Grant Thornton

TOPHIC GIUGNO

Nuove tecnologie: verso una compliance integrata

Contenuti

Overview

Governare l’innovazione: AI, resilienza operativa e compliance

Parere dell’Esperto

Perché l’Intelligenza Artificiale sta cambiando la compliance delle imprese

Approfondimento

DORA come pilastro della compliance digitale integrata

Contatti

Overview

I nostri esperti approfondiscono le principali implicazioni dell'intelligenza artificiale e delle più recenti normative europee in materia di compliance digitale. L'adozione di sistemi di AI offre nuove opportunità per rafforzare il monitoraggio, la gestione del rischio e i processi di controllo interno, ma introduce al contempo nuove responsabilità in termini di governance, trasparenza e supervisione. In questo contesto, discipline come l'AI Act e il Regolamento DORA promuovono una visione integrata della compliance, nella quale intelligenza artificiale, cybersicurezza, resilienza operativa e gestione del rischio tecnologico sono strettamente connesse. Per le imprese e gli operatori finanziari, la sfida consiste nel trasformare gli obblighi normativi in strumenti di crescita, sviluppando assetti organizzativi, competenze e presidi adeguati a governare l'innovazione in modo sicuro, sostenibile e conforme alle regole.

Discipline come l'AI Act e il Regolamento DORA promuovono una visione integrata della compliance, nella quale intelligenza artificiale, cybersicurezza, resilienza operativa e gestione del rischio tecnologico sono strettamente connesse.

Parere dell'esperto

Silvia Laura Rossi
Avvocato - Manager

Investire nella cultura della responsabilità tecnologica consente alle imprese di comprendere opportunità e limiti dell'intelligenza artificiale, ridurre i rischi derivanti da un uso improprio e rafforzare la capacità di governare l'innovazione in modo sostenibile e conforme alle regole.

PERCHÉ L'INTELLIGENZA ARTIFICIALE STA CAMBIANDO LA COMPLIANCE DELLE IMPRESE

QUAL È OGGI IL RUOLO DELL'INTELLIGENZA ARTIFICIALE NELLA COMPLIANCE AZIENDALE?

L'intelligenza artificiale sta trasformando profondamente i sistemi di controllo interno delle imprese. Grazie all'analisi automatizzata dei dati e alla capacità di individuare anomalie e situazioni di rischio, i sistemi di intelligenza artificiale consentono di rendere la compliance un processo continuo e dinamico. Rafforzano l'efficacia delle attività di monitoraggio, favorendo modelli di prevenzione più evoluti e una migliore capacità di gestione del rischio.

L'UTILIZZO DI NUOVE TECNOLOGIE COMPORTA NUOVI OBBLIGHI PER LE IMPRESE?

Le imprese che sviluppano o utilizzano sistemi di intelligenza artificiale sono chiamate a confrontarsi con un quadro normativo sempre più articolato. Con l'entrata in vigore dell'AI Act, l'Unione europea ha introdotto una disciplina fondata su un approccio basato sul rischio, che prevede obblighi differenziati in funzione delle caratteristiche dei sistemi impiegati. La compliance non può più essere considerata un insieme di adempimenti formali, ma rappresenta un elemento strategico della governance aziendale e della gestione del rischio tecnologico.

PERCHÉ SI PARLA SEMPRE PIÙ DI COMPLIANCE DIGITALE INTEGRATA?

