DORA 2025

The Definitive Guide to Compliance for the Financial Sector

Turn Regulatory Obligation into Competitive Advantage with Decentralized Cloud

A publication by Certiblok
January 2025 - Version 1.0

Table of Contents

Executive Summary

The Digital Operational Resilience Act (DORA), in force since January 17, 2025, represents the most significant regulatory revolution for the European financial sector in the last ten years. It is not merely a new rule to comply with, but a strategic opportunity to completely rethink your institution's ICT architecture.

Key Figures

- **22,000+ financial entities** involved in Europe
- **Fines up to 1%** of global turnover for non-compliance
- **85% of banks** still not fully prepared
- **€2.3 billion in planned investments for compliance**

The Challenge

While most institutions focus on traditional and costly solutions to achieve compliance, there is a revolutionary approach: decentralized cloud. This technology not only ensures DORA compliance but also turns compliance costs into long-term competitive advantages.

What is DORA and Why It's Crucial

Definition and Objectives
The Digital Operational Resilience Act is a regulation of the European Union establishing a comprehensive framework for ICT risk management in the financial sector. The objectives are twofold:

1. Harmonize existing regulations across member states
2. Strengthen the digital resilience of the entire European financial system

Scope of Application
DORA applies to:

- **Banks** and credit institutions
- **Insurance** and reinsurance companies
- **Investment firms** and asset managers
- **Payment service** providers
- **Crypto service** providers
- **Third-party ICT providers deemed critical**

Consequences of Non-Compliance
Non-compliance with DORA entails:

- **Administrative fines** up to 1% of global turnover
- **Suspension** of operational authorizations
- Irreversible **reputational damage**
- **Loss of competitiveness in the European market**

The 5 Pillars of DORA Compliance

1. ICT Risk Management

Requisiti chiave:

- Framework integrato di gestione del rischio Responsabilità chiare dell'organo di gestione Politiche e procedure documentate
- Monitoraggio continuo delle minacce Sfide pratiche:
- Integrazione di sistemi legacy eterogenei
- Formazione del personale su nuovi processi Costi di aggiornamento infrastrutturale

2. ICT Incident Management

Regulatory obligations:

- Classification of incidents by severity
- Mandatory reporting within strict timeframes
- Documented recovery procedures
- Systematic post-incident analyses

Operational complexities:
- Need for 24/7 monitoring systems
- Integration with alerting systems
- Coordination with supervisory authorities

3. Digital Operational Resilience Testing

Types of required tests:
- **Regular vulnerability testing**
- **Annual penetration tests**
- **TLPT** (Threat-Led Penetration Testing) **for significant institutions**

Required investments:
- Internal or external specialized resources
- Isolated test environments
- Advanced simulation tools

4. Third-Party ICT Risk Management

Supervision requirements:
- Thorough due diligence on providers
- Contracts with specific compliance clauses
- Continuous performance monitoring
- Documented exit strategy plans

Traditional cloud critical issues:
- Dependency on single providers (vendor lock-in)
- Risk concentration
- Limited control over data
- Rising and unpredictable costs

5. Information Sharing

Collaborative mechanisms:
- Participation in intelligence networks
- Sharing of indicators of compromise
- Collaboration with supervisory authorities

The Real-World Challenges of the Financial Sector

Current Scenario: A System in Crisis

The European financial sector is facing a perfect storm:

Heavy Technological Legacy
- 1980s mainframe systems still in use
- Non-integrated silo architectures
- Exponentially increasing maintenance costs

Evolving Cyber Threats

- +67% increase in attacks on the financial sector in 2024
- New AI-powered hacking techniques
- Increasingly sophisticated ransomware

Economic Pressures

- Shrinking profit margins
- Need for massive investments in cybersecurity
- Competition from agile fintech companies

Case Study: The Compliance Crisis

European Bank X (name anonymized)

- **Situation:** 850 branches, €45 billion in assets
- **Problem:** IT system fragmented across 12 different providers
- **Estimated DORA compliance cost:** €15 million
- **Implementation time:** 18 months
- **Operational risk:** High during the transition

This scenario is replicated in hundreds of European institutions, highlighting the need for innovative approaches.

