Deloitte.

# Regulatory News Alert

## Digital Operational Resilience Act (DORA): quali implicazioni strategiche per il Board dei player finanziari?

**21 Dicembre 2022**

**Digital Operational Resilience Act (DORA): quali implicazioni strategiche per il Board dei player finanziari?**

**In sintesi:**

- Il Digital Operational Resilience Act (DORA) è stato approvato dai legislatori europei e sarà applicabile a partire da 24 mesi dalla sua entrata in vigore prevista per gennaio 2023.
- Le imprese del settore finanziario sono chiamate ad affrontare le sfide legate all'adeguamento ai requisiti previsti dal DORA, ma dovranno altresì attivarsi per rispondere alle più ampie implicazioni strategiche derivanti dai nuovi standard regolamentari.
- I nuovi standard regolamentari richiederanno un cambiamento di mindset a partire dal top management (Board e CxO), che sono chiamati a rafforzare il livello di resilienza delle proprie organizzazioni ai rischi connessi all'evoluzione digitale, per poter rispondere tempestivamente e dinamicamente all'evoluzione delle minacce e delle vulnerabilità derivanti dal nuovo contesto di mercato.
- Gli impegni - immediati e continuativi - stabiliti dal DORA implicano che i Consigli di Amministrazione e i CxO delle imprese del settore finanziario guidino il processo di cambiamento svolgendo un ruolo attivo nel definire gli interventi di risposta e gli investimenti necessari per rafforzare il livello di resilienza.

**Audience:** Membri CdA, CEO, CFO, CRO, COO, CISO, Compliance Officer.

**Contesto**

Il DORA, la più importante iniziativa UE in ambito resilienza operativa digitale e cyber per il settore finanziario, è stato ratificato dai legislatori europei. Il regolamento europeo introduce un quadro normativo e di vigilanza armonizzato spingendo le imprese operanti nel settore finanziario ad effettuare investimenti significativi per rafforzare il proprio livello di resilienza ai rischi cyber e digitali che impattano sulla continuità operativa delle funzioni e servizi critici.

Deloitte.

Le disposizioni del DORA devono essere attuate entro 24 mesi dalla sua entrata in vigore, che avverrà dopo la pubblicazione del testo nella Gazzetta Ufficiale dell'UE, prevista per la fine del 2022. Le aziende dovranno dunque attivare un programma di adeguamento da completare entro l'inizio del 2025.

**DORA: quali implicazioni strategiche per le imprese del settore finanziario?**

1. **Il concetto di "resilienza operativa" comporterà un cambio di mindset per le imprese:** Il DORA introduce per la prima volta il concetto di resilienza operativa all'interno del framework normativo UE che regola i servizi finanziari, andando oltre le precedenti linee guida incentrate sul rischio cyber e IT con un nuovo approccio olistico atto a rafforzare la resilienza alle digital disruptions. Il DORA rappresenta qualcosa di più di un semplice cambio di terminologia: la resilienza operativa va oltre gli approcci tradizionali di gestione del rischio utilizzati dalle funzioni Cyber, IT risk e Business Continuity; induce le imprese a supporre che gravi interruzioni siano inevitabili (indipendentemente da quanto solidi siano le difese aziendali) e le spinge a costruire un livello più elevato di resilienza a tali interruzioni nell'ambito del modello operativo delle funzioni e servizi più importanti. Questo assunto implicherà un dialogo continuativo tra imprese e autorità le cui modalità devono essere ancora elaborate dalle autorità di vigilanza finanziaria dell'UE.

   Lo sviluppo di tale approccio nel Regno Unito (che ha implementato il suo quadro di resilienza operativa nel marzo 2022) ha fatto sì che le imprese abbiano dovuto fissare elevati standard futuri di resilienza che richiederanno investimenti ingenti per essere raggiunti. L'esperienza del Regno Unito ha anche dimostrato la necessità di una maggiore collaborazione intersettoriale in merito ai rischi e alle vulnerabilità comuni che non possono essere affrontate adeguatamente a livello di singolo operatore ma che richiedono una risposta sistemica. In tal senso, il settore dovrà dare prova di proattività nello sviluppo di modelli e metodologie per affrontare i rischi di concentrazione e le pratiche di test relativi alle terze parti, e la condivisione in tempo reale di informazioni di threat intelligence.