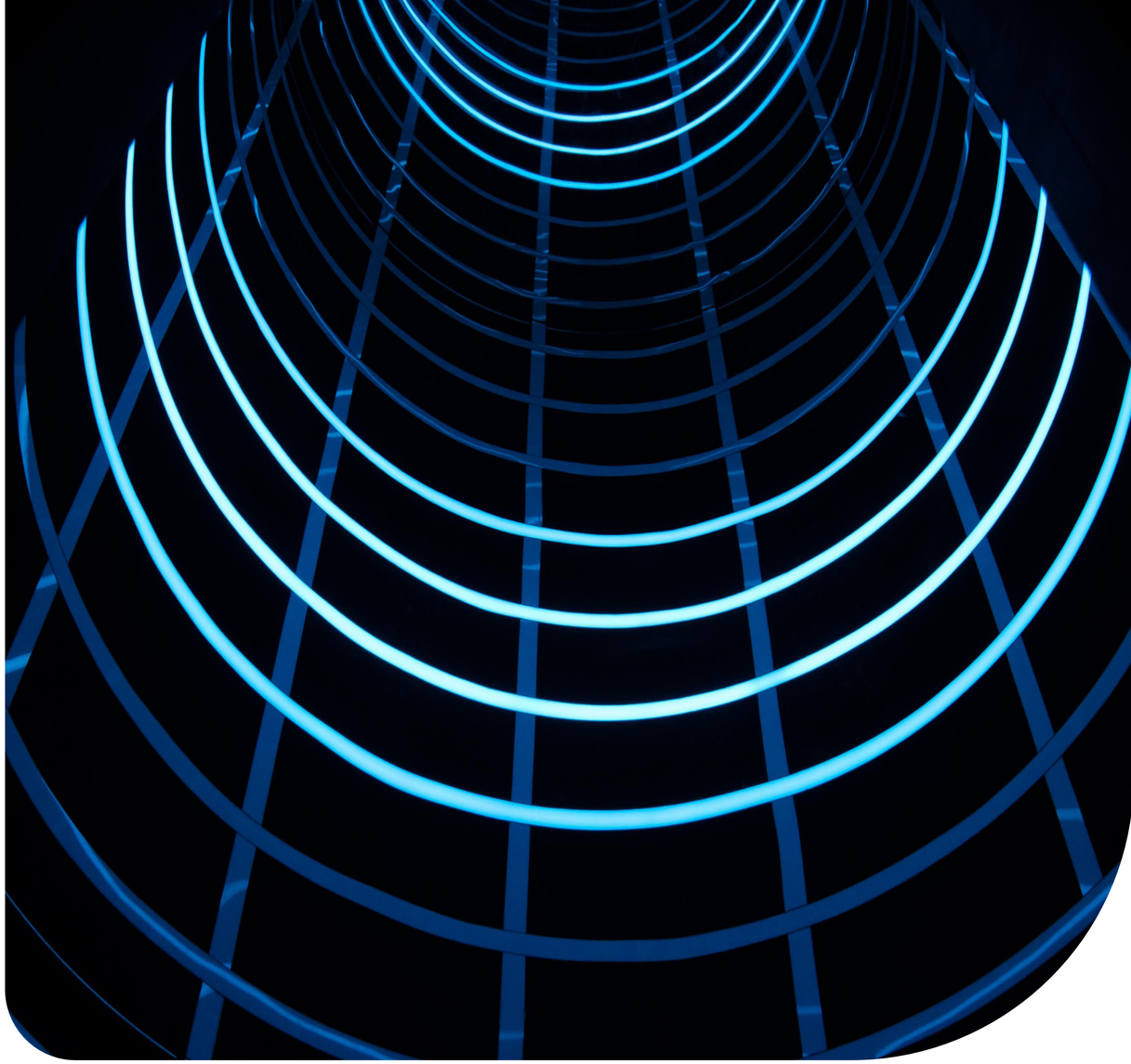
L'evoluzione normativa europea sta progressivamente superando una visione frammentata della compliance. Protezione dei dati, cybersicurezza, resilienza digitale e governance dell'intelligenza artificiale sono sempre più interconnesse e richiedono un approccio unitario. Le aziende devono quindi sviluppare assetti organizzativi capaci di coordinare funzioni legali, IT, cybersecurity, risk management e controllo interno, favorendo una gestione integrata del rischio tecnologico.

QUALI SONO LE PRINCIPALI SFIDE INTRODOTTE DALL'AI ACT?

