



Mastering DORA compliance



What is DORA?

The EU's Digital Operational Resilience Act (DORA) is a regulation intended to strengthen the information and communication technology (ICT) resilience of financial institutions. It sets standards to help businesses withstand, respond to, and recover from ICT disruptions. Financial companies must comply by 17 January 2025.

KEY REQUIREMENTS

- ICT risk monitoring
- ICT risk management framework
- Incident reporting
- Operational resilience testing
- Third-party risk management
- Governance, organisation, and oversight
- Information sharing and cooperation
- Compliance and enforcement

 Requirements	 How to fulfill
<p>CONTRACT COMPLIANCE</p> <p>All contract terms and conditions must meet DORA's comprehensive regulatory requirements.</p>	<p>Use automated contract creation to reduce complexity and ensure all clauses comply with DORA regulations.</p>
<p>DATA SECURITY</p> <p>Stringent data protection measures must be complied with for all contracts.</p>	<p>Implement a robust data encryption and secure storage system to meet data protection requirements.</p>
<p>THIRD-PARTY RISK MANAGEMENT</p> <p>Contractual obligations with third-party vendors must be managed and monitored.</p>	<p>Leverage tools for tracking and managing third-party vendor compliance.</p>
<p>DOCUMENTATION AND REPORTING</p> <p>Thorough records and documentation must be maintained for audits and compliance reporting.</p>	<p>Create comprehensive reporting and audit trails to simplify documentation requirements.</p>
<p>OPERATIONAL RESILIENCE</p> <p>Contracts must include provisions for business continuity and operational resilience.</p>	<p>Embed operational resilience clauses and workflows into all contracts.</p>

Conga Contract Lifecycle Management (CLM)

Uses AI to automate the entire contract process, ensuring efficient and compliant contract creation, management, and renewal.

Contact us for help with DORA compliance

conga.com