Seminario

ICT RISK E SICUREZZA: GLI IMPATTI OPERATIVI DEL 40° AGGIORNAMENTO DELLA CIRCOLARE 285/2013 E DEL QUADRO NORMATIVO EUROPEO IN EVOLUZIONE

1 e 2 febbraio 2023 • Milano, SpazioPola - Aula virtuale

1 febbraio 2023 (10.00 - 16.30)

▸ Saluto di benvenuto ai partecipanti e introduzione ai lavori

Claudia Pasquini, Responsabile Ufficio Analisi, Rischi e Sostenibilità **ABI**

OPEN SESSION

▸ ICT e Sicurezza: un quadro regolamentare in evoluzione

- La gestione del rischio informatico nel sistema bancario e finanziario
- Un quadro d'insieme della regolamentazione a livello europeo e nazionale
- Il Regolamento DORA: principali novità, raccordi con altre normative (PSD2, NIS), stato dei lavori e prospettive

Maria Grazia Miele, Responsabile Divisione Supporto Statistico e informatico della vigilanza **Banca d'Italia**

▸ Dagli Orientamenti EBA sulla gestione dei rischi ICT e di sicurezza al 40° aggiornamento della Circolare n. 285/2013 di Banca d'Italia

▸ I profili di governance e il sistema dei controlli interni

- Le principali novità introdotte
- I ruoli e le responsabilità degli organi aziendali con riferimento ai rischi ICT
- Il sistema dei controlli interni
- La disciplina delle esternalizzazioni ICT
- La timeline di adeguamento

Alessia Paionni, Servizio Regolamentazione e Analisi **Banca d'Italia**

▸ Le nuove norme sulla gestione dei rischi ICT e di sicurezza: profili tecnici

- Definizioni
- La gestione della sicurezza
- La gestione delle operazioni ICT
- La gestione degli incidenti ICT
- La gestione dei progetti e dei cambiamenti ICT

Sebastiano Russo, Divisione Supporto Statistico e informatico della vigilanza **Banca d'Italia**

Questions & Answers

SESSIONE 1

▶ Gli impatti derivati dal 40° aggiornamento della Circolare 285, sfide e prospettive future in ambito Operational Resilience

- Contesto di mercato e regulatory trends
- 40° aggiornamento della Circolare 285
  - Quadro sinottico delle principali novità e loro portata innovativa
  - Il sistema dei controlli interni: focus sugli elementi di novità
  - Il sistema informativo: focus sugli elementi di novità
    - I compiti degli organi aziendali sui profili ICT
    - La funzione di controllo di secondo livello per la gestione e il controllo dei rischi ICT e di sicurezza
    - La gestione della sicurezza dell'informazione, delle operazioni e dei progetti ICT
    - La gestione delle esternalizzazioni e delle terze parti
    - La gestione del rapporto con gli utenti dei servizi di pagamento
  - La continuità operativa: focus sugli elementi di novità

Gianfranco Tessitore, Partner **Deloitte**
Ivan Comunale, Director **Deloitte**

SESSIONE 2

Coordina: **Paolo Carcano**, Partner **Pwc**

▶ CONFRONTO SULLE MODALITÀ DI RECEPIMENTO DELLE PRINCIPALI DISCONTINUITÀ INTRODOTTE

La governance e l'assetto organizzativo dei nuovi controlli ICT: come si stanno orientando le banche

- Le nuove responsabilità dell'organo con funzione strategica e dell'organo con funzione di gestione: gli impatti nella definizione e attuazione della strategia ICT
- La definizione e approvazione della strategia ICT
- La definizione del modello organizzativo per la gestione del rischio ICT e sicurezza
- La nuova funzione di controllo di secondo livello per la gestione e il controllo dei rischi ICT
- L'attribuzione alla funzione Compliance e alla funzione Risk Management dei compiti previsti per la nuova funzione di controllo di secondo livello dei rischi ICT
- Il coordinamento tra le funzioni di controllo di secondo livello
- Il ruolo delle altre funzioni aziendali

