DORA 2025

La guida definitiva alla conformità per il settore finanziario

Trasforma l'obbligo normativo in vantaggio competitivo con il cloud decentralizzato

Una pubblicazione di Certiblok
Gennaio 2025 - Versione 1.0

Indice

Executive Summary

Il Digital Operational Resilience Act (DORA), entrato in vigore il 17 gennaio 2025, rappresenta la più significativa rivoluzione normativa per il settore finanziario europeo degli ultimi dieci anni. Non si tratta semplicemente di un nuovo regolamento da rispettare, ma di un'opportunità strategica per ripensare completamente l'architettura ICT del proprio istituto.

I Numeri Chiave

- **22.000+ entità finanziarie** coinvolte in Europa
- **Sanzioni fino all'1%** del fatturato mondiale per non conformità
- **85% delle banche** ancora non completamente preparate
- **€2.3 miliardi** di investimenti previsti nel settore per l'adeguamento

La Sfida

Mentre la maggior parte degli istituti si concentra su soluzioni tradizionali e costose per raggiungere la conformità, esiste un approccio rivoluzionario: **il cloud decentralizzato**. Questa tecnologia non solo garantisce la conformità DORA, ma trasforma i costi di compliance in vantaggi competitivi duraturi.

Cos'è DORA e perché è cruciale

Definizione e Obiettivi
Il Digital Operational Resilience Act è un regolamento dell'Unione Europea che stabilisce un framework completo per la gestione del rischio ICT nel settore finanziario. L'obiettivo è duplice:

1. Armonizzare le normative esistenti tra i diversi Stati membri
2. Rafforzare la resilienza digitale dell'intero sistema finanziario europeo

Ambito di Applicazione
DORA si applica a:

- **Banche e istituti** di credito
- **Compagnie assicurative** e riassicurative
- **Imprese di investimento** e gestori patrimoniali
- **Fornitori di servizi di pagamento**
- **Fornitori di servizi cripto**
- **Fornitori ICT terzi** considerati critici

Le Conseguenze della Non Conformità
La non conformità a DORA comporta:
- **Sanzioni amministrative** fino all'1% del fatturato mondiale
- **Sospensione delle autorizzazioni** operative
- **Danni reputazionali** irreversibili
- **Perdita di competitività** nel mercato europeo

I 5 pilastri della conformità DORA

1. Gestione del Rischio ICT

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. Gestione degli Incidenti ICT

Obblighi normativi:
- Classificazione degli incidenti per severità
- Segnalazione obbligatoria entro tempi rigorosi
- Procedimenti di ripristino documentati
- Analisi post-incidente sistematiche

Complessità operative:
- Necessità di sistemi di monitoraggio 24/7
- Integrazione con sistemi di alerting
- Coordinamento con autorità di vigilanza

3. Test di Resilienza Operativa Digitale

Tipologie di test richiesti:
- **Test di vulnerabilità** regolari
- **Test di penetrazione** annuali
- **TLPT** (Threat-Led Penetration Testing) per istituti significativi

Investimenti necessari:
- Risorse specializzate interne o esterne
- Ambienti di test isolati
- Strumenti di simulazione avanzati

4. Gestione del Rischio ICT di Terze Parti

Requisiti di supervisione:
- Due diligence approfondita sui fornitori
- Contratti con clausole di conformità specifiche
- Monitoraggio continuo delle performance
- Piani di exit strategy documentati

Criticità del cloud tradizionale:
- Dipendenza da singoli fornitori (vendor lock-in)
- Concentrazione dei rischi
- Limitato controllo sui dati
- Costi crescenti e imprevedibili

5. Condivisione di Informazioni

Meccanismi collaborativi:
- Partecipazione a reti di intelligence
- Condivisione di indicatori di compromissione
- Collaborazione con autorità di vigilanza

Le sfide concrete del settore finanziario
Scenario Attuale: Un Sistema in Crisi

Il settore finanziario europeo si trova ad affrontare una tempesta perfetta:

