



ASSIFACT

Associazione Italiana per il Factoring

Regolamento DORA (Digital Operational Resilience Act)

Gdl Dora

25 settembre 2024

- Documento riservato -

Presupposti della norma

- Il Regolamento DORA è stato introdotto per rispondere all'aumento delle minacce cibernetiche nel settore finanziario e per garantire una maggiore sicurezza operativa.
- Obiettivo principale: aumentare la resilienza operativa digitale di tutte le entità finanziarie dell'UE.
- Il regolamento fa parte di una più ampia strategia dell'UE per la sicurezza digitale, che include anche la Direttiva NIS 2 e altre normative simili.
- La norma punta a armonizzare la gestione dei rischi ICT e migliorare la risposta agli attacchi informatici

«resilienza operativa digitale»: la capacità dell'entità finanziaria di costruire, assicurare e riesaminare la propria integrità e affidabilità operativa, garantendo, direttamente o indirettamente tramite il ricorso ai servizi offerti da fornitori terzi di servizi TIC, l'intera gamma delle capacità connesse alle TIC necessarie per garantire la sicurezza dei sistemi informatici e di rete utilizzati dall'entità finanziaria, su cui si fondano la costante offerta dei servizi finanziari e la loro qualità, anche in occasione di perturbazioni;

Destinatari

- Il Regolamento **DORA** si applica a tutte le entità finanziarie, tra cui:
 - Banche
 - Istituti di pagamento e di moneta elettronica
 - Società di investimento
 - Imprese di assicurazione e riassicurazione
 - Fondi di investimento
 - Fornitori di servizi ICT legati al settore finanziario
 - Società di gestione di cripto-attività
- Non è direttamente applicabile agli intermediari finanziari ex. art. 106 TUB (serve intervento di Banca d'Italia)

Principali contenuti e novità (1)

- **Governance e gestione del rischio ICT:** Le entità finanziarie devono adottare un quadro strutturato per la gestione dei rischi ICT, che includa strategie, politiche e procedure volte a proteggere le infrastrutture ICT e i dati sensibili. Questo quadro deve essere periodicamente riesaminato e migliorato in base alle lezioni apprese e ai nuovi rischi emergenti. Gli obblighi includono l'implementazione di strumenti aggiornati per ridurre al minimo gli impatti dei rischi informatici.
- **Separazione delle funzioni:** È richiesto un alto livello di indipendenza nelle funzioni di gestione e controllo dei rischi ICT. Il regolamento impone che le entità finanziarie stabiliscano una chiara separazione tra gestione dei rischi, controllo e audit interni, per garantire che nessun conflitto di interessi interferisca con il monitoraggio e la gestione dei rischi informatici.
- **Strategia di resilienza operativa digitale:** Le entità finanziarie devono adottare una strategia di resilienza operativa digitale che copra la gestione dei rischi ICT. La strategia deve includere metodi per affrontare le minacce informatiche e fissare obiettivi chiari in termini di sicurezza informatica. Il quadro deve comprendere anche misure per monitorare e prevenire incidenti informatici.



Principali contenuti e novità (2)

- **Gestione dei rischi da fornitori terzi:** Un elemento critico è la gestione dei fornitori terzi di servizi ICT. Il regolamento richiede alle entità finanziarie di monitorare attentamente i fornitori critici, con accordi che assicurino diritti di audit e garanzie contrattuali per mantenere il controllo sui rischi. Questo si applica in particolare ai servizi essenziali o importanti per l'operatività finanziaria.
- **Obblighi di formazione e sensibilizzazione:** Le entità finanziarie devono predisporre programmi di sensibilizzazione e formazione periodica sulla sicurezza informatica e la resilienza digitale per tutto il personale. È fondamentale che dirigenti e dipendenti siano formati per comprendere i rischi informatici e le migliori pratiche per mitigarli.
- **Condivisione delle informazioni sulle minacce:** Il DORA incentiva la collaborazione tra le entità finanziarie per condividere informazioni riguardanti minacce e attacchi cyber (cyber threat intelligence).

Criticità per gli operatori

- **Adeguamento delle infrastrutture IT:** Le banche dovranno modernizzare e rafforzare i loro sistemi per garantire la sicurezza e la continuità operativa in caso di attacchi.
- **Formazione del personale:** Il personale dovrà essere formato su nuove pratiche e protocolli di sicurezza, attraverso programmi di cybersecurity awareness.
- **Gestione dei fornitori terzi:** Le banche dovranno gestire attentamente i rischi derivanti dai servizi IT esternalizzati, con un controllo rigido e continuo delle performance e della sicurezza.
- **Compliance e costi:** Implementare tutte le misure necessarie potrebbe comportare significativi costi e richiederà tempo per conformarsi alle scadenze del 2025.
- **Reporting complesso degli incidenti:** Dovranno essere sviluppati strumenti e procedure per il reporting, il monitoraggio e la gestione degli incidenti ICT in linea con i criteri DORA.

Open discussion

- Quali sono le principali problematiche che state affrontando in tema DORA?
- Ci sono tematiche specifiche per il factoring?
- Quale ruolo per l'Associazione e il Gdl?