ospree

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.





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.

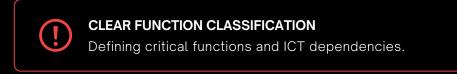
Governance & Organization

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:





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, thirdparty 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.





Let's connect!

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











ospree

DORA Compliance Checklist for CASPs



Governance and Organzation		ICT Risk Management Framework	
\bigcirc	Establish an internal ICT risk management framework with roles and responsibilities.	\bigcirc	Develop and document ICT risk policies, including data protection, incident prevention, and regular reviews.
\bigcirc	Approve business continuity, response, and recovery plans for ICT disruptions.	\bigcirc	Conduct regular assessments to identify vulnerabilities, cyber threats, and risks to ICT assets.
\bigcirc	Allocate a dedicated budget for digital resilience efforts.	Update ICT risk management protocols and resilience measures as technology and threats evolve.	
\bigcirc	Implement a reporting and oversight structure to monitor ICT risk management.		
ICT	Systems, Protocols, and Tools	lder	ntifying ICT Risks
\bigcirc	Ensure ICT systems are scalable, resilient, and capable of handling high data volumes.	\bigcirc	Document all ICT-supported business functions and dependencies within your organization.
\bigcirc	Verify that data processing and storage systems (including non-cloud storage) meet DORA's reliability requirements.	\bigcirc	Conduct periodic risk assessments, especially before major infrastructure or operational changes.
Detection Systems		Business Continuity and Recovery	
\bigcirc	Establish mechanisms to detect and report anomalies and unusual activities in ICT systems.	\bigcirc	Prepare continuity plans detailing actions during ICT disruptions to ensure ongoing service.
\bigcirc	Set alert thresholds to trigger timely incident response. Test systems to prevent single points of failure in ICT infrastructure.	\bigcirc	Establish containment procedures to isolate affected areas during an incident.
		\bigcirc	Define backup and recovery processes, specifying frequency and data criticality levels.
Protection and Prevention Measures		Incident Management and Reporting	
\bigcirc	Implement secure ICT solutions, including encryption, multi-factor authentication, and network segmentation for critical assets.	\bigcirc	Record and classify ICT incidents by their economic and operational impact.
	Regularly update and patch systems to address emerging security vulnerabilities.	\bigcirc	Set up a system to report major incidents to regulators in t initial, intermediate, and final stages.
\bigcirc	Enforce strict access control policies for sensitive data and systems.	\bigcirc	Notify affected clients when necessary, detailing the incident's impact and recovery status.
Digital Operational Resilience Testing		Ong	joing Training and Awareness
\bigcirc	Conduct annual resilience tests on critical ICT systems, engaging independent testers where feasible.	\bigcirc	Train relevant teams on DORA requirements, emphasizing incident management and reporting protocols.
	Prepare Threat-Led Penetration Testing (TLPT) exercises, with regulator coordination if required.	0	Set up regular updates and refresher training to keep staff informed of changes in compliance practices.
Th	ed Porty Diek Monogoment	Cald	Accoment Questions for CASPs

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.

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?
- Are key roles and responsibilities clearly assigned within our ICT risk management framework?