

DORA - Digital Operational Resilience Act - aims to ensure that financial entities within the EU can withstand, respond to, and recover from all types of ICT-related disruptions and threats. **The DORA Directive will enter into force on January 17th 2025.**

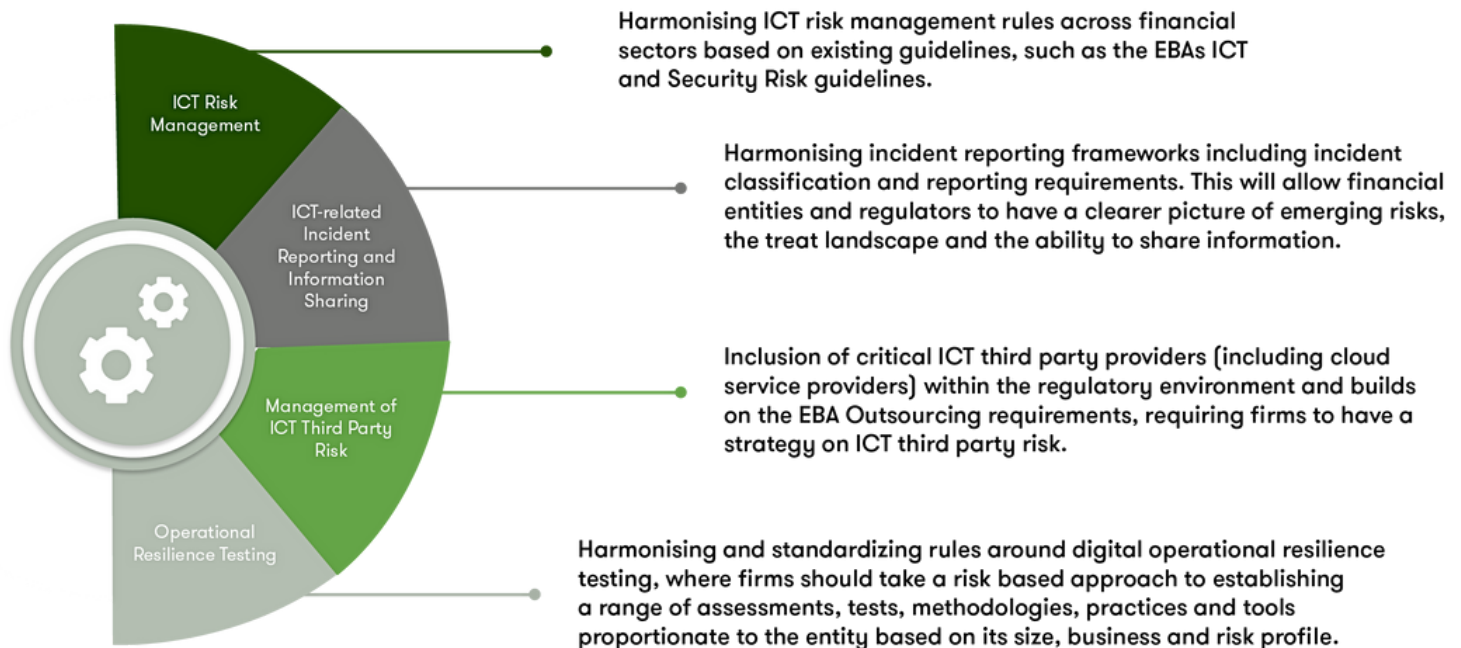
ENTITIES COVERED BY THE DIRECTIVE

EU's financial sector and suppliers of ICT services to that sector – wherever those suppliers are based:

- Central securities depositories
- Central counterparties
- Account information service providers
- Payment institutions and electronic money institutions
- Trading venues and trade repositories
- Administrators of critical benchmarks
- Credit rating agencies
- Data reporting service providers
- Institutions for occupational retirement provision
- Insurance and reinsurance undertakings
- Managers of alternative investment funds (AIFMs) and management companies
- Securitisation repositories

RESPONSIBILITIES IN RELATION TO THE DIRECTIVE

DORA is coming to force in order to lower the potential risk of a bank, insurance company or investment firm and its customers suffering downtime or data loss as the result of a cyber-attack.

