Regolamento Dora: ecco cosa devono fare le aziende del settore finanziario per adeguarsi

Testi a cura di:
Orlando Lio, Director di Intellera Consulting
Claudio Paganelli, Director di Intellera Consulting
Marco Tulliani, Associate Partner di Intellera Consulting

LEGGI SUL SITO

INDICE DEGLI ARGOMENTI

Il Regolamento Dora è entrato in vigore il 16 gennaio 2023 e sarà vincolante a partire dal 17 Gennaio 2025. È pertanto opportuno pianificare e avviare fin da subito un percorso di adeguamento. Ecco tutto quello che c'è da sapere.

Dal 16 gennaio 2023 (20 giorni dopo pubblicazione in Gazzetta ufficiale del 27 dicembre 2022, che ha seguito l'approvazione del Parlamento UE del 10 Novembre 2022) è entrato in vigore il **Regolamento DORA**.

Il **Digital Operational Resilience Act** *ha l'ambizioso obiettivo di consolidare e armonizzare a livello europeo i principali requisiti di cybersecurity con riferimento alla* **resilienza operativa digitale nel settore finanziario**, *rivolgendosi a banche, compagnie di assicurazione, società di servizi di criptovalute, istituzioni finanziarie e i loro fornitori critici.*

Tale Regolamento è parte di un più ampio pacchetto europeo di misure strategiche per l'ambito tradizionale e fintech che intende assicurare che le imprese del settore siano in grado di affrontare attacchi informatici, attraverso l'implementazione di misure in ambito governance, cybersecurity, ICT risk management e incident reporting.

L'obiettivo è di creare un **Framework di Risk Management,** *al fine di garantire la resilienza digitale finanziaria delle Organizzazioni di settore.*

1

IL PERCORSO DI ADEGUAMENTO

Il Regolamento DORA troverà applicazione e **sarà vincolante a partire dal 17 Gennaio 2025** (decorsi 24 mesi dalla sua pubblicazione nella Gazzetta Ufficiale dell'Unione Europea). Entro tale termine, banche, assicurazioni e operatori di criptovalute dovranno adeguare i loro sistemi interni di cyber resilience.

Ma ora che il Regolamento DORA è in vigore, è opportuno pianificare ed avviare un percorso di adeguamento. L'applicazione dei requisiti di DORA, infatti, è già possibile e per le varie realtà è utile iniziare fin da subito a ipotizzare quali impatti avranno queste misure sulla propria organizzazione.

Siamo convinti che la normativa agisca più come semplificazione di quanto già previsto, che come un obbligo complesso da attuare.

Banche, enti finanziari e tutti gli attori che rientrano a perimetro del Regolamento DORA, devono prepararsi a recepire il Regolamento, sviluppando o aggiornando le proprie procedure di segnalazione degli incidenti in linea con i nuovi requisiti normativi.

2.

I 6 PILLAR CHE LE ORGANIZZAZIONI DOVRANNO IMPLEMENTARE

Il Regolamento propone sei diversi "pillar" che le Organizzazioni dovranno implementare:

- **ICT Governance**. In questo ambito l'obiettivo è di favorire un migliore allineamento delle strategie di gestione dei rischi ICT da parte delle entità finanziarie. L'Organo di Gestione avrà un ruolo fondamentale nell'attribuire responsabilità e ruoli per tutte le funzioni ICT, controllare e monitorare la gestione dei rischi ICT e, infine, allocare adeguatamente investimenti e formazione in ambito ICT;
- **ICT Risk Management.** In questo contesto, l'obiettivo di migliorare e armonizzare le regole per la gestione del rischio ICT. Le entità finanziarie dovranno istituire e mantenere strumenti e sistemi ICT resilienti attraverso l'identificazione dei rischi ICT, la predisposizione di misure di protezione e prevenzione, il rilevamento di minacce, la gestione degli incidenti, l'implementazione di strategie di continuità operativa e piani di ripristino in caso di disastro;
- **Gestione degli incidenti.** Prevede specifici obblighi in materia di gestione degli incidenti ICT. Le organizzazioni di settore dovranno implementare un sistema di mappatura, in cui si classificano i vari incidenti sulla base di criteri descritti nel Regolamento e ulteriormente definiti dalle AEV (Autorità Europee di Vigilanza) per specificare le soglie di rilevanza;
- **Test di Resilienza.** Questo pillar rappresenta la maggiore novità, perché viene specificato che le entità finanziarie dovranno essere sottoposte periodicamente a test per accertarne il grado di