Eredità Tecnologica Pesante
- Sistemi mainframe degli anni ‘80 ancora in uso
- Architetture a silos non integrate
- Costi di manutenzione in crescita esponenziale

Minacce Cyber in Evoluzione
- +67% di attacchi al settore finanziario nel 2024
- Nuove tecniche di AI-powered hacking
- Ransomware sempre più sofisticati

Pressioni Economiche
- Margini in contrazione
- Necessità di investimenti massivi in cybersecurity
- Competizione da parte di fintech agili

Case Study: la crisi di conformità
Banca Europea X (nome anonimizzato)

- **Situazione**: 850 filiali, €45 miliardi di asset
- **Problema**: Sistema IT frammentato su 12 fornitori diversi Costo stimato conformità DORA: €15 milioni
- **Tempo implementazione**: 18 mesi
- **Rischio operativo**: Alto durante la transizione

Questo scenario si replica in centinaia di istituti europei, evidenziando la necessità di approcci innovativi.

Cloud decentralizzato: la soluzione del futuro
Perché il Cloud Tradizionale Non Basta

I servizi cloud centralizzati presentano limitazioni strutturali per la conformità DORA:

Single Point of Failure
- Dipendenza da datacenter singoli
- Rischio di interruzioni massive
- Vulnerabilità ad attacchi mirati

Controllo Limitato
- Dati gestiti da terze parti
- Trasparenza limitata sui processi
- Difficoltà nella personalizzazione

Costi Crescenti
- Pricing imprevedibile
- Vendor lock-in costoso
- Scalabilità limitata

La Rivoluzione Decentralizzata

Il cloud decentralizzato ribalta completamente il paradigma:

Architettura Distribuita

- Nessun single point of failure
- Ridondanza automatica
- Resilienza intrinseca

Controllo Totale

- Dati sempre sotto controllo diretto
- Trasparenza completa sui processi
- Personalizzazione illimitata

Economie di Scala

- Costi prevedibili e fissi
- Nessun vendor lock-in
- Scalabilità infinita

Come Funziona: Il Modello Certiblok

Frammentazione Intelligente

1. Ogni documento viene diviso in 80 frammenti
2. Ciascun frammento è criptato con AES-256
3. I frammenti sono distribuiti casualmente su 26.000 nodi globali

Sicurezza Militare

- Impossibile ricostruire il documento senza autorizzazione
- Resistenza ad attacchi quantistici futuri
- Crittografia end-to-end su ogni frammento

Resilienza Automatica

- Se un nodo si compromette, altri 25.999 mantengono i dati
- Riparazione automatica della rete
- Uptime garantito del 99.99%

Il ruolo di certiblok nella strategia DORA

Più di una Semplice Piattaforma

Certiblok non è solo una soluzione tecnologica, ma un **ecosistema completo** per la trasformazione digitale del settore finanziario.

Caratteristiche Tecniche Avanzate

Architettura Decentralizzata

- 26.000 nodi distribuiti globalmente
- Frammentazione intelligente dei dati
- Crittografia AES-256 su ogni frammento
- Zero single point of failure

Sistema DRM® Integrato
- Tracciabilità completa dei documenti
- Versioning automatico
- Controlli di accesso granulari
- Audit trail immutabile

Compliance Nativa
- Conformità GDPR by design
- Integrazione con eIDAS 2.0
- Supporto per firme digitali qualificate
- Archiviazione a norma di legge

Vantaggi Competitivi Unici

Per il Management
- Riduzione rischi operativi del 80%
- ROI medio del 340% in 18 mesi
- Eliminazione vendor lock-in
- Trasparenza totale sui costi

Per il Dipartimento IT
- Deployment in giorni, non mesi
- API native per integrazione
- Scalabilità automatica
- Supporto tecnico specializzato

Per i Clienti Finali
- Servizi più veloci e sicuri
- Maggiore disponibilità (99.99%)
- Protezione dati garantita
- Innovazione continua

Ecosistema di Partnership

Integrazioni Native
- Principali core banking systems
- Sistemi di gestione documentale
- Piattaforme di cybersecurity
- Tool di business intelligence

