

DORA Compliance for CASPs

— All You Need To Know

00. What is DORA?

The Digital Operational Resilience Act (DORA) is a new EU regulation, effective from January 2025, mandating financial entities, including CASPs, to enhance their digital resilience. DORA covers ICT risk management, incident reporting, third-party risk, and resilience testing.

01. Why DORA Matters for CASPs

Increased ICT reliance means greater risk exposure. DORA ensures CASPs like you have measures in place to protect operations and client assets from cyber threats and ICT disruptions.

BUSINESS CONTINUITY
Creating backup plans for wallet infrastructure or off-chain data.

ENHANCED SECURITY
Protecting private keys and client data with regular testing and encryption.

02. Key Areas Impacted by DORA

Incident Management

Identify, classify, and report ICT-related incidents to regulatory authorities.

Third-party Risk Management

Vet ICT providers, assess contract terms, and prepare for exit if standards aren't met.

ICT Risk Management

Policies to protect ICT assets, assess vulnerabilities, and address interdependencies.

Governance & Organization

Establish ICT risk management frameworks with clear roles, responsibilities, and oversight.

03. Key Areas Impacted by DORA

Navigating DORA's requirements can be challenging due to:

THIRD-PARTY MANAGEMENT
Managing ICT service providers' compliance with in-house resources.

CLEAR FUNCTION CLASSIFICATION
Defining critical functions and ICT dependencies.

INCIDENT REPORTING
Standardize reports with frameworks like PSD2.

04. Next Steps for DORA Compliance

DORA readiness requires strategic action across your organization. By following these steps, you'll establish a strong compliance foundation and proactively manage digital operational risks:

START THE PROGRAM
Bring together key teams from IT, compliance, risk, and legal. Set clear goals aligned with DORA's standards and outline a timeline for meeting each requirement. Early engagement across departments ensures cohesive planning and smoother implementation.

DEVELOP POLICIES
Define and document policies that cover ICT risk management, third-party oversight, and incident handling. These policies provide a clear structure for managing risks and support your team in following consistent processes.

TEST SYSTEMS
Regular resilience tests on ICT systems are essential to identify weaknesses before they become critical. Independent assessments will give an objective view of your system's readiness and ensure compliance with DORA's testing requirements.

TRAIN TEAMS
Equip your team with the knowledge and skills they need to manage DORA requirements. Regular training on new processes and updated standards will prepare staff to respond quickly to incidents, maintain compliance, and strengthen overall resilience.

Stay ahead of DORA requirements and build a resilient foundation.

About Us

We are digital asset enthusiasts with backgrounds in compliance, traditional banking, and cybersecurity who want to help shape the future of digital assets. As digital assets are adopted globally, we are building the relevant tools to assist financial institutions in staying updated with the ever-evolving regulatory landscape. We know that regulations of digital assets and interoperability with traditional finance will foster the trust necessary to set mass adoption in motion and offer consumers protection.

The company provides Software-as-a-Service modular solutions to automate and orchestrate compliance processes, including Travel Rule and Blockchain Analytics. We serve customers in the digital asset industry, empowering teams to comply with complex anti-money laundering (AML) and Counter-Terrorism Financing (CTF) requirements at the global and local levels.

Preferred solution by XRP LEDGER | techstars | ^aGTM

Let's connect!

To get you started or learn more about how we can help your company, use the resources below.



DORA Compliance Checklist for CASPs

Governance and Organization

- Establish an internal ICT risk management framework with roles and responsibilities.
- Approve business continuity, response, and recovery plans for ICT disruptions.
- Allocate a dedicated budget for digital resilience efforts.
- Implement a reporting and oversight structure to monitor ICT risk management.

ICT Systems, Protocols, and Tools

- Ensure ICT systems are scalable, resilient, and capable of handling high data volumes.
- Verify that data processing and storage systems (including non-cloud storage) meet DORA's reliability requirements.

Detection Systems

- Establish mechanisms to detect and report anomalies and unusual activities in ICT systems.
- Set alert thresholds to trigger timely incident response. Test systems to prevent single points of failure in ICT infrastructure.

Protection and Prevention Measures

- Implement secure ICT solutions, including encryption, multi-factor authentication, and network segmentation for critical assets.
- Regularly update and patch systems to address emerging security vulnerabilities.
- Enforce strict access control policies for sensitive data and systems.

Digital Operational Resilience Testing

- Conduct annual resilience tests on critical ICT systems, engaging independent testers where feasible.
- Prepare Threat-Led Penetration Testing (TLPT) exercises, with regulator coordination if required.

Third-Party Risk Management

- Maintain a register of ICT third-party providers, noting critical services like wallet management or KYC.
- Establish DORA-compliant contracts with providers, covering inspection rights, exit strategies, and service level agreements (SLAs).
- Regularly assess third-party providers for resilience and compliance, especially those providing critical services.
- Plan exit strategies for non-compliant third-party providers to minimize service disruption risks.

ICT Risk Management Framework

- Develop and document ICT risk policies, including data protection, incident prevention, and regular reviews.
- Conduct regular assessments to identify vulnerabilities, cyber threats, and risks to ICT assets.
- Update ICT risk management protocols and resilience measures as technology and threats evolve.

Identifying ICT Risks

- Document all ICT-supported business functions and dependencies within your organization.
- Conduct periodic risk assessments, especially before major infrastructure or operational changes.

Business Continuity and Recovery

- Prepare continuity plans detailing actions during ICT disruptions to ensure ongoing service.
- Establish containment procedures to isolate affected areas during an incident.
- Define backup and recovery processes, specifying frequency and data criticality levels.

Incident Management and Reporting

- Record and classify ICT incidents by their economic and operational impact.
- Set up a system to report major incidents to regulators in the initial, intermediate, and final stages.
- Notify affected clients when necessary, detailing the incident's impact and recovery status.

Ongoing Training and Awareness

- Train relevant teams on DORA requirements, emphasizing incident management and reporting protocols.
- Set up regular updates and refresher training to keep staff informed of changes in compliance practices.

Self-Assessment Questions for CASPs

1. Are all ICT-supported business functions and their dependencies documented?
2. Do we have clear incident response protocols, and are they tested regularly?
3. Is there a contingency plan if a critical third-party provider fails to meet DORA standards?
4. Are key roles and responsibilities clearly assigned within our ICT risk management framework?