Deloitte.

Regulatory News Alert

Approvato il Digital Operation Resilience Act dell'UE: implicazioni per il settore finanziario

15 Novembre 2022

In sintesi:

- **Nella sessione plenaria del Parlamento Europeo del 10 novembre** è stato raggiunto l'**accordo finale sul Digital Operational Resilience Act (DORA)** che rappresenta la più importante iniziativa regolamentare a livello UE in materia di resilienza operativa e sicurezza informatica nel settore dei servizi finanziari (FS) e costituisce un notevole passo avanti verso il consolidamento e l'evoluzione dei requisiti normativi per gli operatori di mercato in ambito ICT.
- Il DORA richiede agli operatori di adottare una **visione aziendale più ampia della resilienza**, con chiare e rafforzate responsabilità per gli Organi aziendali e il top management; si applica alla maggioranza degli operatori del settore finanziario che operano nell'UE e stabilisce regole vincolanti per la **gestione del rischio ICT, il reporting degli incidenti, i test di resilienza e la gestione del rischio di terze parti (TPRM)**.
- Il DORA costituisce inoltre il **primo framework normativo** al mondo che consente alle **autorità di vigilanza FS di supervisionare i fornitori di servizi ICT critici (CTPPs)**, compresi i fornitori di servizi cloud (CSPs).
- Il Regolamento fornisce agli operatori una base su cui iniziare da subito a lavorare per indirizzare la fase attuativa. Gli operatori sono pertanto chiamati a condurre un'analisi di impatto finalizzata all'identificazione dei gap e delle aree evolutive sui quali sviluppare una **roadmap per l'implementazione di un robusto framework di operational resilience** entro il quarto trimestre 2024, in linea con i nuovi requisiti.
- Il DORA non rappresenta solo un vincolo regolamentare ma un vero e proprio acceleratore nel processo evolutivo dei sistemi di **gestione dei rischi digitali**, oltre ad essere un'opportunità per gli operatori di rafforzare il livello di comprensione e valutazione dell'impatto degli incidenti/interruzioni operative sul proprio business e sui clienti.
  La presente analisi, realizzata dal Deloitte Centre for Regulatory Strategy con il contributo degli esperti di Deloitte di tutta Europa, approfondisce i significativi cambiamenti e le potenziali sfide che gli operatori dovranno affrontare per l'attuazione dei cinque pilastri del DORA.

Deloitte.

Overview

A seguito di approfondite negoziazioni a livello UE è stato raggiunto un **accordo tecnico completo sul regolamento DORA**. Mancano solo pochi passi per la chiusura dell'iter amministrativo con la pubblicazione sulla Gazzetta Ufficiale dell'UE. Il **testo completo del regolamento** è già stato pubblicato dal Parlamento europeo e gli operatori del settore finanziario devono quindi iniziare a valutarne gli impatti sul proprio modello di business, organizzativo e operativo. Siamo convinti che DORA sarà un **"game changer"** che spingerà gli **operatori di servizi finanziari** a **comprendere** appieno come le loro attuali prassi di gestione in ambito ICT Risk, Cyber e Gestione del Rischio Terze Parti impattano sul livello di resilienza delle loro funzioni più critiche, spingendo verso lo **sviluppo di capacità di resilienza operativa completamente nuove**, come metodologie avanzate di testing degli scenari di rischio.

Gli operatori del settore avranno a disposizione un **periodo** relativamente contenuto di **24 mesi** per adeguarsi ai nuovi standard regolamentari. Il periodo di implementazione inizierà dopo 20 giorni dalla pubblicazione sulla Gazzetta Ufficiale dell'UE (prevista per novembre 2022). Ciò significa che, **entro il quarto trimestre del 2024**, le autorità di vigilanza competenti si aspetteranno che le **entità di settore** siano **pienamente conformi** ai nuovi requisiti del DORA, incluse le previsioni che saranno contenute nella regolamentazione di livello 2 che sarà definita dalle autorità di regolamentazione europee (cfr. Parte II di seguito).

Quali sono le implicazioni del nuovo regolamento DORA per gli operatori di settore?