Decentralized Cloud: The Future-Proof Solution

Why Traditional Cloud Is Not Enough

Centralized cloud services present structural limitations for DORA compliance:

Single Point of Failure

- Dependency on single data centers
- Risk of massive outages
- Vulnerability to targeted attacks

Limited Control

- Data managed by third parties
- Limited transparency over processes
- Difficulty in customization

Rising Costs

- Unpredictable pricing
- Costly vendor lock-in
- Limited scalability

The Decentralized Revolution

Decentralized cloud completely overturns the paradigm:

Distributed Architecture
- No single point of failure
- Automatic redundancy
- Built-in resilience

Full Control
- Data always under direct control
- Full transparency over processes
- Unlimited customization

Economies of Scale
- Predictable, fixed costs
- No vendor lock-in
- Infinite scalability

How It Works: The Certiblok Model

Smart Fragmentation
1. Each document is split into 80 fragments
2. Each fragment is encrypted with AES-256
3. Fragments are randomly distributed across 26,000 global nodes

Military-Grade Security
- Impossible to reconstruct the document without authorization
- Resistant to future quantum attacks
- End-to-end encryption on each fragment

Automatic Resilience
- If one node is compromised, the remaining 25,999 preserve the data
- Automatic network repair
- 99.99% guaranteed uptime

The Role of Certiblok in the DORA Strategy

More than Just a Platform

Certiblok is not just a technological solution, but a complete ecosystem for the digital transformation of the financial sector.

Advanced Technical Features

Decentralized Architecture
- 26,000 globally distributed nodes
- Smart data fragmentation
- AES-256 encryption on each fragment
- Zero single point of failure

Integrated DRM® System
- Complete document traceability
- Automatic versioning
- Granular access controls
- Immutable audit trail

Native Compliance
- GDPR compliance by design
- Integration with eIDAS 2.0
- Support for qualified digital signatures
- Legally compliant archiving

Unique Competitive Advantages

For Management
- 80% reduction in operational risks
- 340% average ROI in 18 months
- Elimination of vendor lock-in
- Full cost transparency

For the IT Department
- Deployment in days, not months
- Native APIs for integration
- Automatic scalability
- Specialized technical support

For End Customers
- Faster and more secure services
- Higher availability (99.99%)
- Guaranteed data protection
- Continuous innovation

Partnership Ecosystem

Native Integrations
- Leading core banking systems
- Document management systems
- Cybersecurity platforms
- Business intelligence tools

DORA Compliance Checklist

ICT Risk Management

Governance and Responsibilities
- Defined responsibility of the management body
- Chief Information Security Officer appointed
- ICT risk management policies approved
- Executive reporting system implemented

Risk Framework

- All critical ICT assets mapped
- Risk tolerance levels defined
- Proportional security controls implemented
- Escalation procedures established

Continuous Monitoring

- 24/7 monitoring systems active
- Real-time risk dashboards
- Automatic anomaly alerting
- Periodic review of controls

Incident Management

Classification and Taxonomy

- Incident classification criteria defined
- Ticketing system implemented
- Materiality thresholds established
- Centralized incident register created

Reporting and Notification

- Notification procedures to authorities
- Standardized templates for reporting
- Automatic alerting systems
- Secure communication channels

Response and Recovery

- Tested incident response plan
- Response team trained and operational
- Business continuity procedures
- Backup and recovery systems

Resilience Testing

Vulnerability Testing

- Scheduled automatic scans
- Annual penetration tests
- Web application assessments
- Security configuration verification

Advanced Testing (TLPT)

- Threat-led penetration tests planned
- Qualified providers selected
- Realistic attack scenarios defined
- Isolated test environments prepared

Performance Monitoring

- System availability metrics
- SLAs defined and monitored
- Capacity planning implemented
- Regular stress testing

Third-Party Vendor Management

Due Diligence and Selection

- Vendor assessment process
- Defined security criteria
- Financial and reputational checks
- Validated certifications and compliance

Contract Management

- DORA clauses included in agreements
- Specified security SLAs
- Audit rights included
- Defined exit procedures

Continuous Monitoring

- Monitored security KPIs
- Periodic supplier reviews
- Incident reporting from vendors
- Updated contingency plans

Information Sharing

Network Participation

- Membership in sector networks
- Sharing of threat intelligence
- Participation in technical working groups
- Collaboration with authorities

Sharing Systems

- Secure platforms implemented
- Anonymization protocols
- Data classification procedures
- Granular access controls

Next Steps

The Time to Act Is Now

DORA compliance is no longer an option, but a strategic imperative. Institutions that act first will not only avoid devastating penalties but also gain lasting competitive advantages.

To get started right away:
Email: commerciale@certiblok.com
Web: https://certiblok.com/en/dora-digital-operational-resilience-act-2/
Demo: https://calendly.com/e-bonetto/certiblok

Conclusion
The Digital Operational Resilience Act represents a historic turning point for the European financial sector. Institutions that embrace this challenge as an opportunity for technological innovation will emerge stronger, more secure, and more competitive. Decentralized cloud is not just the future of data management in the financial sector—it is the present for those who want to lead the transformation rather than endure it.

The question is not whether to adopt innovative solutions for DORA, but how quickly you can implement them before your competitors do.
The time for uncertainty is over. The time for action has arrived.

This white paper was developed by the DORA expert team at Certiblok, the first Italian platform for decentralized cloud specifically designed for compliance in the financial sector.

Certiblok S.r.l.
Piazza della Libertà, 14, 38121 Trento, Italia
P.IVA: IT02633560228