L'AI Act rappresenta il primo quadro normativo organico dedicato all'intelligenza artificiale e introduce un approccio basato sul rischio. La conformità non si esaurisce nel rispetto formale delle regole, ma richiede una governance strutturata, sistemi di valutazione dei rischi, adeguata documentazione interna e una costante supervisione umana. L'obiettivo è garantire che l'innovazione tecnologica sia sviluppata e utilizzata in modo sicuro, affidabile e rispettoso dei diritti fondamentali.

PERCHÉ LA FORMAZIONE DIVENTA UN ELEMENTO STRATEGICO DELLA COMPLIANCE AI?

La diffusione dei sistemi di intelligenza artificiale rende indispensabile sviluppare competenze adeguate all'interno delle organizzazioni. Il principio di *AI literacy*, introdotto dall'AI Act, attribuisce particolare rilievo alla formazione dei soggetti coinvolti nello sviluppo e nell'utilizzo dei sistemi di intelligenza artificiale. Investire nella cultura della responsabilità tecnologica consente alle imprese di comprendere opportunità e limiti dell'intelligenza artificiale, ridurre i rischi derivanti da un uso improprio e rafforzare la capacità di governare l'innovazione in modo sostenibile e conforme alle regole. L'evoluzione normativa europea richiede una visione sempre più integrata della compliance, nella quale governance dell'intelligenza artificiale, cybersicurezza e resilienza operativa rappresentano elementi strettamente connessi. In questo contesto si inseriscono le più recenti discipline europee, che trasformano tali principi in requisiti organizzativi e operativi concreti per le imprese.



Approfondimento

Marco Ondoli
Senior Manager

DORA come pilastro della compliance digitale integrata

REGOLAMENTO (UE) 2022/2554 - DORA

La crescente integrazione tra gestione del rischio tecnologico, cybersicurezza e resilienza operativa trova una delle sue espressioni più significative nel Regolamento (UE) 2022/2554 (DORA), che rappresenta uno dei principali tasselli del percorso europeo verso una compliance digitale integrata.

Il Regolamento DORA è in applicazione dal 17 gennaio 2025 per banche, istituti di pagamento, imprese di investimento e altri intermediari finanziari vigilati. Per questi soggetti la domanda non è più “dobbiamo adeguarci?” bensì “quanto siamo davvero pronti?” Per gli intermediari finanziari iscritti all’albo ex art. 106 TUB — Confidi, società di leasing, di factoring e di credito al consumo — la scadenza è fissata nel 1° gennaio 2027; undici mesi, considerata la complessità degli interventi richiesti, sono pochi.

