

## 10 Insights for DORA Compliance



### 1. Understand the Importance of DORA:

The Digital Operational Resilience Act (DORA) is a regulation that focuses on security requirements for financial sector organizations and their third-party service providers. Recognize the significance of DORA and its impact on your business.



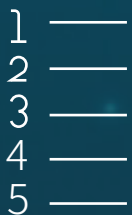
### 2. Start Early:

Begin your DORA compliance efforts well before the enforcement date (17 January 2025) to allow ample time for assessment, planning, and implementation.



### 3. Distinguish Regulation from Directive:

Unlike a directive, DORA is a regulation, meaning it will be in effect without the need for further translation into laws. Understand the implications of this distinction and the urgency it brings to compliance efforts.



### 4. Familiarize Yourself with the 5 Pillars of DORA:

DORA is structured around five pillars that address specific areas of digital resilience. These pillars include risk management, third-party risk management, incident reporting, information sharing, and digital operational resilience testing. Gain a deep understanding of each pillar and its requirements.



### 5. Prioritize Risk Management:

The risk management pillar of DORA focuses on identifying, assessing, and mitigating risks associated with operational resilience. Establish internal governance and control frameworks to effectively manage ICT risks and ensure a high level of operational resilience.





## 6. Assess Third-Party Risks:

Third-party risk management is a crucial aspect of DORA compliance. Evaluate and manage the risks posed by your third-party service providers. Follow the key principles outlined in DORA to establish sound management practices and robust contractual relationships.



## 7. Implement Incident Reporting Processes:

Promptly reporting significant operational disruptions or cyber incidents is a critical requirement of DORA. Define and establish a management process to detect, manage, and notify incidents as part of your ICT-related incidents management process.



## 8. Foster Information Sharing:

Collaboration and the exchange of cyber threat intelligence among organizations are encouraged by DORA. Establish information-sharing arrangements to enhance digital operational resilience. Raise awareness of cyber threat information, indicators of compromise, tactics, and cybersecurity alerts.



## 9. Embrace Digital Operational Resilience Testing:

Regular testing is essential to ensure operational resilience. Establish and maintain a comprehensive digital operational resilience program as part of your ICT risk management framework. Regularly review and update your testing approach to stay ahead of emerging threats.



## 10. Leverage Software Security Solutions:

To achieve DORA compliance, organizations involved in finance, insurance, and customer data within the EU can benefit from partnering with a trusted software security provider. Veracode, for example, offers comprehensive testing capabilities aligned with DORA's requirements, including Static Analysis (SAST), Dynamic Analysis (DAST), Penetration Testing (PTaaS), and Software Composition Analysis (SCA).

