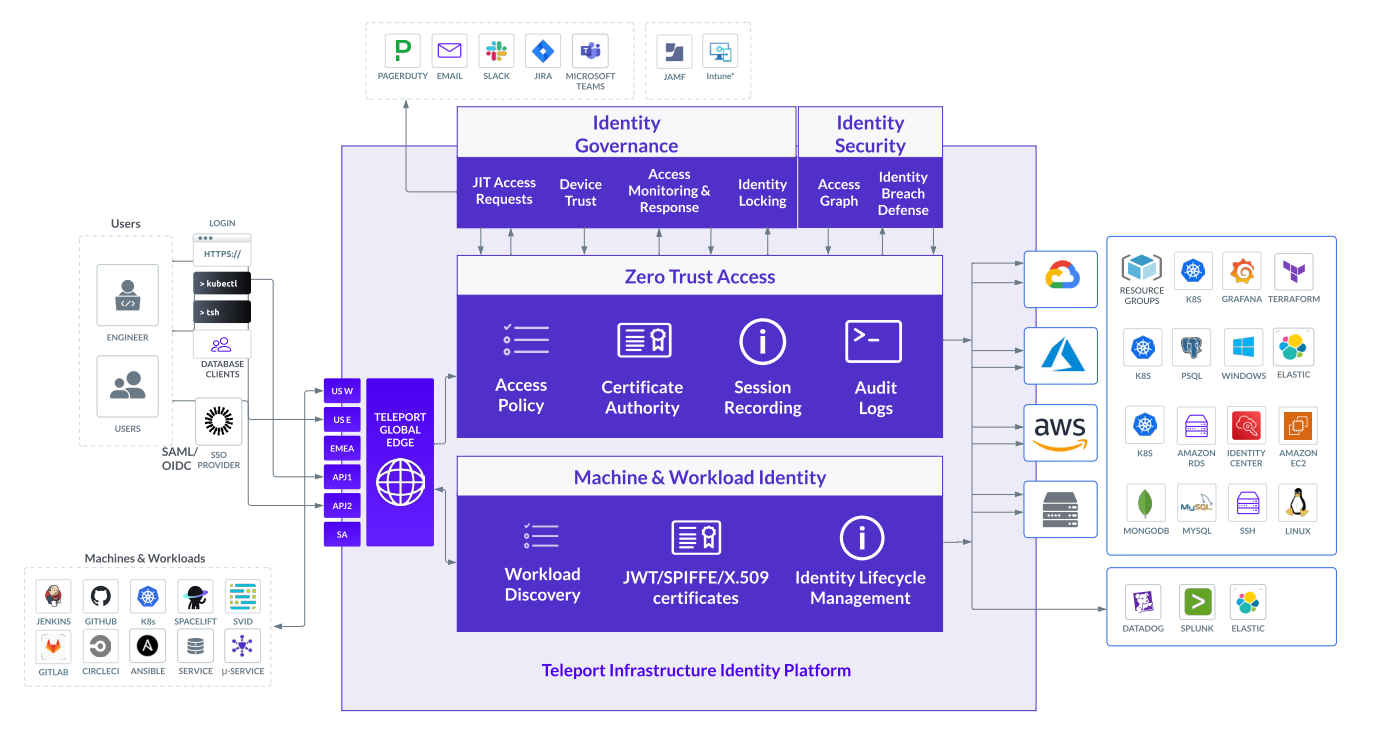
Stop threat actors in their tracks

Secure identities & access policies across all your infrastructure. Erase shadow access & blind spots.

Teleport Machine & Workload Identity

Unify human & non-human access policies

Improve infrastructure resiliency by securing access to systems & data between machines & workloads



Eliminating Credentials and Standing Privileges

One of DORA's key requirements is the protection of information and communication systems by minimizing the risk of unauthorized access.

Teleport directly supports this by eliminating credentials such as passwords, SSH keys, and static tokens, which are often the target of cyberattacks. Instead, Teleport uses certificate-based ephemeral credentials, drastically reducing the risk of credential theft or misuse.

Compliance with DORA's Access Control Mandates

By eliminating standing privileges and moving to dynamic, certificate-based access, Teleport aligns with DORA's focus on securing systems through minimized privilege and context-based access controls. This approach ensures users only have access to systems when they need it, and that access expires automatically after a session — closing the door to potential backdoor exploits.

Secure Remote Access

Teleport enables secure remote access to applications, databases, and workloads from anywhere, without compromising security. This feature is crucial for financial institutions managing globally distributed teams or third-party contractors, ensuring access to critical infrastructure remains tightly controlled and monitored.