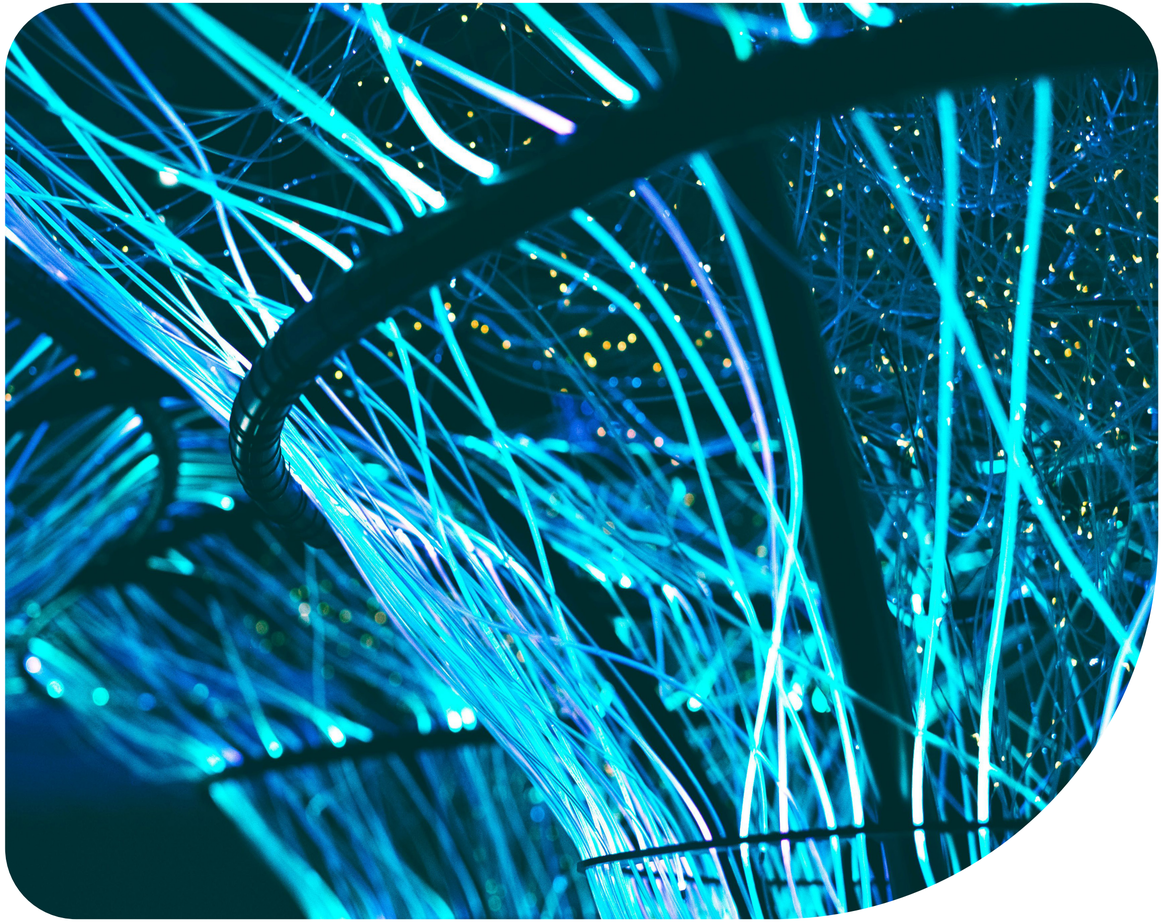
Il team Business Risk Services di Grant Thornton ha maturato una competenza diretta su entrambi i fronti: l’adeguamento ai requisiti DORA, con gap analysis e implementazione di framework e politiche, e la verifica indipendente del livello di conformità raggiunto, attraverso audit strutturati applicabili a tutte le entità per cui il Regolamento è già in vigore. I casi riportati di seguito mostrano come i principi della compliance digitale integrata trovino concreta applicazione nei processi di gestione del rischio e della resilienza operativa, offrendo una rappresentazione concreta delle sfide e del livello di maturità raggiunto dal mercato italiano.

CASE STUDY 1

Gap analysis e costruzione del framework DORA presso un intermediario finanziario vigilato

SCENARIO

Il primo progetto ha avuto origine nel 2023, quando un intermediario finanziario vigilato ha deciso di affrontare in anticipo le implicazioni del Regolamento DORA, ben prima della scadenza del 17 gennaio 2025. La richiesta non era una verifica ex post, ma un accompagnamento proattivo: condurre una gap analysis strutturata sui cinque pilastri DORA per poi costruire e implementare i framework e le politiche necessarie all'adeguamento. Come accade frequentemente, esistevano procedure di gestione del rischio ICT, ma sviluppate in modo non sistematico rispetto alla logica del Regolamento: il punto di partenza era ricondurle a coerenza integrandole con gli elementi mancanti.



1

Il metodo

La gap analysis ha coperto tutti e cinque i pilastri attraverso analisi documentale, interviste strutturate con i referenti delle funzioni coinvolte (ICT, Risk Management, Compliance, Internal Audit) e verifica a campione dei processi operativi. Lo strumento centrale è stata una matrice di assessment su tre dimensioni per ciascun requisito: esistenza del presidio, adeguatezza rispetto alle definizioni DORA, operatività effettiva nel quotidiano. Questa distinzione — tra ciò che esiste sulla carta, ciò che è conforme e ciò che funziona davvero — ha permesso di prioritizzare gli interventi in modo realistico.

