

FACT SHEET

Digital Operational Resilience Act (DORA) | *Regolamento (UE) 2022/2554 – Resilienza Operativa Digitale nel settore finanziario*

1. Cos'è DORA

Il **Digital Operational Resilience Act (DORA)** è il regolamento europeo che definisce un quadro unico, vincolante e direttamente applicabile per garantire la **resilienza operativa digitale** delle entità finanziarie. Stabilisce requisiti uniformi per:

- gestione del rischio ICT
- gestione e notifica degli incidenti
- testing della resilienza digitale
- continuità operativa
- gestione dei fornitori ICT
- governance del Board

È applicabile a banche, assicurazioni, intermediari finanziari, fornitori ICT critici e infrastrutture essenziali dal **17 gennaio 2025**.

2. Perché è importante

DORA impone un livello di coordinamento tra ICT, cybersecurity, Business Continuity e governance che prima non era richiesto in forma così strutturata.

È rilevante perché:

- introduce criteri uniformi per incident reporting, test e gestione dei fornitori
- integra resilienza digitale e continuità operativa
- richiede evidenze documentate di processi e capacità
- impone clausole contrattuali obbligatorie per i fornitori ICT critici
- stabilisce responsabilità precise per il Board
- collega la resilienza digitale alla stabilità finanziaria dell'UE

Per molti operatori, rappresenta il più grande cambiamento normativo degli ultimi anni nel settore.

3. Elementi chiave da conoscere

• Gestione del rischio ICT

Framework completo, governance, classificazione dei rischi, controlli minimi.

• Incident reporting

Categorie, soglie, classificazione, notifiche obbligatorie.

- **Testing della resilienza operativa digitale**

Test annuali, scenari avanzati, TLPT per entità designate.

- **Gestione dei fornitori ICT**

Due diligence, monitoraggio, contratti, audit, exit strategy.

- **Registro ICT**

Elenco strutturato dei fornitori e servizi, secondo template ITS.

- **FEI – Funzioni Essenziali o Importanti**

Perimetro critico per cui valgono requisiti rafforzati.

4. Errori comuni delle organizzazioni

- Separare BCM, ICT e cyber: processi non integrati
 - Mancare criteri coerenti per definire un “servizio ICT critico”
 - Testing formale, non basato su scenari reali
 - Contratti ICT senza clausole obbligatorie DORA
 - Incident reporting non allineato alle soglie e ai tempi normativi
 - Registro delle Informazioni incompleto o non aggiornato
 - Board coinvolto solo formalmente, non sostanzialmente
-

5. Come implementarlo correttamente (modello operativo in 6 passi)

1 Governance & Board

- responsabilità formali
- policy ICT
- KPI/KRI per resilienza

2 Framework di rischio ICT

- mappatura servizi e fornitori
- classificazione dei rischi
- controlli minimi e mitigazioni

3 Incident Management

- categorie e soglie
- flussi interni di escalation
- modelli di notifica formale

Continuità operativa & DR ICT

- allineamento RTO/RPO
- scenari FEI-based
- piani BC-DR aggiornati e testati

5 **Gestione fornitori ICT**

- due diligence
- contratti con clausole obbligatorie
- registro conforme a ITS
- monitoraggio continuo

6 **Testing della resilienza**

- test annuali
- test avanzati per FEI
- TLPT dove richiesto
- evidenze formali

6. Normativa tecnica e principali RTS/ITS di riferimento

Regolamento base

Regolamento (UE) 2022/2554 (DORA) – Digital Operational Resilience Act.

RTS – Regulatory Technical Standards

- **Reg. Delegato (UE) 2024/1772**
Criteri di classificazione degli incidenti ICT e minacce cibernetiche; soglie e contenuti delle notifiche.
- **Reg. Delegato (UE) 2024/1773**
Contenuto della policy per contratti ICT relativi a funzioni critiche o importanti.
- **Reg. Delegato (UE) 2024/1774**
Strumenti, metodi e processi per l'ICT Risk Management; framework semplificato.
- **Reg. Delegato (UE) 2025/301**
Contenuti e scadenze per la notifica di incidenti gravi; notifica volontaria minacce cyber.
- **Reg. Delegato (UE) 2025/1190**
Criteri per individuare le entità soggette a TLPT e requisiti dei tester.

ITS – Implementing Technical Standards

- **Reg. di Esecuzione (UE) 2024/2956**
Template standard per il registro delle informazioni sui fornitori ICT.
- **Reg. di Esecuzione (UE) 2025/302**
Moduli e modelli per la notifica di incidenti ICT.

7. Checklist di autovalutazione (12 punti)

La tua organizzazione è pronta per DORA?

- Governance ICT e ruoli formalizzati
- Framework del rischio ICT documentato
- Classificazione rischi coerente e ripetibile
- Incident reporting conforme RTS
- Fornitori ICT critici identificati
- Registro ICT aggiornato e conforme ITS
- Contratti Fornitori ICT DORA-compliant
- Testing annuale in essere
- FEI formalizzate e mappate
- Piani DR/BCM aggiornati e allineati a FEI
- KPI/KRI per resilienza digitale
- Evidenze pronte per audit e supervisor

8. Come Continuity supporta le organizzazioni

■ Formazione specialistica

Corsi dedicati a resilienza operativa, BCM, cyber resilience, DORA, FEI, vendor risk e testing.

■ Certificazioni professionali DRI International

Continuity eroga i corsi ufficiali DRI utili ad ottenere:

- **ABCP – Associate Business Continuity Professional**
- **CBCP – Certified Business Continuity Professional**
- **ACRP – Associate Cyber Resilience Professional**
- **CCRP – Certified Cyber Resilience Professional**

■ Supporto consulenziale

- Mappatura FEI vs servizi critici da BIA
- Analisi rischio ICT e vendor risk
- Creazione registro ICT conforme ITS
- Revisione contratti ICT secondo DORA
- KPI/KRI e framework di testing