La versione del regolamento approvata conferma i cinque pilastri fondamentali della proposta originale della Commissione Europea. Dalle nostre analisi sul testo dell'accordo tecnico finale, emergono le seguenti principali implicazioni:

1. Gestione del rischio ICT – focus sulle funzioni aziendali critiche

DORA attribuisce un ruolo pivotale all'**organo di gestione** attribuendogli **"piena responsabilità"** nell'adozione, gestione e monitoraggio della strategia di resilienza operativa digitale, nella gestione dei **rischi ICT** e nella revisione e approvazione della politica aziendale sul ricorso a fornitori terzi di servizi ICT (cd. ICT Third Party Providers – TPPs), rafforzando inoltre il ruolo e le responsabilità delle funzioni interne ICT. DORA conferisce inoltre alle autorità competenti il potere di applicare sanzioni amministrative e misure correttive ai membri dell'organo di gestione per qualsiasi violazione del regolamento .

I **requisiti** di **DORA** relativi alla gestione del rischio ICT risultano coerenti con le linee guida della European Banking Authority (EBA) sulla sicurezza e la gestione del rischio ICT (EBA/GL/2019/04) e dell'European Insurance and Occupational Pensions Authority (EIOPA) sulla sicurezza e la governance ICT (EIOPA-BoS-20/600) rafforzandone tuttavia la portata e il relativo approccio di supervisione. Inoltre la **natura vincolante del regolamento** e dei nuovi requisiti, rientrando nell'ambito della legislativa

primaria, intensificherà e renderà maggiormente incisiva l'azione di vigilanza sugli operatori che dovranno farsi trovare preparati al confronto con le autorità.

Il nuovo framework per la gestione del rischio ICT richiede di stabilire dei **livelli di tolleranza del rischio** per interruzioni ICT supportati da **indicatori di performance** e **metriche** di rischio. Gli operatori devono inoltre identificare le loro **"funzioni critiche o importanti" (CIFs)** e mappare i relativi asset e interdipendenze. L'inclusione del concetto di CIFs nel testo finale del DORA rappresenta un'evoluzione significativa che affina il focus dell'intero framework (in particolare per quanto riguarda la segnalazione degli incidenti, i test e la gestione del rischio delle terze parti). L'aderenza ai requisiti in tale ambito richiederà alla maggior parte degli operatori di **ampliare e rafforzare** le proprie **capacità di resilienza operativa**, di definire e **articolare** più chiaramente la propria **propensione al rischio di interruzione delle funzioni critiche** (non solo per un guasto tecnologico o cyber incident) e di essere in grado di **mappare e comprendere** con maggiore precisione le **interconnessioni** tra i propri **asset**, **processi** e **sistemi ICT** e le modalità con le quali questi supportano l'erogazione dei **servizi**.

Una novità del testo finale del DORA è l'obbligo di effettuare **business impact analysis** basate su **scenari di "grave interruzione dell'attività"** (requisito previsto anche dalle linee guida EBA). Tale requisito accrescerà la **pressione** della **vigilanza** verso lo sviluppo di metodi più sofisticati di costruzione e testing degli scenari di rischio (trend che si sta già osservando in UK per gli operatori tenuti ad applicare il nuovo framework di resilienza operativa del Regno Unito) e il rafforzamento del livello di ridondanza e sostituibilità dei sistemi che supportano le CIFs.

2. Classificazione e segnalazione degli incidenti ICT – consolidamento dei requisiti esistenti con significativi aspetti evolutivi

I requisiti DORA riguardanti la segnalazione degli incidenti consentiranno di **semplificare** una serie di **obblighi UE già esistenti** per gli operatori del settore finanziario rafforzandone la portata. I nuovi requisiti infatti puntano a creare un **nuovo framework** per la classificazione, notifica e segnalazione degli incidenti, che richiederà agli operatori di **rafforzare** la loro **capacità di raccogliere**, **analizzare**, **scalare** e **diffondere** le **informazioni** relative agli incidenti e alle minacce ICT. Nell'attuale contesto di mercato la maggior parte degli operatori non dispone di capacità sufficienti per valutare l'impatto quantitativo degli incidenti e analizzarne le cause in linea con gli standard DORA.