Milo Gusmeroli, Chief Operation Officer **Banca Popolare di Sondrio**
Francesco Magri, Chief Information Security Officer **Banca Aidexa**
Francesco Martiniello, Chief Compliance & AFC Officer **illimity**

▶ L'evoluzione della gestione dei rischi di sicurezza e ICT: un framework dinamico e integrato

- Come cambia la nozione di ICT risk alla luce del nuovo quadro regolamentare
- Verso un cambiamento culturale: ICT risk come rischio strategico
- L'analisi del rischio informatico: la correlazione con le altre tipologie di rischio
- Un framework dinamico e integrato per la gestione del rischio di sicurezza ICT
- Analisi degli scenari di rischio di sicurezza ICT per la definizione dei presidi di mitigazione
- Indicatori quantitativi per il rischio ICT (KRI) e il raccordo con l'impianto RAF

Luca Bechelli, Partner **Partner4Innovation**
Giampiero Raschetti, Chief Information Security Officer **Banca Popolare di Sondrio**

2 febbraio 2023 (10.00 - 16.30)

SESSIONE 3

Coordina: **Luca Bechelli**, Partner **Partner4Innovation**

▸ Focus on: la misurazione dell'ICT risk e dei rischi connessi alla continuità operativa

- La definizione di una metodologia dedicata
- È possibile una valutazione oggettiva del rischio? Il ruolo della seconda linea di difesa in ambito IT risk e continuity risk
- I rischi legati alla continuità operativa: come misurare i rischi relativi ai fornitori esterni

Stefano Biondi, Chief Risk Officer **Banca Mediolanum**
Cinzia Cristofoli, Head of ORM, IRM & Fraud **ING Bank**
Ivan Mussida, Information Risk Management Senior Specialist **ING Bank**

▸ La gestione delle operazioni ICT

- Le novità in materia di gestione di incidenti e problemi ICT
- La gestione della continuità operativa: il percorso della resilienza operativa nella logica di servizio
- L'evoluzione dell'ICT Business Continuity
- Soggetti esterni per la prestazione di servizi ICT
- L'attività di monitoraggio, classificazione e segnalazione degli incidenti occorsi
- La definizione del framework dei test di sicurezza e dei test dei sistemi

Romano Stasi, Segretario Generale del Consorzio **ABI Lab**
Stephane Speich, Head of Business Continuity & Resilience Group Governance **Unicredit**

SESSIONE 4

▸ ICT risk ed esternalizzazioni: gli impatti del nuovo quadro regolamentare

- L'esternalizzazione del sistema informativo e il ricorso a soggetti terzi per la prestazione di servizi ICT
- Come cambia la relazione con terze parti e fornitori
- Gli impatti sulla contrattualistica

Gabriele Faggioli, CEO **Digital360**

SESSIONE 5

Coordina: **Paolo Carcano,** Partner **Pwc**

▸ Le prospettive di evoluzione

- Regolamento DORA: da obiettivo di compliance a obiettivo strategico
- Focus-on Regolamento DORA e Direttiva sulla resilienza operativa digitale per il settore finanziario: le linee di continuità con la Circolare 285/2013 e le novità che impatteranno su banche e fornitori
- La Direttiva NIS2 e la Direttiva sulla resilienza dei soggetti critici: focus-on Capo II su strategie e valutazione del rischio
- Focus-on Framework Tiber EU

Alberto Grigoletto, Head of operational & IT risks Generali Group, Chief Risk Officer **GOSP**
Paolo Carcano, Partner **Pwc**
Samantha Trama, Partner **PwC**
Edoardo Montrasi, Manager CryptonetLabs **Gruppo Digital360**

▸ I nuovi obblighi formativi previsti dal nuovo quadro regolamentare: tra cultura del rischio ICT e nuove skill necessarie

- La rilevanza del fattore umano nella gestione della sicurezza
- I presidi da attivare
- Le competenze da sviluppare: la nuova offerta formativa

Maria Cristina Daga, Partner **Partner4Innovation**
Barbara Filippella, Responsabile Settore Sviluppo competenze **ABIFormazione**