



ABISERVIZI  **ABI
FORMAZIONE**

SEMINARIO

IL NUOVO QUADRO EBA SUL RISCHIO TERZE PARTI NEI SERVIZI NON-ICT

Impatti organizzativi, gestione degli accordi
e priorità di adeguamento per le banche

10 e 11 dicembre | Aula virtuale

PREMESSA

I nuovi Orientamenti EBA sulla gestione del rischio di terze parti nei servizi non-ICT segnano un'evoluzione del quadro regolamentare: dalla disciplina delle esternalizzazioni a una gestione più ampia e strutturata dei rischi connessi alle dipendenze esterne. **L'obiettivo è promuovere un approccio coerente con DORA, mantenendo distinti i riferimenti applicabili ai servizi ICT e non-ICT e graduando i presidi in funzione della rilevanza degli accordi e delle funzioni supportate.**

Gli Orientamenti rafforzano la responsabilità degli organi aziendali e richiedono una visione del rischio che accompagni l'intero ciclo di vita del rapporto con il fornitore. Particolare attenzione è riservata agli accordi che supportano funzioni critiche o importanti, per i quali assumono maggiore rilievo la valutazione preventiva, i presidi contrattuali, il controllo della subfornitura e la praticabilità delle strategie di uscita.

ABIFormazione dedica un seminario, articolato in due giornate, all'approfondimento del perimetro applicativo e le principali implicazioni organizzative del nuovo quadro, traducendole in criteri e strumenti operativi per le banche. Dalla classificazione degli accordi alla due diligence, dalla governance alla contrattualizzazione, fino al monitoraggio, alla continuità operativa e alle verifiche di vigilanza, il percorso offrirà elementi utili per valutare il modello esistente e definire le priorità di adeguamento, secondo un principio di proporzionalità

PRIMA GIORNATA

DAL NUOVO PERIMETRO REGOLAMENTARE AL MODELLO ORGANIZZATIVO

LA PROSPETTIVA DELLA VIGILANZA

► Finalità e architettura del nuovo quadro sul rischio di terze parti non-ICT: dall'outsourcing al third-party risk management

- Le logiche nell'aggiornamento delle Linee Guida EBA 2019 sull'outsourcing
- Analisi degli esiti della consultazione
- La gestione delle terze parti: il perimetro di applicazione delle nuove EBA Guidelines on Third-Party Riski
- La timeline regolamentare, regime transitorio e piano di adeguamento richiesto alle banche

Questions & Answers

Djamel Bouzemarene, Senior Policy Expert, Prudential Regulation and Supervisory Policy, **EBA - European Banking Authority**

► Il raccordo alla normativa nazionale

- Il punto sul recepimento degli Orientamenti EBA nel quadro normativo nazionale
- La coerenza tra i requisiti DORA e Linee Guida EBA e la relazione rispetto alla Circolare Banca d'Italia 285/201

Questions & Answers

Tommaso Ceparano, Servizio Ispettorato Vigilanza, **Banca d'Italia**

Salvatore Vitiello, Servizio Supervisione Bancaria 2, **Banca d'Italia**

► Dall'esternalizzazione alla gestione complessiva delle dipendenze esterne: responsabilità della banca ed effettività dei presidi

- Responsabilità degli organi aziendali e mantenimento della capacità di governo delle attività
- Rischio di svuotamento organizzativo, o "empty shell"
- Competenze e risorse interne necessarie per controllare i fornitori
- Il processo di outsourcing: best practice operative ed esperienze applicative

► Individuare e classificare gli accordi: perimetro non-ICT

- Distinzione fra accordi con terze parti, outsourcing e subappalto: criteri di inclusione ed esclusione dal perimetro
- Le peculiarità per servizi ricorrenti o continuativi e accordi intragruppo
- Identificazione delle funzioni critiche o importanti
- Servizi misti e confini fra componente ICT e non-ICT

► Governance del rischio terze parti: responsabilità, decisioni e coordinamento

- Strategia e politica di gestione del rischio di terze parti
- Governance e responsabilità degli organi aziendali: le responsabilità non delegabili
- Integrazione nel sistema di gestione dei rischi e raccordo con il RAF
- Processi di approvazione, gestione delle eccezioni ed escalation

► Focus-on: La declinazione della governance per le entità finanziarie meno complesse

► Il processo di valutazione del rischio e la due diligence del fornitore

- Capacità operativa, competenze, solidità economica e sostenibilità della prestazione
- Concentrazione per fornitore, gruppo, servizio e area geografica
- La valutazione del rischio sulla filiera: dipendenze da subfornitori e disponibilità di alternative
- Profondità della due diligence in funzione della rilevanza dell'accordo

SECONDA GIORNATA

DAL CONTRATTO AL MONITORAGGIO E ALLA GESTIONE DELL'USCITA

► **Contrattualizzazione: tradurre la valutazione del rischio in presidi verificabili**

- Revisione dei contratti esistenti e priorità di intervento
- SLA, obblighi di reporting, comunicazione dei cambiamenti rilevanti, diritti di accesso, ispezione e audit
- Graduazione delle clausole in funzione della criticità dell'accordo

► **Subfornitura: comprendere e presidiare la catena delle dipendenze**

- Individuazione dei subfornitori rilevanti per l'erogazione del servizio: effettività dei diritti di controllo
- Gestione dei casi in cui la banca dispone di visibilità limitata sulla catena

► **Contrattualizzazione: tradurre la valutazione del rischio in presidi verificabili**

- Raccordo con il registro DORA: le lezioni apprese
- Opportunità di un'anagrafe integrata e distinzione degli adempimenti regolamentari
- Informazioni utili per reporting, vigilanza e decisioni gestionali: costruzione di una vista utile agli organi aziendali

► **Monitoraggio nel continuo e ruolo delle funzioni di controllo**

- KPI di servizio e KRI di rischio: scelta, soglie e frequenza di rilevazione
- Ripartizione delle verifiche fra responsabili operativi, Risk Management e Compliance
- Attività dell'Internal Audit

► **Continuità operativa e strategie di uscita: verificare la capacità di sostituire il fornitore**

- Collegamento fra servizio esterno e continuità dei processi bancari
- Alternative disponibili, capacità interna e tempi di sostituzione
- Strategie di uscita per gli accordi a supporto di funzioni critiche o importanti

► **Dalla gap analysis al piano di adeguamento**

- Ricognizione degli accordi esistenti e definizione delle priorità
- Interventi su policy, responsabilità, dati, contratti e controlli
- Distinzione fra nuovi affidamenti e rapporti già in essere