Omada

DORA

Compliance Playbook

The Digital Operational Resilience Act (DORA) aims to strengthen the digital operational resilience of the EU's financial sector by establishing a harmonized, technology-neutral regulatory framework. It applies to a wide range of financial entities—such as banks, investment firms, insurance companies, and payment service providers—as well as their critical ICT service providers. DORA's core pillars include:

- robust internal governance and oversight,
- a comprehensive ICT risk management framework,
- thorough digital operational resilience testing,
- effective management of ICT third-party risk,
- streamlined ICT incident reporting.

This playbook serves as a resource for professionals responsible for safeguarding their organization's digital resilience, including CISOs, Compliance Officers, Risk Managers, and other senior decision-makers. It outlines the key obligations, practices, and procedures needed to comply with DORA's regulatory framework, ensuring that stakeholders can methodically identify gaps, implement solutions, and drive continuous improvement. By addressing a wide range of operational, governance, and technical considerations, this playbook provides leadership with practical guidance to navigate the evolving landscape of digital operational resilience within the EU's financial sector.

Building a Strong Foundation

Any compliance initiative must begin with a strong foundation. This starts by identifying all relevant DORA-related obligations, technical standards, and guidelines, as well as determining the scope and applicability of DORA requirements, including criteria outlined in Article 16[1] for simplified ICT risk management frameworks. Applying the proportionality principle ensures that strategies are tailored to the organization's size, complexity, and risk profile. From the outset, management should endorse the initiative and assemble an implementation team dedicated to overseeing the entire rollout, ensuring smoother progress. Finally, establishing a systematic document management process to maintain DORA-related records sets the stage for ongoing, organized compliance.

Establish Internal Governance and Control

Performing a governance gap analysis establishes a baseline for identifying areas that require strengthening. Documenting roles, responsibilities, and formal structures helps senior management, committees, and critical functions—such as risk, compliance, internal audit, and business continuity—operate more effectively. In addition, updating codes of conduct, conflict of interest policies, and internal alert mechanisms ensures that all stakeholders work within a framework of integrity and transparency. This structured approach, supported by periodic executive training sessions and adequate budgetary resources, ultimately fosters a more resilient and cohesive governance environment.

Build and Strengthen the ICT Risk Management Framework (ICT RMF)

Conducting a gap analysis on existing ICT Risk Management Frameworks (ICT RMFs) establishes a foundation for setting a clear and tailored ICT and digital operational resilience strategy. This involves defining a customized ICT risk methodology and classifying all ICT assets to ensure comprehensive oversight and management. By identifying critical third-party ICT dependencies, managing legacy systems effectively, and regularly assessing ICT risks, the organization can proactively address potential vulnerabilities. Implementing robust ICT security measures—such as continuous monitoring, anomaly detection, and well-defined incident response plans—fortifies an organization's defenses against cyber threats. Integrating Identity Governance and Administration (IGA) solutions helps maintain strict control over user access to critical systems and data, ensuring that privileges aligned with defined roles, responsibilities, and regulatory requirements. Developing comprehensive business continuity functions, including crisis management protocols, backup and recovery processes, and system redundancies, prepares the organization to maintain operations during disruptions. Finally, gathering ongoing threat intelligence, measuring performance through key performance indicators (KPIs), and maintaining clear communication policies for both internal and external stakeholders further enhance the organization's ability to respond proactively to emerging risks and maintain digital resilience.

[1] https://www.digital-operational-resilience-act.com/Article_16.html

Omada

Incident Management and Reporting

Establishing a clear incident management process requires well-defined procedures that include both root cause analysis and comprehensive reporting frameworks, ensuring that every disruption is thoroughly understood and documented. By integrating processes for timely notification to authorities and promptly informing affected clients of major ICT-related incidents, the organization maintains transparency and compliance with regulatory expectations. In addition, tracking annual costs and losses related to these incidents, and keeping that information readily available, ensures that the organization can promptly respond to competent authority requests and continuously refine its resilience strategies.

Digital Operational Resilience Testing (DORT)

Implementing a continuous testing program allows for ongoing scrutiny of the organization's ICT environment, ensuring vulnerabilities are promptly identified and mitigated. By conducting annual evaluations of critical ICT systems, regularly performing vulnerability assessments, and organizing threat-led penetration tests (TLPTs), the organization maintains a proactive stance against emerging threats. Meticulous documentation of results, remediation plans, and proof of adherence to DORA testing guidelines further demonstrates a structured, diligent approach to sustaining digital operational resilience.

