The Digital Operational Resilience Act (DORA) and Third-Party Risk Management

Preparing for the Digital Operational Resilience Act: Third-Party Risk Management

Are you ready to tackle the Digital Operational Resilience Act (DORA)? This groundbreaking EU regulation is set to transform how financial firms manage their digital risks and third-party relationships. As the Digital Operational Resilience Act timeline approaches, it's crucial to understand its far-reaching impact on your organization's cybersecurity practices and governance structures. DORA compliance isn't just about ticking boxes; it's about strengthening your digital resilience in an increasingly interconnected financial ecosystem.

To get you up to speed, we'll dive into DORA's scope and how it affects your business. You'll learn about the specific third-party risk management requirements outlined in the regulation and gain insights on how to set up a DORA-compliant risk program.

We'll also explore the regulatory technical standards and risk assessment processes you must implement. By the end of this article, you'll have a clear roadmap to navigate the complexities of DORA and ensure your organization is well-prepared for this new era of digital operational resilience.

Understanding DORA's Scope and Impact

The Digital Operational Resilience Act (DORA) harmonizes the approach to managing Information and Communication Technology (ICT) risks in the financial sector across the European Union. It consolidates and updates rules on digital operational resilience, filling gaps and remedying inconsistencies in existing legislation [1]. DORA acknowledges that ICT incidents can jeopardize the soundness of the entire financial system, even with adequate capital for traditional risk categories [1].

DORA lays down uniform requirements concerning the security of network and information systems supporting the business processes of financial entities [1]. These requirements cover ICT risk management, reporting of major ICT-related incidents, digital operational resilience testing, information sharing on cyber threats and vulnerabilities, and measures for sound management of ICT third-party risk [1].

Key Provisions of DORA

DORA establishes crucial requirements for companies to enhance their ability to withstand, respond to, and recover from ICT-related disruptions.
Its key pillars include:

1. ICT risk management: Companies must implement a comprehensive ICT risk management framework, regularly assessing risks and adapting defense mechanisms.
2. Incident reporting: A robust incident reporting mechanism must be established, with companies promptly reporting significant cyber and ICT-related incidents to relevant authorities.
3. Digital operational resilience testing: Regular testing of digital operational resilience is prescribed, including vulnerability assessments, penetration testing, and scenario-based exercises.
4. Third-party risk management: DORA focuses on managing and monitoring ICT risks arising from relationships with third-party service providers, ensuring they adhere to the same ICT risk management standards.

Entities Affected by DORA

DORA has a broad scope, covering "financial entities," which includes most types of financial services providers regulated in the EU, such as:

- Banks
- Payments and e-money firms
- Investment firms
- Insurers
- Cryptoasset firms

Notably, DORA also applies to some entities typically excluded from financial regulations, such as third-party service providers that supply financial firms with ICT systems and services (e.g., cloud service providers and data centers).

These ICT third-party service providers (ICT TPPs) will face indirect impacts, needing to align their services and contractual terms with DORA to support clients' compliance requirements. They should anticipate increased due diligence on existing operational and technical frameworks and additional demands from clients.

Certain ICT TPPs may be designated as "critical" (CTPPs) if they are systemically important to a high number of financial entities, support critical functions, and are difficult to substitute. CTPPs will be subject to direct regulatory supervision by the ESAs

In conclusion, DORA introduces a comprehensive framework for managing ICT risks in the financial sector, with far-reaching implications for both financial entities and their ICT service providers. As the implementation timeline progresses, affected organizations must proactively align with DORA's requirements and strengthen their digital operational resilience.

DORA Implementation Timeline:

November 2022: The European Parliament and the European Council formally adopted the Digital Operational Resilience Act as part of the EU's Digital Finance Strategy.

December 27, 2022: DORA was officially published in the Official Journal of the European Union, marking the start of its legislative journey.

January 16, 2023: DORA entered into force, setting a two-year transitional period for financial entities and ICT service providers to become compliant.

2023–2024: Throughout this period, European Supervisory Authorities (ESAs) will develop regulatory technical standards, guidelines, and other supporting frameworks to help financial entities comply with DORA.

