

LE RICHIESTE DELLA VIGILANZA IN TEMA DI SICUREZZA E RESILIENZA DIGITALE

Le indicazioni di BCE e Banca d'Italia sul nuovo
scenario di rischio tra cyber threat, AI e continuità operativa

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.

L'iniziativa 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: DALL'ASSESSMENT AL PIANO D'AZIONE

12 ottobre 2026 (10.00/13.30)

► OPEN SESSION

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

Giuseppe Amato, Servizio Ispettorato di Vigilanza, **Banca d'Italia**

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

- L'evoluzione delle minacce cyber abilitate dall'AI e il nuovo threat landscape
- Perché la velocità di identificazione e sfruttamento delle vulnerabilità cambia radicalmente
- AI agentica in banca: perché sfugge al controllo e come governarla

Romano Stasi, Segretario Generale di **ABI Lab**

Pierguido Iezzi, Cyber Security Director **Zenita Group**

Massimo Messina, Senior Advisor

► Governance e responsabilità: il ruolo del Board e del management

- Accountability degli Organi di amministrazione e Alta Direzione
- Ruolo di CISO, Risk Management, Compliance, Internal Audit e funzioni IT
- Governance & Resources: responsabilità, competenze, investimenti e strumenti
- Definizione delle modalità di monitoraggio dell'avanzamento da parte del CdA
- KPI e indicatori per monitorare il rafforzamento della cyber resilience
- Il ruolo dei fornitori ICT
- Benchmark di mercato

Laura Manganaro, Manager Cyber & Resilience, **PwC Italia**

► Dall'assessment alla roadmap: costruire il piano di azione

- Perimetro critico e come individuarlo
- Definizione di azioni, responsabilità, milestone e tempi di attuazione
- Individuazione delle carenze e definizione delle priorità
- Prioritizzazione degli interventi in funzione del profilo di rischio della banca: come valutare esposizione al rischio e adeguatezza dei presidi per ciascuna area

Laura Manganaro, Manager Cyber & Resilience, **PwC Italia**

Massimo De Nardi, Senior Associate Risk Capital & Reporting, **PwC Italia**

► I presidi di seconda linea da rafforzare: il Ruolo del Risk Management

- Integrazione con RAF, propensione al rischio, responsabilità, competenze e risorse
- Relazione Frontier AI e Riesame dei rischi: punti di contatto e differenze
- Integrazione dello scenario nelle metodologie di analisi del rischio ICT
- Prioritizzazione e criteri per vulnerability e patch management
- Governo dei fornitori ICT

Pasquale Iannelli, Director Risk Capital & Reporting, **PwC Italia**

Massimo De Nardi, Senior Associate Risk Capital & Reporting, **PwC Italia**



RESILIENZA OPERATIVA E SICUREZZA DIGITALE: DAI PRESIDI AI TEST

16 ottobre 2026 (10.00/13.00)

► OPEN SESSION

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

Maria Morbidelli, Servizio Rapporti Istituzionali di Vigilanza, **Banca d'Italia**

► AI Strategy e misure di sicurezza per AI

- Security by design nell'adozione strategia AI
- Protezione delle non-human identities
- Classificazione e protezione dei dati

Marco Rotoloni, co-responsabile Ricerca **ABI Lab**

Maria Cristina Daga, Partner, **Digital360ADV**

Manuela Santini, Associate Partner, **Digital360ADV**

► Challenge e fronti di intervento: dall'identificazione delle vulnerabilità ai test

- Riduzione del perimetro esposto: identificazione e protezione di asset, sistemi, terze parti e infrastrutture critiche e loro modalità di protezione nel breve periodo
- Evoluzione della gestione delle vulnerabilità
- Accelerazione nel Patching: capacità di individuare e correggere rapidamente le vulnerabilità
- Defence -in-Depth: oltre la cyber hygiene
- Difesa aumentata dall'AI: rafforzamento delle capacità di monitoraggio, rilevazione e risposta
- Presidio delle Terze Parti
- Resilienza Operativa e Test

Relatori confermati:

Paolo Carcano, Partner Cyber & Privacy Financial Services Leader, **PwC Italia**

Samantha Trama, Partner Cyber & Privacy Financial Services Leader, **PwC Italia**

► AI Act vs. AI for defence

- Utilizzo dell'AI nei presidi di difesa: rischi, monitoraggio e supervisione umana
- Gli approcci di mercato per l'adozione AI 4 defence
- Esempi di agenti
- I requisiti dell'AI act e come gestirli nel nuovo scenario

Relatori confermati:

Paolo Carcano, Partner Cyber & Privacy Financial Services Leader, **PwC Italia**

Samantha Trama, Partner Cyber & Privacy Financial Services Leader, **PwC Italia**