2

Le criticità emerse

Le aree più critiche hanno riguardato la gestione degli incidenti ICT (le procedure esistenti non erano allineate ai sei criteri di classificazione dell'art. 18 DORA, con rischio concreto di mancata notifica a Banca d'Italia) e la gestione del rischio di terze parti, con mappatura dei fornitori parziale e contratti privi delle clausole minime richieste.

3

Gli interventi e la soluzione

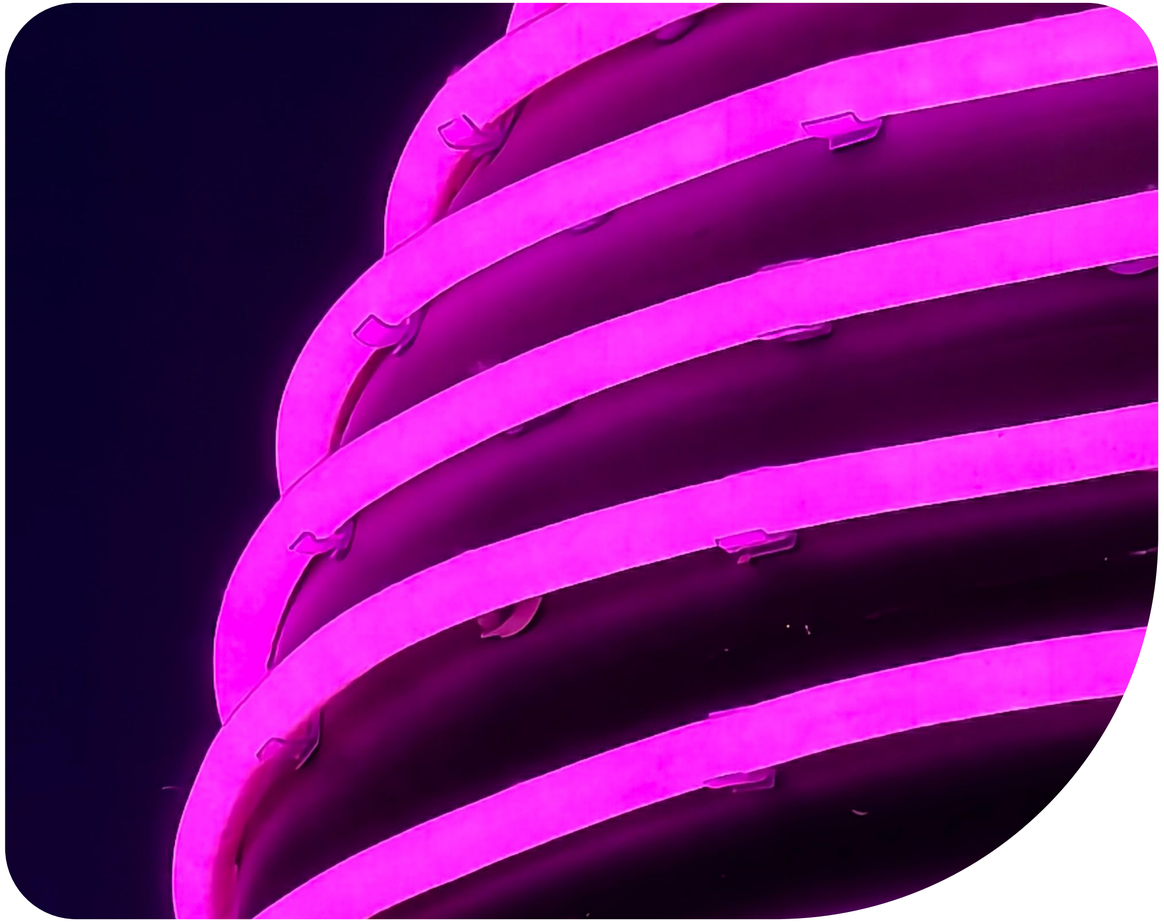
Nel corso del 2024 il team ha affiancato l'organizzazione nell'implementazione: revisione della procedura di Incident Management, costruzione del Registro delle Informazioni per i fornitori critici, aggiornamento dei contratti con clausole DORA-compliant e definizione di una matrice RACI per il rischio ICT.

