Trustwave®

DORA Readiness Accelerator

PREPARE FOR DORA COMPLIANCE AND INCREASE OPERATIONAL RESILIENCE

Benefits

- Access a team of Trustwave consultants with deep subject matter expertise in governance, risk, and compliance.
- Align compliance processes to minimize disruption and optimize costs.
- Evaluate ICT third-party providers to ensure compliance with oversight requirements and increase visibility into your vendor partners.
- Proactively protect your security investments from potential vulnerabilities.
- Identify security weaknesses and corrective actions for the DORA requirements.
- Ensure preparedness for audits and inspections by authorities.

The Digital Operational Resilience Act (DORA) is a European Union (EU) regulation aimed at fortifying the financial sector against cyber risks and operational disruptions. The Council of the European Union and the European Parliament formally adopted DORA in November 2022, with DORA taking effect on January 17, 2025.

As part of DORA, organizations will need to strengthen their risk management frameworks and incident reporting processes, enhance operational resilience, and implement rigorous oversight of their information and communication technology (ICT) third-party providers. This regulation represents not only a regulatory obligation but also an opportunity for organizations to build more resilient, secure, and future-proof operations that minimize vulnerabilities and enhance customer trust.

The Trustwave DORA Readiness Accelerator provides you with a roadmap to prepare your security programs for DORA compliance. Trustwave will provide guidance and remediation planning to help you align with the DORA requirements.

Understanding DORA

DORA is a regulatory framework established by the EU to strengthen the operational resilience of financial institutions against technology and cyber risks. DORA applies broadly across the financial sector in the EU:

- **Financial Entities** – Banks, payment service providers, investment firms, etc.
- **ICT Third-Party Providers to Financial Entities** – Cloud computing vendors, software providers, outsourced technology partners, etc.

The European Supervisory Authorities (ESAs) are empowered to impose substantial fines on organizations that fail to comply with DORA. For instance, organizations that violate DORA's requirements face fines of up to 2% of their total annual worldwide turnover, and ICT third-party providers designated as critical by the ESAs face fines of up to EUR 5 million.

DORA's framework is built around five key pillars, each designed to strengthen different aspects of operational resilience:

1. **ICT Risk Management:** Focuses on ensuring that financial entities have robust frameworks for managing risks associated with ICT.
2. **ICT-Related Incident Management, Classification, & Reporting:** Establishes a standardized process for reporting ICT-related incidents to authorities.
3. **Digital Operational Resilience Testing:** Mandates regular testing of digital systems, including penetration testing, to ensure resilience against disruptions.
4. **Managing of ICT Third-Party Risks:** Addresses the risks associated with outsourcing ICT services to third-party providers.
5. **Information Sharing Arrangements:** Encourages collaboration between financial entities by facilitating the exchange of information on threats, vulnerabilities, and incidents.

The Approach

Trustwave produces a roadmap for you to prepare for DORA compliance and increase operational resilience, and can adopt a modular, pillar-based approach to address your specific requirements for DORA compliance:

1. **Requirements Gathering:** Trustwave works with you to outline the DORA requirements and identify the in-scope areas based on DORA. This includes reviewing the DORA articles and requirements and defining the assessment scope to establish clear boundaries.
2. **Gap Analysis:** Trustwave conducts a gap analysis to identify weaknesses in your current in-scope security and resilience programs as they pertain to DORA. This includes reviewing existing policies, procedures, and technical controls, and identifying areas that need improvement.
3. **Roadmap Development:** Trustwave works with you to develop a prioritized roadmap tailored to your needs, based on findings from the gap analysis. This includes developing recommendations for addressing identified gaps and best-practice controls to meet DORA requirements.

Implementation Support: Trustwave can also help you implement changes to your security environment in alignment with DORA requirements. Implementation services may include implementing the corrective actions from the roadmap or any other activities that you are looking to achieve to increase your operational resilience, such as providing Trustwave Managed Vendor Risk Assessment, Trustwave Penetration Testing, or Trustwave Scenario-Based Crisis Simulation. Implementation services are not included in the DORA Readiness Accelerator service but may be purchased separately.

Microsoft & DORA

Trustwave is endorsed and validated by Microsoft as a leading cybersecurity partner.

Microsoft provides a broad set of ICT risk management and incident management, classification, and reporting capabilities in their services. This includes Microsoft Defender for Cloud, Microsoft Purview, Microsoft 365 Service Health Dashboard, Microsoft Secure Score, and Azure Security Center.

Trustwave can help you prepare for DORA with Microsoft Security via the Trustwave Accelerators for Microsoft Security service. This service provides you with a roadmap to accelerate value and security outcomes from Microsoft Security products.

Build, Test, & Run a Secure Organization

Trustwave's range of capabilities help you get the right service to suit your specific needs:

Cyber Advisory Services:

- Digital Forensics & Incident Response
- Threat Detection & Response
- Managed Vendor Risk Assessment
- Scenario-Based Crisis Simulation
- Data Protection
- Governance, Risk, & Compliance
- Security Colony
- Technology Partnerships
- Executive & Technical Training
- Threat Intelligence as a Service

Security Testing Services:

- Penetration Testing (Network, Application – Internal, External, Wireless)
- Vulnerability Scanning (Discovery, Network, Application, Database)
- Red/Purple Teaming
- Intrusion Detection & Prevention
- Database Security (DbProtect, AppDetectivePRO)
- Secure Email & Web Gateways
- Physical Assessments

Managed Security Services:

- Managed Threat Detection & Response
- Co-Managed SIEM/SOC
- Security Technology Management
- Managed Web Application Firewall
- Proactive Threat Hunting

Trustwave®

www.trustwave.com