maturità, identificarne punti deboli e definire eventuali misure correttive. Tale disposizione evidenzia l'obiettivo del regolatore di adottare un approccio proattivo che non si limiti alle sole misure correttive "di reazione". In questa fase, le attività di Penetration Test e, più in generale, di Red-Teaming, dovranno essere svolte solo da soggetti autorizzati e opportunamente certificati. Al riguardo, per lo svolgimento di questi Test, può essere utilizzato il Framework previsto dalla Comunità Europea, ossia il TIBER EU, recepito in Italia come TIBER IT, adottato anche da Banca d'Italia, la Consob e l'IVASS.

- **Rischi Terze Parti.** Per questo ambito il regolatore specifica che le varie entità dovranno garantire il rispetto di norme che si applicano al monitoraggio dei rischi ICT derivanti da Terze Parti e armonizzare gli elementi essenziali del servizio in tutte le fasi del contratto: stipula, esecuzione, estinzione e fase post-contrattuale;
- **Condivisione delle informazioni.** In questo pillar l'obiettivo è quello di sopperire alla mancanza di comunicazioni tra le varie entità all'interno della Comunità Europea. Viene infatti consentita, alle organizzazioni finanziarie, la stipula di accordi per scambiarsi informazioni e dati sulle minacce informatiche, al fine di rafforzare la cooperazione tra gli Stati membri.

3.

LE AZIONI ESSENZIALI

Concretamente, cosa devono fare le aziende per conformarsi agli obblighi più imminenti? Abbiamo definito una metodologia concreta, che prevede 3 azioni essenziali da eseguire:

- **Gap analysis dell'ICT risk management framework**, iniziando da un confronto tra gli obiettivi da raggiungere e la situazione attuale;
- **Revisione del Report degli incidenti**;
- **Assessment dei fornitori critici e rinegoziazione dei contratti con gli stessi**.

È importante porre attenzione al terzo punto: l'ultimo Report del Word Economic Forum (Global Security Outlook 2023) mette in guardia le aziende dal Rischio Terze Parti nel contesto geopolitico, poiché gli ultimi incidenti noti hanno coinvolto pesantemente la Supply Chain. E le autorità di vigilanza finanziaria hanno poteri di sorveglianza sui rischi dovuti alla dipendenza delle entità finanziarie da fornitori terzi di servizi.

In questo contesto, gli aspetti contrattuali chiave come stipula, esecuzione, fase post-contrattuale saranno armonizzati per garantire che le società finanziarie monitorino i rischi di terzi. E i fornitori terzi di servizi ICT critici saranno sottoposti a un quadro di sorveglianza dell'Unione. In questo ambito, per ciascun fornitore terzo di servizi ICT critico sarà definita un'autorità di sorveglianza capofila alla quale sono conferiti poteri idonei a garantire l'adeguato monitoraggio dei fornitori di servizi tecnologici che assolvono una funzione critica per il funzionamento del settore finanziario.

NETWORK DIGITAL 360

Network Digital360 è il più grande network in Italia di testate e portali B2b dedicati ai temi della Trasformazione Digitale e dell'Innovazione Imprenditoriale, con oltre 50 fra portali, canali e newsletter.
Ha la missione di diffondere la cultura digitale e imprenditoriale nelle imprese e pubbliche amministrazioni italiane e di fornire a tutti i decisori che devono valutare investimenti tecnologici informazioni aggiornate e approfondite.
Il Network è parte integrante di Digital360HUB, il polo di Demand Generation di Digital360, che mette a disposizione delle tech company un'ampia gamma di servizi di comunicazione, storytelling, pr, content marketing, marketing automation, inbound marketing, lead generation, eventi e webinar.

VIA COPERNICO, 38
20125 - MILANO
TEL. 02 92852785
MAIL: MARKETING@DIGITAL4.BIZ