January 2023 – January 2025: The transitional period for compliance allows financial entities and ICT providers time to adapt their systems, policies, and practices to meet the new requirements.

January 17, 2025 Deadline for Full Compliance: Financial institutions, ICT providers, and critical third-party providers must fully comply with DORA's operational resilience requirements. This includes the implementation of:

- ICT risk management frameworks
- Incident reporting procedures
- Digital operational resilience testing (including threat-led penetration testing)
- ICT third-party risk management policies

February 2025 Post-Implementation Monitoring and Compliance: Financial entities will be subject to regular supervision and audits to ensure ongoing compliance with DORA. Non-compliance can result in penalties, and financial regulators will monitor ICT risks continuously.

Third-Party Risk Management Requirements

DORA introduces strict requirements for managing risks associated with ICT third-party service providers. Financial entities must take a proactive, risk-based approach to ensure their third-party relationships do not compromise their digital operational resilience.

DORA's Chapter V, Section I outlines the key principles for sound management of ICT third-party risk. It aims to ensure that financial entities appropriately manage and mitigate risks stemming from their use of ICT services provided by third parties. The degree of risk management and oversight is expected to be proportional to the criticality and potential impact of the third-party ICT service on the financial entity, known as the Proportionality Principle.
Before entering into contractual arrangements with ICT third-party service providers, financial entities must:

1. Define the criticality or importance of the ICT services to their operations.
2. Assess if supervisory conditions for contracting are met.
3. Identify and assess all relevant risks, including the possibility of ICT concentration risk.
4. Conduct comprehensive due diligence on prospective providers.
5. Identify potential conflicts of interest with the ICT third-party service providers.
6. Ensure that the providers comply with appropriate information security standards, especially for critical functions.

Due Diligence and Vendor Assessment

Financial entities must vet prospective ICT third-party service providers before entering into any contractual agreement. This due diligence process involves evaluating the provider's reliability, security measures, compliance track record, and ability to meet the entity's specific requirements.

The vendor selection process should be rigorous and transparent, ensuring that the chosen provider aligns with the financial entity's needs and regulatory obligations. Entities must also proactively identify and assess potential conflicts of interest with ICT third-party service providers, taking appropriate steps to manage, mitigate, or eliminate them.

Contractual Obligations

Every ICT services contract under DORA must:

- Be in writing and digitally accessible at all times
- Be understandable
- Provide a register of information for all contractual agreements and respective vendors
- Document critical and non-critical ICT vendors
- Contain mandatory clauses addressing access and audit rights, performance standards, service locations, data protection, business continuity, termination rights, cooperation with authorities, incident reporting, and compliance with information security standards

Contracts with providers supporting critical functions have additional prescriptive requirements, such as subcontracting provisions, reporting obligations, business contingency planning and testing, participation in threat-led penetration testing, and exit planning. Financial entities must ensure that contractual arrangements can be terminated under specified circumstances, such as significant breaches by the provider, changes affecting the arrangement or provider's situation, evidenced weaknesses in the provider's ICT risk management, or inability of the competent authority to effectively supervise the financial entity.

Ongoing Monitoring and Reporting

After signing contracts, financial entities must continuously monitor and oversee their ICT third-party service providers to ensure compliance with contractual requirements, appropriate risk management, and maintained resilience.

DORA mandates the development of robust exit strategies for ICT services supporting critical or important functions. These strategies should consider potential risks from provider failure, quality deterioration, business disruptions, and material risks to ongoing ICT service deployment. Exit plans must be well-documented, thoroughly tested, and periodically reviewed.

Financial entities are required to report annually on the number of new arrangements, categories of ICT third-party service providers, types of contractual arrangements, and the ICT services and functions being provided.

By adhering to these third-party risk management requirements, financial entities can effectively mitigate risks associated with their ICT service providers and maintain their digital operational resilience in line with DORA's objectives.

Implementing a DORA-Compliant Third-Party Risk Program

To implement a DORA-compliant third-party risk program, you should start with a comprehensive gap analysis. This involves assessing your current ICT risk management practices against the requirements outlined in DORA. The gap analysis will help you identify areas of non-compliance, prioritize improvements, and develop an actionable plan to address gaps. The outcome of conducting a gap analysis typically includes a detailed report outlining compliance gaps, recommendations for aligning practices with regulatory standards, and an implementation roadmap with timelines for achieving full compliance.