Checklist di conformità DORA

Gestione del Rischio ICT

Governance e Responsabilità
- Definita responsabilità dell'organo di gestione
- Nominato Chief Information Security Officer
- Approvate politiche di gestione rischio ICT
- Implementato sistema di reporting esecutivo

Framework di Rischio

- Mappati tutti gli asset ICT critici
- Definiti livelli di tolleranza al rischio
- Implementati controlli di sicurezza proporzionati
- Stabilite procedure di escalation

Monitoraggio Continuo

- Sistemi di monitoraggio 24/7 attivi
- Dashboard di rischio in tempo reale
- Alerting automatico per anomalie
- Review periodiche dei controlli

Gestione degli Incidenti

Classificazione e Tassonomia

- Definiti criteri di classificazione incidenti
- Implementato sistema di ticketing
- Stabilite soglie di materialità
- Creato registro incidenti centralizzato

Segnalazione e Reporting

- Procedure di notifica alle autorità
- Template standardizzati per segnalazioni
- Sistemi automatici di alert
- Canali di comunicazione sicuri

Response e Recovery

- Piano di incident response testato
- Team di risposta formato e operativo
- Procedure di business continuity
- Sistemi di backup e ripristino

Test di Resilienza

Test di Vulnerabilità

- Scansioni automatiche schedulati
- Penetration test annuali
- Assessment delle applicazioni web
- Verifica configurazioni sicurezza

Test Avanzati (TLPT)

- Pianificati test guidati da minacce
- Selezionati fornitori qualificati
- Definiti scenari di attacco realistici
- Preparati ambienti di test isolati

Monitoraggio Performance

- Metriche di disponibilità sistemi
- SLA definiti e monitorati

- Capacity planning implementato
- Test di stress regolari

Gestione Fornitori Terzi

Due Diligence e Selezione

- Processo di vendor assessment
- Criteri di sicurezza definiti
- Verifiche finanziarie e reputazionali
- Certificazioni e compliance validate

Gestione Contrattuale

- Clausole DORA negli accordi
- SLA di sicurezza specificati
- Diritti di audit inclusi
- Procedure di exit definite

Monitoraggio Continuo

- KPI di sicurezza monitorati
- Review periodiche dei fornitori
- Incident reporting dai vendor
- Piani di contingenza aggiornati

Information Sharing

Partecipazione Reti

- Adesione a reti settoriali
- Condivisione threat intelligence
- Partecipazione a tavoli tecnici
- Collaborazione con autorità

Sistemi di Condivisione

- Piattaforme sicure implementate
- Protocolli di anonimizzazione
- Procedure di classificazione dati
- Controlli di accesso granulari

Prossimi passi

Il Momento di Agire è Ora

La conformità DORA non è più un'opzione, ma un imperativo strategico. Le istituzioni che agiranno per prime non solo eviteranno sanzioni devastanti, ma otterranno vantaggi competitivi duraturi.

Per iniziare subito:
Email: commerciale@certiblok.com
Web: https://certiblok.com/dora-digital-operational-resilience-act/
Demo: https://calendly.com/e-bonetto/certiblok

Conclusioni
Il Digital Operational Resilience Act rappresenta un punto di svolta storico per il settore finanziario europeo. Le istituzioni che sabranno cogliere questa sfida come un'opportunità di innovazione tecnologica emergeranno più forti, sicure e competitive. Il cloud decentralizzato non è solo il futuro della gestione dati nel settore finanziario: è il presente per chi vuole guidare la trasformazione invece di subirla.

La domanda non è se adottare soluzioni innovative per DORA, ma quanto velocemente riuscirai a implementarle prima dei tuoi competitor.
Il tempo dell'incertezza è finito. Il momento dell'azione è arrivato.

Questo white paper è stato sviluppato dal team di esperti DORA di Certiblok, la prima piattaforma italiana di cloud decentralizzato specificamente progettata per la conformità del settore finanziario.

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