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

▸ Saluto di benvenuto ai partecipanti e introduzione ai lavori

OPEN SESSION

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

- Gli obiettivi perseguiti dagli Orientamenti EBA sui rischi ICT e di sicurezza
- Il recepimento nella Circolare n. 285/2013 di Banca d'Italia: le modifiche ai Capitoli 4 e 5
- Focus sulle principali novità introdotte: i ruoli e le responsabilità degli organi aziendali, la funzione di controllo dei rischi ICT, gestione dei rischi, gestione delle esternalizzazioni, misure di sicurezza, gestione degli incidenti, formazione
- La timeline di adeguamento

▸ ICT e Sicurezza: un quadro regolamentare in evoluzione

- La gestione del rischio informatico in banca: un quadro d'insieme della regolamentazione a livello europeo
- Una visione organica delle normative di prossima emanazione tra punti di contatto e discontinuità
- Il Regolamento DORA: timeline implementativa e principali impatti
- La nuova Direttiva NIS2: perimetro di applicazione e gli obblighi in materia di cyber sicurezza

▸ Information Asset

- Perimetro di intervento e aspetti definitori
- Policy di gestione dei progetti ICT
- Repository incident
- Prospettive evolutive

Questions & Answers

SESSIONE 1

▸ Tavola rotonda - 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
- Il presidio in capo alla funzione Compliance e alla funzione Risk Management
- Il coordinamento tra le funzioni di controllo di secondo livello
- Il ruolo delle altre funzioni aziendali

- **Gli impatti operativi derivati dal 40° aggiornamento della Circolare 285 : disamina dei processi aziendali impattati dalle novità**
  - Governance e strategia
  - Gestione del rischio ICT e sicurezza
  - Gestione e reporting degli incidenti
  - Policy, procedure, operation
  - Organizzazione
  - Risorse umane e awareness
  - La gestione delle esternalizzazioni e dei servizi ICT delle terze parti: aspetti di governance e adeguamento dei contratti
  - La continuità operativa

SESSIONE 2

- **La nuova frontiera del rischio ICT e Sicurezza: 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
  - Il rischio ICT all'interno del RAF

- **La definizione di un nuovo framework per la gestione del rischio ICT e Sicurezza**
  - Come costruire una metodologia di calcolo del rischio ICT
  - La gestione del rischio by design
  - La definizione delle misure e dei controlli per l'attenuazione dei rischi ICT e di sicurezza
  - L'attività di monitoraggio, classificazione e segnalazione degli incidenti occorsi
  - La definizione del framework dei test di sicurezza e dei test dei sistemi

2 febbraio 2023

SESSIONE 3

▶ Tavola rotonda - La gestione della Sicurezza dell'informazione

- La differenza tra sicurezza informatica e sicurezza delle informazioni
- Le novità in relative alla definizione della policy di sicurezza dell'informazione
- Le nuove procedure per assicurare la gestione della sicurezza logica
- L'impatto dell'estensione all'ambito della sicurezza fisica
- Analisi, valutazione e verifica della sicurezza dell'informazione
- La sicurezza dei componenti hardware e dell'IoT

▶ La gestione delle operazioni ICT

- Le novità in materia di gestione di incidenti e problemi ICT

▶ La gestione dei progetti e dei cambiamenti ICT

- Acquisizione sviluppo dei sistemi ICT e la gestione dei cambiamenti

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 i fornitori
- Gli impatti sulla contrattualistica

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

- La rilevanza del fattore umano nella gestione della sicurezza
- Le competenze da sviluppare
- I presidi da attivare

SESSIONE 5

▶ Le prospettive di evoluzione

- Focus-on Regolamento Digital Operational Resilience ACT
- Focus-on Framework Tiber EU