Il testo finale del DORA integra inoltre le **minacce informatiche significative ("significant cyber threats")** tra le casistiche di **eventi da classificare**, ma, coerentemente con le modifiche apportate alla Direttiva sulla Sicurezza delle Reti e dell'Informazione (Direttiva NIS), la segnalazione di tali eventi sarà facoltativa. Tuttavia, nel caso in cui un cliente o una controparte siano esposti a una minaccia informatica significativa, DORA prevede per gli operatori l'obbligo di notifica e di fornitura di adeguate informazioni sulle misure di protezione. I nuovi standard prevedono inoltre l'obbligo di **registrare tutte le minacce informatiche significative**, il che richiederà **capacità più avanzate** di monitoraggio, gestione e risoluzione degli **incidenti cyber**.

Per quanto riguarda la **segnalazione** degli **incidenti legati alle tecnologie ICT**, il testo finale del regolamento elimina tutte le scadenze della proposta originaria e delega alle autorità europee di

vigilanza (EBA, ESMA, EIOPA) il compito di specificarle negli standard tecnici (entro 18 mesi dall'entrata in vigore del regolamento). Per avere un quadro più chiaro degli impatti operativi in tale ambito bisognerà pertanto attendere.

Infine, ci si attende dalle autorità europee di vigilanza (ESAs) una **relazione congiunta** sugli esiti della **valutazione di fattibilità** in merito ad un'ulteriore **centralizzazione del processo di reporting degli incidenti** attraverso l'istituzione di un **unico Hub UE** per la segnalazione degli incidenti ICT. La semplificazione del processo segnaletico consentirebbe di ridurre l'onere di adempiere a molteplici obblighi di reporting, favorendo al contempo una migliore comprensione delle minacce informatiche su base transfrontaliera.

3. Test di resilienza operativa digitale - nuovi requisiti sfidanti

DORA prevede requisiti di test del livello di resilienza operativa digitale per **tutte le entità** incluse nell'ambito di applicazione (ad eccezione delle microentità) che dovranno:

- dimostrare di condurre **almeno annualmente** un adeguato set di **test di sicurezza e resilienza sui propri "sistemi e applicazioni ICT critici"** (un livello potenzialmente più granulare delle CIFs);
- **indirizzare** le **vulnerabilità individuate** dai test. Unitamente al requisito sulla business impact analysis, questo aspetto potrebbe diventare un'**area significativa di controllo da parte delle autorità di vigilanza** spingendo gli operatori a sviluppare capacità di test e di analisi di scenario più ampie e accurate rispetto ai modelli attualmente in uso.
- inoltre, le **entità che superano una certa soglia di rilevanza e maturità sistemica** (che sarà specificata dai Regulatory Technical Standard), dovranno condurre **Threat Lead Penetration Test (TLPT)** "avanzati" **ogni tre anni** (salvo diverse previsioni delle autorità nazionali su base individuale).

A riguardo i regolatori hanno specificato che la **metodologia** per i test TLPT deve essere sviluppata **in linea** con il framework **TIBER-EU della Banca Centrale Europea** (BCE), in modo che gli operatori che stanno già conducendo o hanno programmato la conduzione di tali test possano far leva sugli investimenti anche ai fini del rispetto dei requisiti DORA.

DORA richiede inoltre l'inclusione di **tutti i fornitori esterni** che **supportano le funzioni critiche o importanti (CIFs)** negli esercizi di test avanzati **(TLPT)**. Tale prassi risulta implementata raramente ad oggi e richiederà sicuramente un significativo effort nella pianificazione oltre che nella mappatura puntuale dei fornitori esterni critici. Qualora uno di questi non potesse partecipare ai test per motivi di sicurezza, DORA consente al fornitore stesso di condurre autonomamente il proprio TLPT in forma di "pooled testing" per le entità di settore cui fornisce servizi. Questa, ad oggi, è un'area di "shared assurance" tutta da sviluppare che richiederà un'azione collettiva condivisa a livello di settore per poter essere attuata.