Real-Time Monitoring and Incident Response

DORA emphasizes the importance of continuous monitoring and rapid incident response in order to address emerging ICT risks. Teleport enables organizations to monitor user behavior in real-time, detecting and quickly responding to potential threats as they arise. With the ability to lock compromised accounts and the enforcement of just-in-time access requests, Teleport ensures that only authorized users can access critical systems — and only for a limited period of time.

Real-Time Detection of Weak Access Patterns

Teleport continuously analyzes user activity to identify anomalies — such as unusual login locations or abnormal access requests — and automatically flagging and responding to these anomalies. This provides organizations with the controls necessary to meet the act's requirements for proactive risk management and early detection of security incidents.

Access Reviews and Requests

Teleport supports the DORA directive's requirement for auditable access management through its just-in-time access request and review system. This system ensures access is granted on an as-needed basis with complete traceability and approvals, helping financial institutions adhere to DORA's standards for controlled access to critical systems.

Comprehensive Policy Management and Incident Intervention

DORA requires financial institutions to have comprehensive ICT risk management policies in place to ensure all aspects of operational resilience are addressed. Teleport offers a centralized platform to manage security policies across the organization's entire infrastructure, helping financial institutions develop and enforce policies that are consistent with DORA's requirements.

Managing and Analyzing Access Relationships

Teleport provides a detailed view of access relationships, allowing administrators to easily audit and understand who has access to what systems — and when they were accessed. This granular visibility supports DORA's requirements for ongoing risk assessments and helps ensure that only authorized personnel have access to sensitive systems, reducing the risk of unauthorized access.

Incident Intervention

In the event of a threat or breach, Teleport enables rapid intervention by allowing administrators to quickly modify, revoke, or isolate access as needed. This capability is aligned with DORA's emphasis on swift incident response, ensuring that institutions can act immediately to contain threats and prevent escalation.

Modernizing Privileged Access: Improving Security and Productivity

DORA's framework emphasizes the need to secure privileged access to critical systems, but traditional methods of managing privileged access often result in productivity bottlenecks — generating friction for developer and engineering teams. Teleport modernizes privileged access by eliminating static credentials and manual processes, offering an identity-based solution that not only enhances security, but also improves productivity — even for the requestor.

Identity-Centered Access

By centering access around user identity and authentication rather than static credentials, Teleport reduces the risks of credential theft and simplifies the management of access controls. This makes it leaps and bounds easier to enforce DORA's identity and access management requirements while also making infrastructure access more seamless for engineering and IT roles.

Increased Productivity

Teleport's streamlined approach to access management improves the productivity of engineers and developers without compromising on compliance controls, enabling faster, more secure access to infrastructure without the need for cumbersome password or token management — which create significant risk. Eliminating the option for static credentials allows teams to focus on innovation and operational efficiency, ensuring security and compliance measures do not stand in the way of business goals like time-to-market and innovation.

Supporting DORA's Reporting and Incident Response Requirements

DORA places heavy emphasis on incident reporting and ensuring operational continuity in the face of ICT-related disruptions. Teleport's built-in auditing and logging capabilities provide financial institutions with a detailed record of every access attempt, session, and activity, enabling full traceability and compliance with DORA's reporting requirements.

Incident Reporting

Should a breach or incident occur, Teleport provides a complete audit trail of all access activity, giving organizations all the information needed to report incidents in line with DORA's strict reporting guidelines. This includes the ability to share reports with regulators and demonstrate proper security measures are in place at any point in time.

Operational Continuity

Teleport's focus on automated access controls and real-time monitoring helps organizations maintain operational continuity during security incidents. Access can be quickly adjusted or revoked to mitigate risks, preventing further disruptions in the event of a breach.

Integrations with SIEM Tools

Teleport integrates reporting with popular SIEM tools like Datadog and Splunk.

Teleport as a Solution for DORA Compliance

Teleport's secure infrastructure access solutions provide EU financial institutions with the tools they need to meet the comprehensive requirements listed by the Digital Operational Resilience Act. By eliminating credentials and secrets, implementing finely-tunable access controls, providing real-time monitoring, and supporting policy management, Teleport quickly enables organizations to secure their infrastructure in compliance with DORA's mandates.

Teleport's modernized approach to privileged access not only strengthens security and compliance, but also enhances productivity — empowering financial institutions to achieve both their compliance and operational objectives without compromise. For organizations seeking to build resilience and streamline compliance, Teleport offers a unified, scalable solution that addresses the core challenges posed by DORA's operational resilience requirements.