reflectiz

Protecting Your Financial Institution

DORA COMPLIANCE CHECKLIST

Comply with DORA by January 2025 with the complete checklist for financial institutions

What is DORA?

DORA stands for the Digital Operational Resilience Act, a European regulation targeting financial institutions' cybersecurity. It aims to make financial systems more resistant to disruptions by requiring:

Stronger data protection

Financial firms must have board-approved plans to safeguard data and prevent breaches.

Clear communication

They need plans for communicating ICT incidents effectively.

Third-party vetting

Risks from ICT service providers need to be addressed.

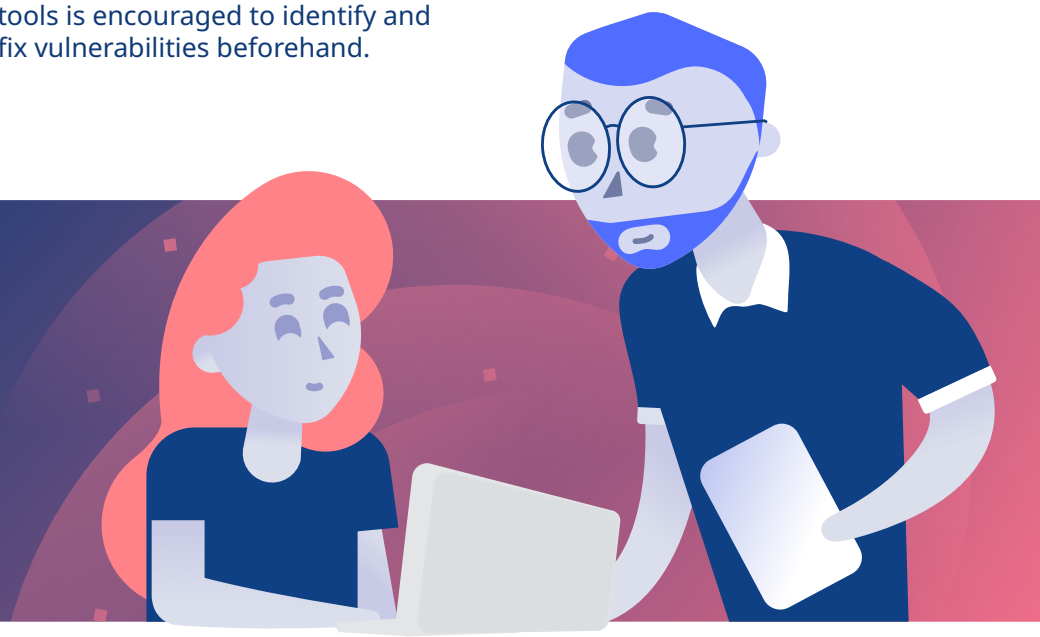
Information sharing

Collaboration between organizations is promoted so they stay informed about evolving cyber threats.

Proactive measures

Regular testing with automated tools is encouraged to identify and fix vulnerabilities beforehand.

Importantly, even if those infrastructure providers are outside of the EU but serve companies within it, they must still satisfy certain DORA requirements.



The Five Pillars of DORA

DORA contains five main pillars:

Board oversight

Requires board approval of a strategy to protect data and prevent breaches.

Incident reporting

Mandates clear communication plans for ICT incidents.