Policy and Process Updates

Once you have identified the gaps in your current practices, the next step is to update your internal policies and procedures to meet DORA's standards. This includes emphasizing ICT asset management, encryption controls, vulnerability management, and incident reporting.

Financial entities must review and potentially amend contracts with technology service providers to ensure compliance with DORA, which includes preparing for heightened scrutiny and oversight. If providing services to EU financial entities, technology service providers, whether located in the EU or abroad, must align their services and contractual terms with DORA to support clients' compliance requirements.

Technology and Tools

Selecting the right cybersecurity tools is crucial for meeting the requirements of regulations like DORA. This demands a deep understanding of both the cybersecurity landscape and the specific regulatory requirements.

DORA mandates that data be protected at rest and in motion, irrespective of the environment. Financial entities must use encryption tools that safeguard data in both states, ensure robust access management through defined user roles and groups, and implement a role-split methodology to separate network management from security management duties.

However, regulatory compliance extends beyond encryption. Continuous monitoring and managing third-party risks are vital to maintaining a secure and resilient digital environment. This is where ProcessBolt excels as a premier provider of third-party risk management solutions. Our platform not only supports comprehensive data protection but also provides continuous monitoring, real-time risk assessments, and automated workflows to ensure that third-party relationships remain compliant with DORA and other stringent regulations.

By utilizing ProcessBolt, organizations can effectively manage third-party risks, ensuring data security and regulatory adherence. Our solutions provide enhanced visibility, persistent encryption, and the separation of critical duties to maintain confidentiality and minimize data exposure risks.

In conclusion, implementing a DORA-compliant third-party risk program requires ongoing gap analysis, continuous monitoring, and advanced tools. ProcessBolt’s innovative solutions strengthen financial entities' digital operational resilience, ensuring ongoing compliance with this pivotal regulation.

Conclusion

The Digital Operational Resilience Act has a significant influence on the financial sector's approach to managing ICT risks and third-party relationships. It introduces a comprehensive framework to strengthen digital resilience, requiring financial entities to beef up their risk management practices, incident reporting mechanisms, and testing procedures. This legislation also places a strong emphasis on the oversight of ICT third-party service providers, recognizing their crucial role in the financial ecosystem.

As financial organizations gear up to comply with DORA, they need to take a hard look at their current practices and make necessary adjustments. This involves updating policies, enhancing due diligence processes, and leveraging the right tools and technologies to manage third-party risks effectively. ProcessBolt offers real-time Third-party Risk Monitoring through its comprehensive Vendor Risk Management platform, allowing you to continuously identify and assess your most critical third-party vendors. To wrap up, DORA represents a significant step forward in creating a more resilient financial sector, and by embracing its requirements, organizations can better protect themselves and their customers in an increasingly digital world.

FAQs

1. How can organizations get ready for the Digital Operational Resilience Act (DORA)?

Organizations should perform regular cyber resilience tests as mandated by DORA. This includes vulnerability assessments, penetration testing, red team exercises, tabletop simulations, and third-party risk assessments to ensure robust cyber defenses.

2. What is the connection between operational resilience and risk management?

Operational resilience is closely tied to risk management, which deals with the processes, people, systems, and external factors that could potentially lead to operational disruptions. These components are critical as they represent potential points of failure from both internal and external threats.

3. What are the three main components of operational resilience?

Operational resilience is structured around three key elements:

- Identification and Preparation: Recognizing and readying for potential threats.
- Response and Adaptation: Effectively managing and adapting to disruptions.
- Recovery and Learning: Bouncing back from incidents and gaining insights to prevent future occurrences.

4. In what ways does the Digital Operational Resilience Act support the European Digital Finance Strategy?

DORA establishes a unified regulatory framework for digital operational resilience, requiring all relevant firms across EU member states to ensure they can endure, respond to, and recover from ICT-related disruptions and threats. This contributes to a more resilient digital finance environment across Europe.

References

[1] - https://www.digital-operational-resilience-act.com