CASE STUDY 2

Un'autovalutazione su impulso di Banca d'Italia: rispondere a una richiesta di autovalutazione sulla gestione dei rischi ICT DORA

SCENARIO

Il secondo progetto ha coinvolto un intermediario finanziario vigilato che aveva già completato autonomamente un significativo percorso di adeguamento ai requisiti DORA, dotandosi di un corpus documentale strutturato (framework di gestione del rischio ICT, politiche di sicurezza, procedure di incident management, piani di business continuity e disaster recovery, regolamenti per la gestione dei fornitori terzi) approvato dagli organi aziendali. In questo caso non è stata una scelta interna ad avviare il progetto, ma una richiesta esplicita di Banca d'Italia: l'autorità ha chiesto all'intermediario di condurre un'autovalutazione strutturata del proprio livello di presidio sui rischi ICT, specificamente ai fini DORA, utilizzando il modello di autovalutazione predisposto dall'Autorità stessa.



1

Il metodo

Il modello di autovalutazione di Banca d'Italia copre cinque sezioni principali, corrispondenti ai pilastri DORA applicabili: gestione dei rischi ICT (artt. 5-15), classificazione e segnalazione degli incidenti (artt. 17-19), test di resilienza operativa (art. 24-25), gestione del rischio di terza parte (artt. 28-30) e meccanismi di scambio informativo (art. 45). Per ciascun requisito, l'intermediario è chiamato a esprimere un posizionamento e a fornire evidenza documentale della conformità, con riferimento esplicito a policy, procedure e regolamenti interni.

2

I risultati dell'autovalutazione

Grazie al percorso di adeguamento già condotto, la quasi totalità dei requisiti ha ricevuto un posizionamento di piena conformità. I pochi scostamenti rilevati riguardavano aree fisiologicamente in evoluzione: la Business Impact Analysis relativa all'anno precedente era ancora in corso di aggiornamento; l'adeguamento contrattuale con alcuni fornitori ICT terzi, pur avviato con un piano strutturato in due fasi, era parzialmente in attesa dei cicli di rinnovo contrattuali; il processo di change management per applicativi fuori dal perimetro del fornitore principale era in fase di consolidamento attraverso l'adozione di strumenti di ticketing dedicati.