2. **Viene rafforzata la responsabilità del management sulla resilienza operativa:** Il DORA prevede chiare responsabilità sulla resilienza operativa per il Board e i CxO che dovranno assumere un ruolo di primo piano nell'implementazione di soluzioni per il raggiungimento degli standard previsti dal nuovo framework regolamentare. In termini pratici, il Board e il top management dovranno approvare una serie di programmi chiave, come la strategia di resilienza operativa digitale aziendale, la politica di gestione delle terze parti ICT (TPPs) che richiederà un rafforzamento mirato dei presidi rispetto allo status quo. Inoltre, il senior management sarà anche responsabile di prendere le decisioni a valere sul modello operativo al fine di incorporare i requisiti del DORA nell'ambito delle operazioni quotidiane, come ad esempio la definizione dei livelli di tolleranza al rischio e la prioritizzazione delle azioni di rimedio per rispondere alle vulnerabilità operative identificate.

   Anche se le aspettative di vigilanza sui Board emergeranno appieno solo in un secondo momento, le componenti del DORA che necessitano di un ruolo attivo in termini di indirizzo, approvazione e supervisione richiederanno competenze e risorse aggiuntive per la maggior parte dei Consigli di Amministrazione. L'implementazione degli standard DORA richiederà ai Boards e CxO di dimostrare alle autorità di vigilanza la resilienza aziendale alle minacce specifiche e alle più ampie minacce settoriali. Dovranno inoltre

rafforzare la comprensione e il livello di consapevolezza circa la capacità dell'azienda di far fronte a potenziali interruzioni ICT mantenendo la continuità dei servizi. Dovranno dimostrare di aver preso le giuste decisioni gestionali, di aver rivisto e messo in discussione i piani di resilienza e di aver conseguentemente rafforzato la resilienza complessiva della propria azienda. Le informazioni gestionali sulle minacce e le vulnerabilità provenienti dal contesto esterno dovranno essere considerate in modo dinamico nell'ambito del complessivo framework di resilienza operativa dell'azienda.

3. **Gli adempimenti continuativi previsti guideranno le azioni delle imprese oltre il periodo di implementazione:** Il periodo di implementazione di 24 mesi metterà alla prova la maggior parte delle aziende del settore finanziario, comprese le più grandi e strutturate in aree quali *digital operational resilience testing*, *incident reporting* e *business impact analysis*. Il DORA introduce inoltre un approccio continuativo di gestione della resilienza nelle aziende del settore finanziario, sulla base di un processo di revisione ed evoluzione costante che avrà implicazioni nel lungo termine. A titolo esemplificativo, le imprese dovranno effettuare test di resilienza ricorrenti e valutare periodicamente i rischi e l'adeguatezza dei loro piani di resilienza. Saranno tenute a raccogliere nel continuo informazioni sulle minacce e gli incidenti al fine di conformarsi ai nuovi obblighi di segnalazione, nonché ad elaborare i propri scenari di rischio. Il DORA richiede alle aziende una puntuale identificazione delle funzioni critiche o importanti (CIFs) come punto focale di indirizzo dei presidi per rafforzare la loro resilienza, in particolare per quanto riguarda l'identificazione delle minacce e i test di scenario.

   La ratio del nuovo framework regolamentare è che il raggiungimento di un "buon" livello di resilienza operativa costituirà un obbligo normativo continuativo che evolverà costantemente all'evolvere delle minacce e delle vulnerabilità derivanti dal contesto di riferimento. Investendo in capacità strategiche, come la threat intelligence e i test di resilienza, i Boards e i CxO avranno a disposizione ulteriori strumenti per comprendere non solo come gli scenari di rischio possano influenzare le funzioni critiche aziendali, ma anche quali investimenti saranno necessari per raggiungere un livello sufficiente di preparazione. Inoltre, capacità strategiche di questo tipo saranno fondamentali anche per garantire maggiori capacità di risposta alle interruzioni impreviste.

4. **Le strategie di esternalizzazione delle imprese verranno messe alla prova:** Indirizzare le vulnerabilità delle terze parti rappresenta una delle sfide principali del percorso di rafforzamento della resilienza operativa. Il DORA introduce a livello mondiale il primo framework di supervisione dei fornitori terzi di servizi critici (CTPs) attribuendo alle Autorità Europee di Vigilanza europee (ESAs) nuovi poteri di supervisione sui fornitori terzi e di gestione dei rischi che questi operatori potrebbero rappresentare per il settore dei servizi finanziari. A riguardo, le autorità di regolamentazione dell'UE hanno anche ribadito che il nuovo regime di supervisione non implica una revisione delle responsabilità individuali delle imprese del settore finanziario in materia di esternalizzazione. Di fatto, il DORA impone alle aziende del settore finanziario diversi nuovi requisiti per la gestione del rischio delle terze parti, il cui livello di severità cresce nel caso in cui i fornitori terzi svolgano un ruolo di supporto alle funzioni critiche o importanti (CIFs) dell'azienda. Ciò può diventare particolarmente impattante per le FinTech e le imprese digital-native, la cui dipendenza da determinate piattaforme digitali potrebbe potenzialmente renderle più esposte al rischio ICT e richiedere un maggiore controllo da parte dell'autorità di vigilanza su tale rischio.