Resilience testing

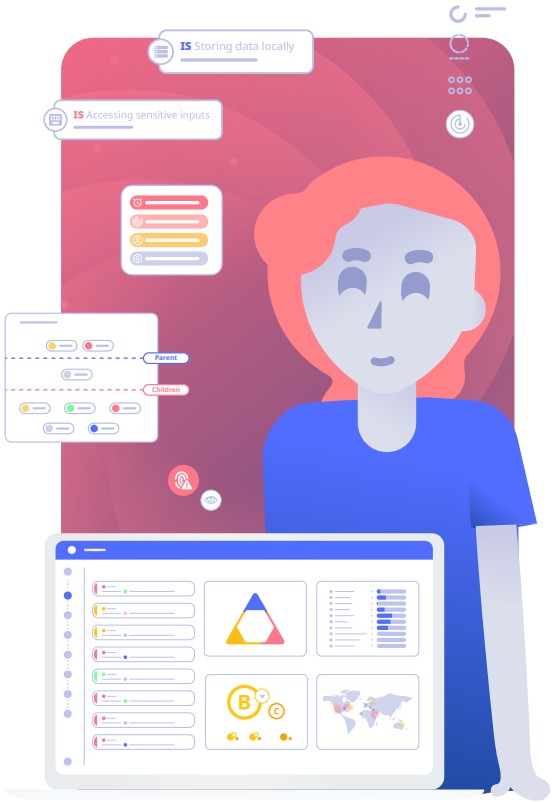
Promotes the use of automated tools to proactively identify and fix vulnerabilities.

Third-party risk management

Addresses risks from ICT service providers.

Threat intelligence sharing

Encourages collaboration so organizations stay informed about cyber threats.



DORA for the Web: How Reflectiz Helps

Reflectiz is a cybersecurity company specializing in web security, privacy, and compliance. Years of research by infosec experts have gone into the creation of our cutting-edge platform, which global companies are now using to keep their websites safe and compliant with industry-specific regulations. Reflectiz, recognized by Gartner for innovation in website security, is ready to face today's web threats head-on, making the internet a safer place for both businesses and their customers.

The Complete Checklist

Learn how Reflectiz can help you meet the DORA regulations by covering the following of its articles:

- **Article 5 | Governance and Organization**
  Reflectiz reviews and approves the use of web third-party applications, defines permissible actions, monitors for unauthorized behaviors, assesses risks, and evaluates overall website risk exposure.

- **Article 6 | ICT Risk Management Framework**
  Reflectiz offers alert mechanisms with approval processes for quick responses, manages risk exposure ratings, and aligns with your company's risk appetite. The comprehensive Reflectiz Dashboard provides detailed asset information and categorized alerts for efficient monitoring.

- **Article 6 | Holistic ICT Multi-Vendor Strategy**
  Reflectiz maintains a detailed third-party apps inventory, including risk factors and potential justifications for each application, ensuring thorough risk assessment and transparency.

Article 8 | Identification
Reflectiz's Exposure Rating measures website risk levels within industry contexts for a comprehensive assessment. It maintains a third-party asset inventory that's updated regularly to reflect major changes.

Article 9 | Protection and Prevention
Reflectiz's Exposure Rating measures website risk levels within industry contexts for a comprehensive assessment. It maintains a third-party asset inventory that's updated regularly to reflect major changes.

Article 10 | Detection
Reflectiz integrates with ticketing apps and SIEM, providing multi-layered control mechanisms, alert thresholds, and automated responses for ICT-related incidents. To comply with Article 10.1's requirement for prompt detection of anomalous activities and identification of potential single points of failure in ICT infrastructure, Reflectiz offers its advanced alerting mechanism.

Article 11 | Response and Recovery
Reflectiz features an on-demand blocking mechanism activated by detailed alert information, facilitating immediate containment and response to incidents.

Article 13 | Learning and Evolving
Reflectiz leverages its cyber-attack expertise and customer insights to continuously update its platform with new risk factors and assessments, enhancing threat detection and mitigation.

Article 17 | ICT-related incident management process
Reflectiz offers a detailed incident report with timelines and risk ratings, enabling proactive management and industry benchmarking of cybersecurity risks.

Article 31 | Designation of critical ICT third-party service providers
Reflectiz empowers you to streamline your cybersecurity response. Its system features alerts with approval workflows for faster action and manages risk exposure with dynamic ratings. The comprehensive dashboard provides detailed asset information and categorized alerts for efficient monitoring. Additionally, Reflectiz offers transparency into third-party risks by maintaining a detailed inventory that includes potential risk factors and justifications for each application. We also measure the popularity of third-party vendors among specific industries, including G-SIIs and O-SSIs. It can even suggest alternatives for low-popularity vendors, strengthening your overall security posture.