BANKING RESILIENCE 2026:
DALLE RICHIESTE DELLA VIGILANZA AL PIANO DI AZIONE IN VISTA DELLE SCADENZE

12 e 16 ottobre 2026 • Aula virtuale (10.00/13.00)

PREMESSA

La crescente complessità dello scenario tecnologico e l'evoluzione delle minacce cyber stanno portando sicurezza e resilienza operativa al centro delle priorità delle banche e dell'attenzione delle Autorità di Vigilanza. La capacità di proteggere gli asset ICT, prevenire e rilevare le minacce, gestire le vulnerabilità, assicurare continuità e capacità di risposta e rafforzare governance e presidi organizzativi è oggi un elemento essenziale per la solidità e l'affidabilità dell'intermediario.

Banking Resilience 2026 nasce in questo scenario e propone due giornate formative dedicate alle più recenti aspettative della Vigilanza e alle azioni che le banche sono chiamate a intraprendere. La prima giornata è focalizzata sulle richieste pervenute dalla Banca Centrale Europea e sul piano d'azione richiesto entro il 31 ottobre 2026 per rafforzare la cyber resilience rispetto alle minacce abilitate dall'AI; la seconda è dedicata alle richieste della Banca d'Italia e alla Relazione, corredata dal piano di lavoro, da trasmettere entro il 31 dicembre 2026.

Le due giornate condividono una prospettiva comune e permettono di costruire una visione complessiva dell'evoluzione delle aspettative di Vigilanza in materia di sicurezza e resilienza. Gli incontri offrono un aggiornamento fondamentale sui rischi connessi all'AI, inseriti nel più ampio quadro della sicurezza ICT e della resilienza operativa, e fornisce una chiave di lettura utile per valutare i presidi esistenti, individuare le principali aree di intervento e tradurre le aspettative delle Autorità in azioni, priorità e piani di lavoro concreti.

MINACCE CYBER ABILITATE DALL'AI: LA ROADMAP E IL PIANO DI AZIONE

12 ottobre 2026 (10.00/13.00)

La nuova frontiera del cyber risk: cosa cambia con l'AI

- Una lettura integrata delle responsabilità previste dal quadro regolamentare DORA sui singoli Pillar
- L'evoluzione delle minacce cyber abilitate dall'AI e il nuovo threat landscape
- Perché la velocità di identificazione e sfruttamento delle vulnerabilità cambia radicalmente
- Le aspettative della BCE e il piano d'azione richiesto alle banche entro il 31 ottobre 2026
- Il collegamento con cyber resilience, operational resilience e DORA
- Dalla richiesta della Vigilanza alle priorità della banca

I quattro fronti di intervento: dalla vulnerabilità alla risposta

- Attack surface: identificazione e protezione di asset, sistemi e infrastrutture critiche
- Patching: capacità di individuare e correggere rapidamente le vulnerabilità
- Detection & Response: rafforzamento delle capacità di monitoraggio, rilevazione e risposta
- Governance & Resources: responsabilità, competenze, investimenti e strumenti
- Prioritizzazione degli interventi in funzione del profilo di rischio della banca

Dall'assessment alla roadmap: costruire il piano di azione

- Come effettuare il gap assessment rispetto alle aspettative BCE
- Individuazione delle vulnerabilità e delle remediation prioritarie
- Definizione di azioni, responsabilità, milestone e tempi di attuazione
- KPI e indicatori per monitorare il rafforzamento della cyber resilience

Governance e responsabilità: il ruolo del Board e del management

- Accountability degli Organi di amministrazione e Alta Direzione
- Governance del cyber risk e integrazione con ICT Risk Management
- Ruolo di CISO, Risk Management, Compliance, Internal Audit e funzioni IT
- Risorse, competenze e investimenti necessari per sostenere la roadmap
- Terze parti ICT, supply chain e dipendenze critiche

Il piano di azione: le lezioni apprese

- Come strutturare il piano di azione richiesto dalla BCE
- Evidenze, documentazione e audit trail da predisporre
- Coerenza del piano con DORA, framework di ICT risk e cyber strategy
- Monitoraggio dell'avanzamento e gestione delle remediation

RESILIENZA OPERATIVA DIGITALE E AI: LA ROADMAP E IL PIANO DI LAVORO

16 ottobre 2026 (10.00/13.00)

La Comunicazione di Banca d'Italia: aspettative e adempimenti

- Resilienza operativa digitale e nuove minacce abilitate dall'AI
- Il perimetro della Comunicazione e i soggetti interessati
- Il raccordo con DORA e con il quadro di gestione dei rischi ICT
- La Relazione al CdA e il piano di lavoro da trasmettere alla Vigilanza entro il 31 dicembre 2026

I presidi da rafforzare: dalla Governance all'igiene informatica

- Governance: RAF, propensione al rischio, responsabilità, competenze e risorse
- Sicurezza e gestione dei dati e governo dei fornitori ICT
- Igiene informatica: autenticazione, autorizzazione, accessi e segmentazione
- Defence-in-depth e integrazione dei rischi derivanti dalle tecnologie di frontiera
- Utilizzo dell'AI nei presidi di difesa: rischi, monitoraggio e supervisione umana

Asset, vulnerabilità e capacità di detection: i punti di attenzione

- Mappatura della superficie di esposizione e classificazione delle risorse critiche
- Gestione del legacy, cloud e sistemi esposti su Internet
- Vulnerability management, patching e priorità per le vulnerabilità critiche e zero-day
- Monitoraggio, rilevazione e difesa: applicazioni, accessi, traffico e fornitori ICT

Test, risposta agli incidenti e resilienza: verificare che i presidi funzionino

- Test di vulnerabilità, sicurezza delle reti e scenari di attacco
- Test dei processi di risposta, recupero e gestione delle crisi
- Scenari realistici e progressivamente più complessi
- Il ruolo dei fornitori ICT nella resilienza e nella continuità operativa

Dalla gap analysis alla Relazione e al piano di lavoro

- Come valutare esposizione al rischio e adeguatezza dei presidi per ciascuna area
- Individuazione delle carenze e definizione delle priorità
- Definizione delle modalità di monitoraggio dell'avanzamento da parte del CdA