Deloitte.

Le imprese dovranno inoltre prestare particolare attenzione a valutare il rischio di concentrazione delle terze parti. Le potenziali vulnerabilità – come l'eccessiva dipendenza da un singolo fornitore o la criticità delle funzioni servite – possono esporre gli operatori finanziari ad una più incisiva azione di controllo da parte delle autorità di vigilanza. Ciò potrebbe inoltre mettere pressione sui Boards affinché rivedano le loro strategie di sourcing (puntando ad esempio ad una strategia multi-vendor), la loro propensione al rischio per l'avvio di relazioni con terze parti e il ruolo delle funzioni di gestione del rischio e di procurement.

5. **Il percorso di rafforzamento della resilienza operativa richiederà decisioni di investimento da parte del Top Management:** Per costruire la resilienza operativa in un'azienda è necessario che la stessa diventi un fattore chiave nelle decisioni di business e nella progettazione dei modelli operativi *(resilience by design)*. Più specificamente, le aziende del settore finanziario avranno il compito di identificare il livello di resilienza atteso nell'ambito della strategia di resilienza operativa digitale che DORA richiedere di definire, vincolando nella sostanza il top management ad assumere un ruolo decisionale proattivo in materia di gestione del rischio ICT e resilienza. Ciò implica che i Boards e i CxO dovranno valutare il complessivo business case che deve prevedere l'investimento per rafforzare le capacità di resilienza, ed essere altresì in grado di dimostrare come i costi iniziali siano compensati da un modello operativo più resiliente e sostenibile in relazione alla costante evoluzione regolamentare e all'intensificarsi dell'azione di vigilanza. A livello pratico, dovrebbe essere data priorità alle aree che potrebbero potenzialmente essere centrali nell'agenda delle autorità di vigilanza nel coso dell'implementazione del DORA, come ad esempio i requisiti che richiedono output ricorrenti che possano essere messi in discussione dalle autorità di vigilanza (ad esempio, l'identificazione delle CIFs, le business impact analysis, i test di resilienza operativa, i processi di segnalazione degli incidenti).

   Nell'assunzione delle decisioni chiave il management dovrà inoltre tenere conto di come le autorità di vigilanza applicheranno concretamente il principio di proporzionalità del DORA. Gli operatori di maggiori dimensioni e complessità operativa avranno verosimilmente a disposizione capacità più avanzate in determinate aree (ad esempio i test di resilienza), ma saranno anche soggetti ad un controllo molto più forte, in considerazione della potenziale importanza sistemica dei loro servizi chiave. Gli operatori di minori dimensioni, al contrario, potranno beneficiare di requisiti meno stringenti (ad esempio, non sono tenuti a svolgere test TLPT avanzati e sono soggetti al quadro semplificato di gestione del rischio ICT del DORA), ma si troveranno comunque ad affrontare di investimenti ingenti per dotarsi delle capacità necessarie per allinearsi ai requisiti del regolamento che si applicano a livello generale, come l'obbligo di segnalazione degli incidenti ICT e le disposizioni sulla gestione del rischio di terze parti.

**<u>Considerazioni finali</u>**

Il DORA non sarà un esercizio di conformità "*one-off*", ma spingerà le aziende a mantenere un adeguato livello di resilienza in un panorama di minacce in continua evoluzione e in un ambiente tecnologico sempre più complesso.

Sebbene nei prossimi 24 mesi le autorità di vigilanza europee saranno occupate nella declinazione di una parte significativa della regolamentazione secondaria del DORA e nel calibrare le loro reali aspettative in materia di resilienza operativa, è già chiaro che i Boards e i CxO saranno chiamati a svolgere un ruolo centrale in materia di resilienza assumendo direttamente decisioni nel corso del periodo di implementazione del DORA. Sarà pertanto importante stabilire un forte "*tone from the top*" per quanto riguarda l'impegno delle imprese nella costruzione

Deloitte.

della propria resilienza operativa - un elemento che le autorità di regolamentazione e vigilanza, gli investitori e gli altri stakeholders prenderanno sempre più in considerazione con l'aumentare delle minacce operative nel settore finanziario.

# Contatti

**Andrea Rigoni**
EU Digital Policy Center Director – Deloitte Risk Advisory
Tel: + 39 3355772342
arigoni@deloitte.it

**Gianfranco Tessitore**
Partner | Regulatory Strategy & Controls Transformation Leader – Deloitte Risk Advisory
Tel: + 39 3488862150
gtessitore@deloitte.it

Deloitte Risk Advisory S.r.l. S.B.
Via Tortona 25, Milano, 20144, Italia