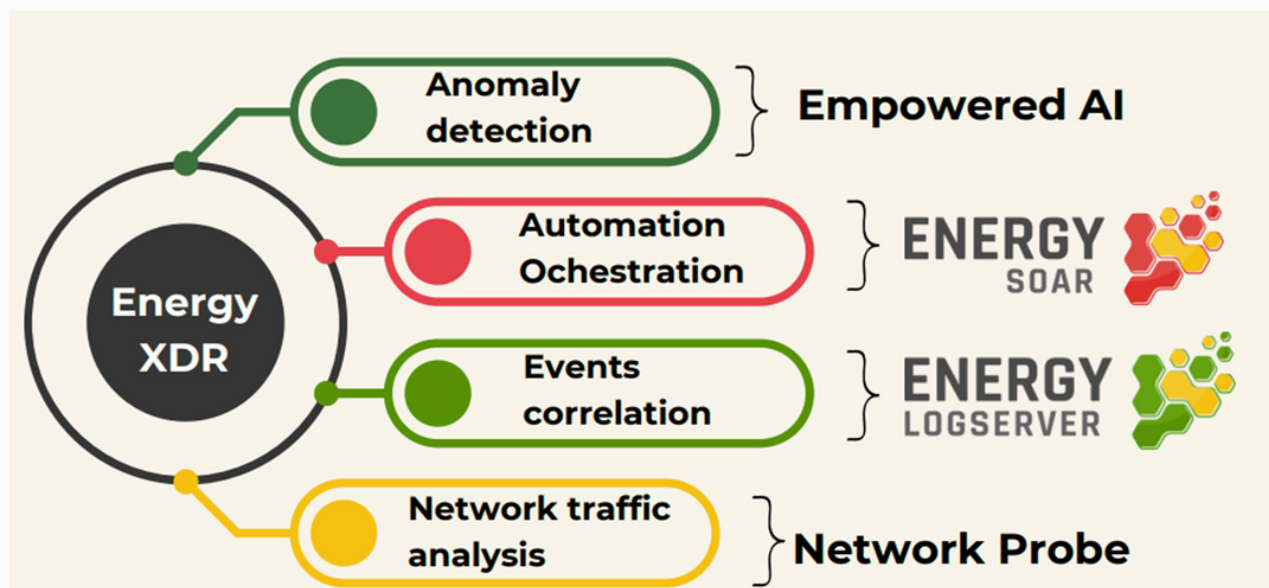


DORA establishes rigorous **financial penalties** for violations of its requirements. A breach could see institutions fined up to **2%** of their total annual worldwide turnover or up to **1% of the company's average daily turnover worldwide**.

Third-party **ICT service providers** may face fines of **up to EUR 5,000,000** or, in the case of an individual, a maximum fine of **EUR 500,000** for non-compliance with the Act's requirements.

HOW ENERGY LOGSERVER CAN PREPARE YOU FOR DORA?

OUR SOLUTIONS



DORA COMPLIANCE CHECKLIST:

ICT Risk Management:

- **SIEM:** Aggregates and analyzes security data from across the organization, identifying potential risks and vulnerabilities.
- **XDR:** Provides a unified view of threats across multiple environments (network, endpoint, servers, etc.), enhancing risk management capabilities.

Incident Reporting:

- **SIEM:** Automatically collects and correlates security events, helping to quickly identify and report major incidents.
- **SOAR:** Automates the incident response process, ensuring timely and accurate reporting to regulatory authorities.

Regular Testing:

- **SOAR:** Facilitates automated and continuous security testing and validation processes.
- **SIEM:** Enhances threat detection capabilities through continuous monitoring and advanced analytics.

Third-Party Risk Management:

- **SIEM:** Monitors third-party activities and integrates their logs into the broader security monitoring framework.
- **SOAR:** Automates the assessment and management of third-party risks.

If you need support in preparing for DORA, or if you'd like to explore how your organisation can take steps to enhance its overall cyber security posture, contact us to learn more.