

UniCredit Factoring S.p.A.

DORA

Business Services & Process Excellence

Milano, 27 marzo 2025

Agenda

1

DORA

Che cosa è DORA?

2

Ambito di applicazione

3

I quattro pilastri obbligatori di DORA

4

Attività principali



Che cosa è DORA? Fa parte del percorso evolutivo della regolamentazione sulla resilienza

1 2 3 4



Qual è lo scopo di DORA?

- DORA è volta a migliorare la **resilienza operativa digitale complessiva del settore finanziario dell'UE**. Pubblicata nella Gazzetta Ufficiale il 27 dicembre 2022, e **applicabile dal 17 gennaio 2025**
- DORA **armonizza** le regole relative alla resilienza operativa per il settore finanziario, applicandosi a **21 diverse tipologie di entità**, compresi i fornitori terzi di servizi IT
- Si concentra su 3 aree principali: **sicurezza informatica**, **resilienza operativa complessiva dell'IT** e **supervisione dei fornitori ICT**



Perché conformarsi?

- Per adattarsi allo **scenario di mercato e al panorama dei rischi in continua evoluzione**
 - Per garantire **sicurezza, agilità e competitività dei servizi offerti** supportando il processo di trasformazione digitale
 - Per rafforzare il livello di resilienza ai **rischi digitali delle funzioni e dei servizi critici**
 - Per **ridurre gli impatti e i costi** della risposta ai principali incidenti di sicurezza
- ...in ultima analisi per evitare **sanzioni amministrative** (considerando anche il previsto crescente livello di attenzione da parte delle ESA - Autorità di vigilanza europee*)

Roadmap normativa DORA



* EBA : Autorità bancaria europea; ESMA : Autorità europea degli strumenti finanziari e dei mercati; EIOPA : Autorità europea delle assicurazioni e delle pensioni aziendali e professionali



Il **perimetro di applicazione** del regolamento è chiaramente indicato all'articolo 2, che indica:

«...Fatti salvi i paragrafi 3 e 4, il presente Regolamento si applica alle entità seguenti:

- a) enti creditizi;*
- b) istituti di pagamento, compresi gli istituti di pagamento esentati a norma della direttiva (UE) 2015/2366;*
- c) prestatori di servizi di informazione sui conti;*
- d) istituti di moneta elettronica, compresi gli istituti di moneta elettronica esentati a norma della direttiva 2009/110/CE;*
- e) imprese di investimento;*
- f) fornitori di servizi per le cripto-attività autorizzati a norma del Regolamento del Parlamento europeo e del Consiglio concernente i mercati delle cripto-attività e recante modifica dei regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e delle direttive 2013/36/UE e (UE) 2019/1937 (Regolamento sui mercati delle cripto-attività) ed emittenti di token collegati ad attività;*

.....»

UniCredit Factoring S.p.A.



Atto del Governo n.242 del 13 gennaio 2025

L'**articolo 17** dispone **un'applicazione differita al 1° gennaio 2027** per quanto riguarda la disciplina relativa alla resilienza operativa Digitale applicabile agli intermediari finanziari (contenuta nell'art 6, commi 1 e 2, del decreto), per accordare ad essi un congruo periodo per adattarsi alle nuove disposizioni.

Il Gruppo UniCredit ha deciso di includere nel perimetro di applicazione UniCredit Factoring per un adeguamento al 17 gennaio 2025:

- armonizzare l'approccio della Holding;
- evitare possibili rischi reputazionali.



I quattro pilastri obbligatori di DORA

1 2 3 4



Obiettivi

Argomenti principali

1. Governance ICT e gestione dei rischi



Creazione di un **framework comune per una gestione armonizzata dei rischi ICT** applicabile a tutti gli istituti finanziari interessati

- Governance ICT
- Strategia per la resilienza operativa digitale
- Gestione del rischio basata su scenari ICT
- Continuità aziendale ICT

2. Gestione e segnalazione degli incidenti



Armonizzazione della classificazione degli incidenti ICT e della logica di segnalazione. Tempi di segnalazione rapidi (entro lo stesso giorno dell'evento)

- Gestione degli incidenti di sicurezza
- Gestione degli incidenti IT
- Comunicazione degli incidenti

3. Operatività digitale Test di resilienza



Norme armonizzate dell'UE per i test di resilienza operativa digitale in modo proporzionale (test di base vs. avanzati)

- Test basati su scenari (ripristino di emergenza, attacco informatico, ecc.)
- Test di penetrazione delle minacce (TLPT)

4. Gestione dei rischi dei fornitori ICT



Affrontare gli **elementi contrattuali minimi per consentire un monitoraggio completo delle terze parti ICT**

- Gestione di terze parti ICT
- Registro delle informazioni
- Negoziazione degli accordi contrattuali



Attività principali (1/2)

1 2 3 4

Pilastri DORA

Governance ICT e gestione dei rischi.