3

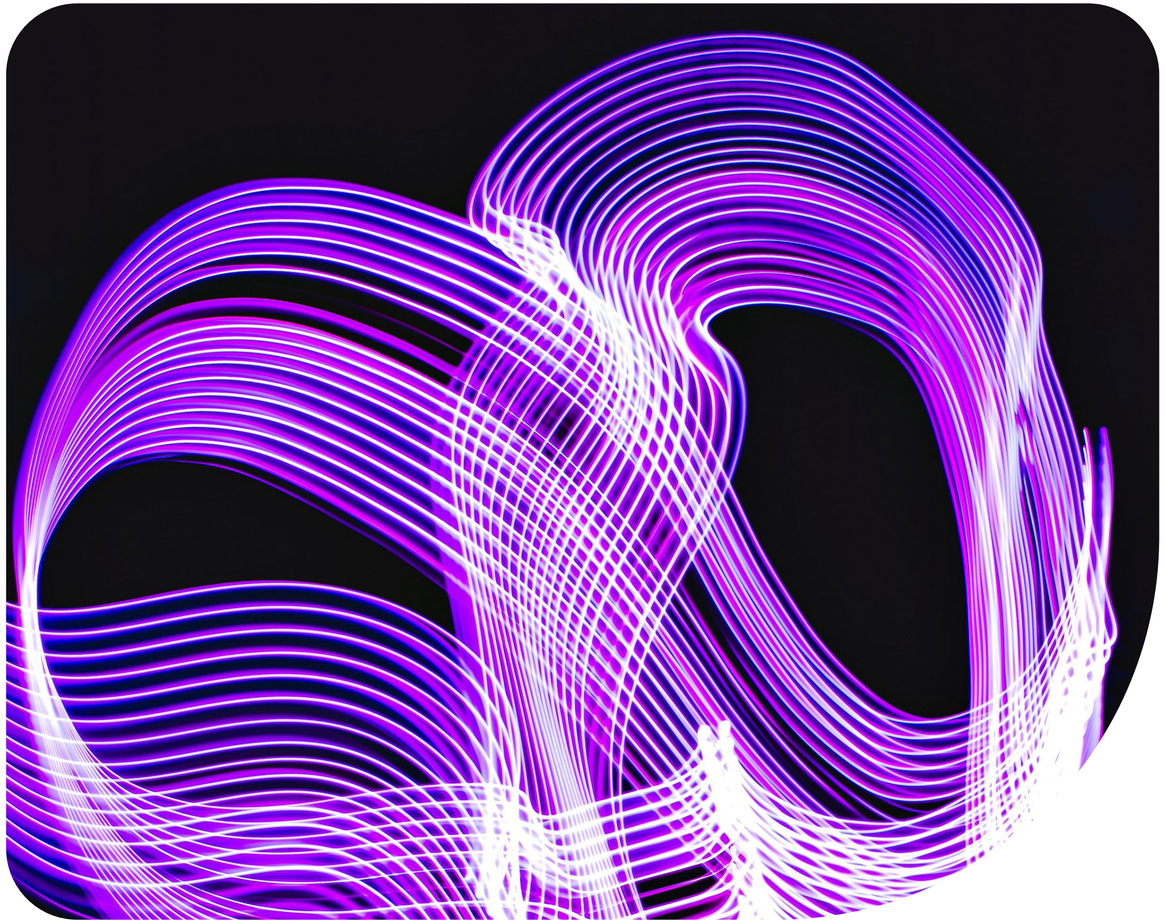
Il segnale per il mercato

Questo caso illustra una dinamica destinata a diventare sempre più frequente: Banca d'Italia non si limita ad attendere le dichiarazioni di conformità delle istituzioni, ma esercita già oggi una vigilanza attiva sui requisiti DORA — anche prima che tutte le scadenze siano scattate. Saper rispondere a questo tipo di richiesta richiede non solo di aver fatto, ma di poterlo dimostrare con evidenza documentale strutturata. La capacità di produrre un'autovalutazione rigorosa, con riferimenti precisi alla normativa interna e ai requisiti regolamentari, è una competenza distinta dall'adeguamento in sé — ed è quella che i supervisori verificano.

Due esperienze, un’unica lezione

La crescente integrazione tra gestione del rischio tecnologico, cybersicurezza e resilienza operativa trova una delle sue espressioni più significative nel Regolamento (UE) 2022/2554 (DORA), che rappresenta uno dei principali tasselli del percorso europeo verso una compliance digitale integrata.

Il Regolamento DORA è in applicazione dal 17 gennaio 2025 per banche, istituti di pagamento, imprese di investimento e altri intermediari finanziari vigilati. Per questi soggetti la domanda non è più “dobbiamo adeguarci?” bensì “quanto siamo davvero pronti?” Per gli intermediari finanziari iscritti all’albo ex art. 106 TUB — Confidi, società di leasing, di factoring e di credito al consumo — la scadenza è fissata nel 1° gennaio 2027; undici mesi, considerata la complessità degli interventi richiesti, sono pochi.



Contatti

I nostri professionisti sono a disposizione per eventuali domande o chiarimenti.

Silvia Laura Rossi
Avvocato - Manager
silvia.rossi@bgt.it.gt.com

Marco Ondoli
Senior Manager
marco.ondoli@gtc.it.gt.com

Grant Thornton

Applying AI where **business happens**