4. Governo e gestione del rischio delle terze parti – rafforzamento del framework europeo in ambito finanziario

Deloitte.

I requisiti per la gestione del rischio delle terze parti previsti dal DORA risultano allineati agli attuali orientamenti delle autorità di vigilanza europee, prevedendo tuttavia un ampliamento del perimetro di applicazione dato che gli attuali orientamenti ESMA e EIOPA riguardano esclusivamente l'esternalizzazione ai fornitori critici (CSPs). DORA estenderà pertanto i requisiti al perimetro riguardante l'esternalizzazione ICT a fornitori non critici anche agli operatori che non applicano già le linee guida EBA.

I requisiti DORA per la gestione del rischio delle terze parti, in linea con gli orientamenti ESAs, prevedono una serie di **condizioni contrattuali minime che gli operatori devono includere nei contratti di outsourcing ICT** entro il termine di attuazione del DORA previsto per il quarto trimestre 2024. La previsione da parte di una disposizione legislativa vincolante come DORA di clausole contrattuali specifiche incrementerà il potere negoziale degli operatori di settore nella negoziazione di tali termini con i fornitori, aspetto sul quale in passato non si sono avuti riscontri tangibili. Si prevede inoltre che alcuni termini contrattuali, come la clausola di "accesso illimitato ai locali" del fornitore nei contratti a supporto delle funzioni critiche o importanti, comporteranno un percorso di implementazione non semplice rispetto ad altre condizioni.

Nel corso dell'iter di costruzione del DORA il regolamento è stato emendato per rendere lo **sviluppo di una "strategia olistica multi-vendor"** una componente **opzionale** della complessiva strategia di gestione del rischio ICT, anche se le autorità di vigilanza avranno comunque diverse leve per indirizzare gli operatori in tal senso. È infatti richiesto di effettuare una **valutazione del rischio di concentrazione** di tutti i contratti di outsourcing che supportano le funzioni critiche o importanti, aspetto che potrebbe rendere difficile giustificare determinate decisioni sui modelli operativi senza l'adozione di un approccio multi-CSP o multi-vendor o dimostrare i razionali per i quali ciò non sia necessario.

5. Framework di supervisione dei fornitori ICT critici – la prima iniziativa a livello mondiale di regime di supervisione delle terze parti in ambito finanziario

I nuovi poteri di supervisione delle autorità europee di vigilanza previsti dalla proposta originaria del DORA sono stati in gran parte mantenuti nel testo finale. Ciò significa che i **fornitori** designati come **critici** saranno soggetti ad **ampi poteri di supervisione** che consentiranno alle autorità di vigilanza europee di valutarli, di richiedere loro di modificare le misure di sicurezza e sanzionarli in caso di mancata conformità ai requisiti. Ciò spingerà i fornitori a dimostrare di essere in grado di rafforzare il livello di resilienza delle operations a supporto degli operatori del settore finanziario, con particolare focus ai casi in cui i servizi forniti impattano le funzioni critiche o importanti.

Nel regolamento sono state aggiunte anche diverse **salvaguardie** in merito alla possibilità per le autorità di **imporre agli operatori di sospendere o risolvere i loro contratti con fornitori critici**. Ovviamente questi poteri saranno esercitati solo in circostanze eccezionali e previa valutazione del loro impatto a livello di settore.

La versione finale del DORA, inoltre, amplia in modo significativo il **ruolo** del **Joint Oversight Forum (JOF),** gruppo composto dalle autorità europee di vigilanza (ESAs), altre autorità competenti, supervisori ed esperti indipendenti. Il JOF avrà un ruolo più importante nello sviluppo di best practice per la

supervisione dei fornitori critici e potrebbe, col tempo, stabilire standard più precisi per il livello di resilienza atteso da tali fornitori.

Importanti standard tecnici sono in arrivo

Una caratteristica chiave del regolamento DORA è che i **dettagli tecnici** sul funzionamento operativo **delle nuove norme sono delegati alla regolamentazione secondaria** (nota nella politica dell'UE come "livello 2"). Le **autorità europee di vigilanza** (ESAs) svilupperanno le regole operative prevalentemente sotto forma di **Regulatory Technical Standard (RTS)** o **Implementing Technical Standards (ITS)**. Relativamente al framework di supervisione dei fornitori critici, la Commissione europea svilupperà due Atti Delegati (si veda la Tabella 1 per un elenco di tutte le misure di Livello 2 del DORA).