Creazione di un framework comune per una gestione armonizzata dei rischi ICT applicabile a tutti gli istituti finanziari interessati

Strategia di resilienza operativa digitale (DORS)

Impostazione della governance (ruoli e responsabilità) e **definizione l'approccio interno**, approvato dal Consiglio di Amministrazione, in linea con la Strategia Digitale, di Sicurezza e di Business.

La Strategia di UCF recepisce quanto declinato nella strategia di Gruppo a sua volta è strettamente collegata alla Digital e Security Strategies.

Funzioni critiche o importanti (CoIFs)

Definizione di una metodologia per identificare i processi E2E rilevanti nel perimetro DORA
In linea con la metodologia di Gruppo l'identificazione è basata su un subset di processi BIA.

Quadro di gestione dei rischi ICT (1° e 2° livello)

Aggiornamento delle policy IT e evoluzione del RAF *, compresi i livelli di tolleranza al rischio ICT, in linea con la strategia aziendale e ICT

Continuità aziendale ICT

Evoluzione del framework, inclusi policy, metodologia, piano, test, anche per Disaster Recovery e Backup

Misure di sicurezza

Adeguamento delle misure di sicurezza secondo RTS* sulla gestione del rischio (ad esempio, crittografia e miglioramento della sicurezza di rete, ecc.).

Gestione e segnalazione degli incidenti

Armonizzazione della classificazione degli incidenti ICT e della logica di segnalazione. Tempi di segnalazione rapidi

Criteri per gli incidenti ICT

Definizione di diversi criteri primari e secondari per determinare la gravità dell'incidente e la rilevanza ai fini della segnalazione

Tassonomia degli incidenti ICT

Classificazione degli incidenti, comprese le soglie di materialità dei principali incidenti correlati alle ICT, soggetti a segnalazione

Costi e perdite derivanti da incidenti gravi

Definizione di una metodologia per stimare i costi aggregati e le perdite derivanti da incidenti gravi

* RAF : Risk Appetite Framework; RTS : Norme tecniche di regolamentazione; ICT TPP : Fornitori terzi di ICT



Attività principali (2/2)

1 2 3 4

Pilastri DORA

Operativo digitale
Test di resilienza
Norme armonizzate
dell'UE per i test di
resilienza operativa
digitale in modo
proporzionale

Test annuale

Definizione ed esecuzione di una **metodologia e di un programma di test** per condurre **test, almeno annualmente**, su tutti i sistemi e le applicazioni ICT a supporto di funzioni critiche o importanti

Test di penetrazione guidato dalle minacce (TLPT)

Definizione ed esecuzione di una **metodologia di test, programma ed esercizio TLPT** obbligatorio **ogni tre anni**, seguendo un approccio basato sul rischio

Gestione dei rischi
di terze parti ICT
Affrontare gli
elementi contrattuali
minimi per
consentire un
monitoraggio
completo delle terze
parti ICT

Quadro di gestione dei rischi di terze parti ICT

Evoluzione del quadro attuale che estende tutte le attività di gestione dell'outsourcing (ad esempio, valutazione del rischio, monitoraggio, strategia di uscita) anche **all'ICT TPP ***

Accordi contrattuali

Adattamento e negoziazione dei contratti con i TPP ICT * con clausole aggiuntive rispetto alle Linee guida EBA*

Registro delle informazioni

Estensione del registro sulle esternalizzazioni anche ai TPP ICT *, con informazioni e tabelle aggiuntive richieste nell'ITS* dedicato (in bozza)

Miglioramento della supervisione

La supervisione sui TPP* ICT deve essere rafforzata (ad esempio, due diligence, subappalti, ecc.)

* ICT TPP : fornitori terzi di ICT; EBA : Autorità bancaria europea; ITS : standard tecnico di attuazione; RTS : standard tecnici di regolamentazione