Third-Party Risk Management (ICT TPRM)

Establishing comprehensive policies for managing ICT third-party risks involves classifying providers according to criticality, determining appropriate oversight mechanisms, and ensuring transparency throughout the supply chain. Maintaining an up-to-date register of all contractual arrangements and fulfilling reporting obligations reinforces accountability, while embedding resilience requirements within contracts strengthens the organization's defense against potential disruptions. By incorporating thorough due diligence procedures into procurement processes, carefully planning exit strategies, and continuously monitoring third-party performance, the organization creates a robust, adaptable framework that safeguards its digital operational resilience over time.

Information-Sharing Arrangements

Engaging in voluntary information-sharing arrangements to exchange cyber threat intelligence strengthens the organization's collective security posture and increases awareness of emerging risks. Proactively notifying authorities of these collaborations and maintaining thorough documentation of each partnership ensures that the information-sharing efforts remain transparent, accountable, and aligned with regulatory expectations.

Continuous Improvement and Final Steps

Reviewing and adjusting the ICT Risk Management Framework (ICT RMF) each year and readily reporting updates to authorities upon request ensures the organization remains aligned with evolving standards. Completing a final gap analysis confirms full compliance, revealing opportunities for refinement and strengthening of safeguards. Committing to ongoing enhancements, evidence-based corrective actions, and incremental improvements ensures continued adherence to DORA and fosters a culture of continuous operational resilience.

The latest regulatory text, along with any subsequent Technical Standards, Guidelines, and Recommendations, can be found through the EU's official legal database (EUR-Lex: https://eur-lex.europa.eu/) and the websites of the European Supervisory Authorities. DORA entered into force on 16 January 2023 and will apply as of 17 January 2025.

Omada

Checklist for DORA Compliance

This checklist serves as a structured pathway, guiding organizations through understanding requirements, setting strategies, testing resilience, managing third-party risks, and continuously refining their digital operational resilience capabilities in line with DORA's obligations. By following these steps, entities establish a secure, reliable foundation for long-term digital resilience.

Foundation

- [ ] Compile and review all DORA requirements and supportive guidelines
- [ ] Define DORA's scope and relevance to your organization
- [ ] Apply proportionality considerations to tailor your approach
- [ ] Secure management buy-in and form an implementation team
- [ ] Create and maintain a DORA documentation framework

Governance and Control

- [ ] Complete a governance gap analysis
- [ ] Clearly define management roles and responsibilities
- [ ] Establish committees (Risk, Audit, Cybersecurity, etc.)
- [ ] Update corporate values, codes of conduct, and conflict of interest policies
- [ ] Strengthen risk, compliance, and internal audit functions
- [ ] Develop internal alert systems, new product approval policies, and business continuity functions
- [ ] Provide regular training and ensure proper resource allocation

ICT RMF

- [ ] Conduct a gap analysis of existing ICT risk frameworks
- [ ] Set ICT and digital resilience strategies aligned with DORA
- [ ] Define ICT risk management methodologies and identify assets
- [ ] Assess third-party dependencies, legacy systems, and conduct regular risk assessments
- [ ] Enhance ICT security measures, monitoring, and detection processes
- [ ] Implement business continuity strategies, crisis management, backups, and redundancies
- [ ] Gather threat intelligence, track KPIs, and deliver training and communication plans

Omada

Incident Management

- [ ] Develop a formal ICT incident management and reporting procedure
- [ ] Notify authorities and stakeholders of significant incidents
- [ ] Track annual incident-related costs and refine response strategies

Resilience Testing (DORT)

- [ ] Establish a resilience testing program
- [ ] Test critical ICT systems and applications annually
- [ ] Perform vulnerability assessments and regular threat-led penetration tests
- [ ] Document remediation measures and submit results as required

Continuous Improvement

- [ ] Review the ICT RMF annually and adapt as needed
- [ ] Conduct a final gap analysis to confirm compliance
- [ ] Continuously refine processes, implement corrective actions, and enhance resilience maturity

Information Sharing

- [ ] Engage in voluntary threat intelligence exchanges with peers and authorities
- [ ] Document arrangements and notify authorities of participation

Third-Party Risk Management

- [ ] Create strategies and policies for ICT third-party risks
- [ ] Maintain an up-to-date register of third-party arrangements
- [ ] Notify authorities of critical or important third-party functions
- [ ] Include necessary resilience clauses in contracts and plan exit strategies
- [ ] Conduct extended due diligence and maintain ongoing monitoring

Omada simplifies Identity Governance by providing a full-featured, cloud-native IGA solution that streamlines the complex processes of managing user identities, access, and entitlements. With a focus on automation and user-centric design, Omada reduces manual tasks and enhances operational efficiency, ensuring that organizations can easily enforce security policies, comply with regulations, and manage user access at scale. By leveraging advanced technologies such as AI-driven decision-making and role-based access control (RBAC), Omada enables businesses to achieve stronger security, better compliance, and improved user experiences—without the complexities traditionally associated with identity governance.

V020124