SILVERFORT

Comply with Digital Operational Resilience Act (DORA) Requirements with Silverfort

What is the Digital Operational Resilience Act?

The Digital Operational Resilience Act, or DORA, is a European Union (EU) regulation that creates a binding, comprehensive information and communication technology (ICT) risk management framework for the EU financial sector. DORA establishes technical standards that financial entities and their critical third-party technology service providers must implement in their ICT systems by January 17, 2025.

The goal of DORA is to address ICT risk management in the financial services sector comprehensively and to harmonize the ICT risk management regulations that exist in individual EU member states.

What Are DORA's Requirements?

DORA establishes technical requirements for financial entities and ICT providers across four domains: ICT risk management and governance, incident response and reporting, resilience testing, and third-party risk management. Information sharing is encouraged but not required. Requirements will be enforced proportionately, meaning smaller entities will not be held to the same standards as major financial institutions.

DORA requires financial firms to use measures to protect against ICT-related risks. To achieve this, DORA requirements also cover third parties, like cloud providers. Financial sectors impacted by DORA include:

- **Credit institutions**
- **Payment institutions**
- **Electronic money institutions**
- **Investment firms**
- **Crypto-asset service providers**
- **Alternative investment funds**
- **Insurance managers**
- **Critical ICT third-party providers servicing covered entities**

With DORA, the EU aims to establish a universal framework for managing and mitigating ICT risk in the financial sector. By standardizing risk management rules across the EU, DORA seeks to remove the gaps, overlaps, and conflicts that could arise between disparate regulations in different EU states. A shared set of rules can make it easier for financial entities to comply while improving the entire EU financial system's resilience by ensuring every institution is held to the same standard.

Compliance Table: Silverfort Alignment to DORA's Requirements

DORA Requirement	Details	Silverfort
Article 8 Identification	**8.4.** Financial entities shall identify all information assets and ICT assets, including those on remote sites, network resources and hardware equipment, and shall map those considered critical. They shall map the configuration of the information assets and ICT assets and the links and interdependencies between the different information assets and ICT assets.	✓
	8.7. Financial entities, other than microenterprises, shall on a regular basis, and at least yearly, conduct a specific ICT risk assessment on all legacy ICT systems and, in any case before and after connecting technologies, applications or systems.	✓
Article 9 Protection and prevention	**9.4** As part of the ICT risk management framework referred to in Article 6(1), financial entities shall:	
	(c) implement policies that limit the physical or logical access to information assets and ICT assets to what is required for legitimate and approved functions and activities only, and establish to that end a set of policies, procedures and controls that address access rights and ensure a sound administration thereof;	✓
	(d) implement policies and protocols for strong authentication mechanisms, based on relevant standards and dedicated control systems, and protection measures of cryptographic keys whereby data is encrypted based on results of approved data classification and ICT risk assessment processes;	✓
Article 10 Detection	**10.1** Financial entities shall have in place mechanisms to promptly detect anomalous activities, in accordance with Article 17, including ICT network performance issues and ICT-related incidents, and to identify potential material single points of failure.	✓
	10.3 Financial entities shall devote sufficient resources and capabilities to monitor user activity, the occurrence of ICT anomalies and ICT-related incidents, in particular cyber-attacks.	✓