LevelBlue

DORA Maturity Accelerator

Prepare for DORA compliance and increase operational resilience.

The Digital Operational Resilience Act (DORA) is a European Union (EU) regulation to fortify the financial sector against cyber risks and operational disruptions. It's an opportunity for organizations to build more resilient, secure operations.

Understanding DORA

- **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 bult 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.

Benefits

- Access a team of LevelBlue 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 approach

LevelBlue delivers a tailored roadmap to help you prepare for DORA compliance and strengthen operational resilience. Using a modular, pillar-based model, LevelBlue addresses your specific regulatory needs:

1. **Requirements Gathering:** LevelBlue outlines the DORA requirements, reviews applicable articles, and defines the scope to ensure clear compliance boundaries.
2. **Gap Analysis:** A detailed review of your current security and resilience programs identifies gaps in policies, procedures, and technical controls that must be remediated to meet DORA expectations.
3. **Roadmap Development:** Based on gap analysis results, LevelBlue builds a prioritized, best-practice-aligned roadmap with recommendations to close gaps and achieve compliance.

Implementation support (optional): LevelBlue can assist in executing roadmap recommendations, including corrective actions, managed vendor risk assessments, penetration testing, and crisis simulations. These services are available separately from the DORA Maturity Accelerator.

Microsoft and DORA

As an endorsed Microsoft cybersecurity partner, LevelBlue (formerly Trustwave) helps you leverage Microsoft's ICT risk and incident management capabilities, such as Defender for Cloud, Purview, Secure Score, and Azure Security Center, to prepare for DORA. LevelBlue Accelerators for Microsoft Security provide a structured plan to maximize value from Microsoft Security tools.

Build, test, and run a secure organization

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

Cyber Advisory Services:

- Digital Forensics and Incident Response
- Threat Detection and Response
- Managed Vendor Risk Assessment
- Scenario-Based Crisis Simulation
- Data Protection
- Governance, Risk, and 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 and 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