Il processo di costruzione del livello 2 della regolamentazione implica per gli operatori un **ulteriore periodo di 12-18 mesi di incertezza sotto il profilo regolamentare** rispetto ad alcune parti del regolamento, in particolare per quanto riguarda il **framework di segnalazione degli incidenti ICT** e le **regole e ambito di applicazione dei test avanzati di resilienza**. In questo lasso temporale, gli operatori dovranno comunque portare avanti il processo di adeguamento sulla base del testo normativo primario (livello 1). Gli operatori dovranno inoltre agire in ottica proattiva (e non reattiva) prestando molta attenzione alle versioni in consultazione degli RTS/ITS nel momento in cui verranno rilasciate, essendo queste solitamente molto vicine alle versioni finali.

Tabella 1: Timeline per lo sviluppo della regolamentazione di livello 2 del DORA

Mandato di livello 2	Deadline per gli standard definitivi ESAs
RTS sulle procedure di classificazione degli incidenti ICT e delle minacce cyber	12 mesi dall'entrata in vigore (stimato per il 3° trimestre 2023)
RTS sul livello di dettaglio richiesto nelle strategie di gestione dei fornitori terzi (TPP)	
RTS sugli ulteriori elementi del framework di gestione del rischio ICT	
ITS sul Registro delle informazioni relative agli accordi contrattuali con fornitori in ambito ICT	
RTS sulla segnalazione alle autorità di incidenti ICT e cyber gravi	18 mesi dall'entrata in vigore (stimato per il 1° trimestre 2024)
RTS sull'ambito di applicazione e sugli elementi addizionali per i test avanzati	
RTS sulle disposizioni contrattuali chiave per il subappalto di funzioni/servizi a	

	supporto delle funzioni critiche o importanti	
	RTS sulla designazione dei membri di un Joint Examination Team	
	RTS sulle informazioni che un CTPP deve fornire alle autorità di vigilanza (cd. Lead Overseer)	
	Atto delegato della Commissione Europea sulla designazione dei fornitori di servizi critici (CTPP)	
	Atto delegato della Commissione Europea sui contributi di vigilanza per i fornitori di servizi critici (CTPP)	
	Report dell'ESA sulla creazione di un hub centrale UE per la segnalazione degli incidenti	24 mesi dall'entrata in vigore (stimato per il 3° trimestre 2024)

E’ tempo di agire per gli operatori di settore

La finalizzazione del DORA richiede agli operatori del settore finanziario di iniziare a pianificare concretamente la fase di implementazione dei nuovi/rafforzati requisiti previsti dal regolamento. Come detto in apertura della presente analisi, riteniamo che il DORA cambierà il modo in cui gli operatori del settore FS affrontano la resilienza operativa, in quanto li spingerà ad avere una **visione olistica della resilienza** e a **sviluppare nuove e sofisticate capacità** in aree quali l'identificazione delle funzioni critiche o importanti, il reporting degli incidenti, la misurazione dell'impatto sul business e i test. DORA deve essere visto dagli operatori come un **catalizzatore** per promuovere un **cambiamento strategico** nelle **modalità di gestione dei rischi digitali** e nel rafforzamento del livello di consapevolezza con cui il management e i Consigli di amministrazione sono in grado di **valutare l'impatto sul business delle *operational disruptions* e comprendere le misure di mitigazione** a loro disposizione.

Realizzare quanto richiesto dai nuovi standard regolamentari in un periodo di **24 mesi** costituisce un’**importante sfida**, considerando anche che gli operatori dovranno tenere conto degli standard tecnici di livello 2 man mano che saranno finalizzati. In tale contesto, è fondamentale che gli operatori focalizzino e si preparino ad affrontare i due aspetti seguenti:

1. **Azione di vigilanza molto più incisiva in ambito ICT**: dalla sua entrata in vigore DORA conferirà alle autorità di vigilanza nazionali ed europee nuovi e ampi poteri in materia di resilienza operativa digitale. DORA non può pertanto essere visto come un mero esercizio di compliance normativa ma come un fattore abilitante il rafforzamento del livello di resilienza operativa e le capabilities in ambito. Con l’aumentare del livello di comprensione del livello di resilienza

operativa da parte delle autorità di vigilanza, aumenteranno anche le aspettative e le richieste agli operatori, come dimostra ad esempio l'esperienza osservata finora in UK relativamente all'applicazione del nuovo framework di vigilanza sulla resilienza operativa del Regno Unito. Gli operatori devono inoltre essere consapevoli che il coinvolgimento di più autorità competenti, con obiettivi e priorità spesso non perfettamente allineate aumenta il livello di complessità del percorso di adeguamento e dell'interlocuzione.

Per comprendere come si svilupperanno gli approcci di vigilanza, gli operatori dovrebbero porre particolare attenzione alle aree di DORA che richiedono output sistematici sui quali le autorità di vigilanza faranno sicuramente challenge. Ad esempio, i nuovi requisiti per l'analisi di impatto sul business nel capitolo sulla gestione del rischio ICT, unitamente all'obbligo di effettuare almeno annualmente test di resilienza per i sistemi a supporto delle funzioni critiche o importanti e di indirizzare qualsiasi vulnerabilità identificata, rappresentano ambiti di controllo significativi che saranno indubbiamente attenzionati dalle autorità di vigilanza. È molto probabile che le autorità di vigilanza insistano sul livello di severity degli scenari utilizzati, sulla sofisticazione delle metodologie di testing, sulla granularità della mappatura dei sistemi sottostanti le funzioni critiche o importanti e sulla completezza dei piani di rimedio a fronte delle vulnerabilità rilevate.

2. **Identificazione delle aree che richiederanno investimenti e un percorso evolutivo**: molti dei nuovi requisiti di DORA richiederanno investimenti sostanziali nel rafforzamento del framework di governance, risk e compliance in ambito ICT, Cyber e Gestione del Rischio delle Terze Parti, nonché piani di un lavoro per indirizzare le vulnerabilità operative che emergeranno. Gli operatori dovrebbero condurre un'analisi di impatto dei requisiti finali del DORA (livello 1), aggiornandola ed integrandola dinamicamente man mano che saranno disponibili le bozze degli standard regolamentari di livello 2 (RTS/ITS), in modo da identificare e valutare le attuali carenze di capacità, risorse e competenze che dovranno essere corrette nel corso del periodo di adeguamento di 24 mesi. Sulla base delle nostre valutazioni sul testo DORA definitivo, l'analisi dei gap dovrebbe focalizzarsi in particolare su:

- Framework di governance del rischio ICT, compresa l'identificazione delle funzioni critiche o importanti (CIF);
- Livello di maturità dei processi di raccolta e analisi dei dati su incidenti e minacce;
- Livello di sofisticazione degli scenari di test e capacità di costruzione di scenari ad elevata severity;
- Processi e dei dati in ambito outsourcing ICT (compresa la capacità degli operatori di analizzare i rischi di concentrazione su terze e quarte parti).

Alcuni operatori finanziari rilevanti per dimensione/complessità, come i grandi gruppi transfrontalieri, allo stato attuale potrebbero disporre di un livello di maturità e capacità più elevati rispetto ad altri con conseguenti vantaggi nel percorso di adeguamento ai nuovi requisiti DORA. Tuttavia, è più probabile che le autorità di vigilanza abbiano aspettative maggiori verso i grandi operatori e si attendano una capacità di market-leading da parte di operatori per i quali le operational disruptions potrebbero avere conseguenze sistemiche data la criticità dei servizi erogati. Tutti gli operatori, pertanto, saranno inevitabilmente messi alla prova nel periodo di adeguamento di 24 mesi che inizierà

alla fine dell'anno in corso. Per questo motivo nessuno può permettersi di temporeggiare ed è fondamentale iniziare oggi stesso a pianificare il percorso di convergenza verso i nuovi standard regolamentari.

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