

Percorso ICT Compliance: dalla Circolare 285 alle norme sulla sicurezza dei pagamenti agli Standard ISO di Sicurezza informatica

6-7 OTTOBRE - 20-21 OTTOBRE • Aula virtuale



PRIMA GIORNATA • 6 OTTOBRE 2021

➤ Il ruolo della compliance ICT

- Il perimetro normativo di riferimento per l'azione della compliance ICT
- I possibili modelli organizzativi e metodologici in banca
- Benchmark di modelli di compliance ICT presenti nelle banche italiane
- Le normative rilevanti di prossima emanazione con impatto sulla *digital transformation*

➤ Evoluzione del ruolo della compliance ICT

- *Compliance by design* e *compliance advisory*: gli approcci nell'ambito ICT
- *Digital compliance* e *continuous compliance*: identificare i Key Risk Indicator dell'ambito ICT
- L'efficacia del sistema di controlli a distanza su specifici ambiti ICT
- I flussi e le relazioni tra la Compliance ICT e le altre Funzioni Aziendali di Controllo

SECONDA GIORNATA • 7 OTTOBRE 2021

➤ Aspetti introduttivi all'ambito ICT: il Sistema Informativo bancario

- Concetti preliminari e funzioni di un Sistema Informativo
- Le architetture IT *on premise* e *on cloud*: aspetti chiave di compliance ICT
- Tendenze in corso e particolari aspetti tecnologici di impatto per la compliance
- Cenni su infrastrutture tecnologiche e sistemi hardware

➤ Aspetti introduttivi all'ambito ICT: la cyber-security

- Nozioni chiave e principali definizioni di cyber-security
- Punti di attenzione per la compliance: come le vulnerabilità di sicurezza impattano la compliance ICT
- Le possibili modalità di verifica: analisi documentale, *reliance*, testing

ICT Compliance: dalla Circolare 285 alle norme sulla sicurezza dei pagamenti agli Standard ISO di Sicurezza informatica

6-7 OTTOBRE - 20-21 OTTOBRE • Aula virtuale



TERZA GIORNATA • 20 OTTOBRE 2021

➤ La compliance ICT nei servizi di pagamento

- La sicurezza dei pagamenti e le normative di riferimento, nazionali e comunitarie
- Modalità di conduzione delle verifiche di compliance sulla sicurezza dei pagamenti
- *Open banking* e gli impatti delle *open API*: fin dove spingersi
- Le evoluzioni previste e gli impatti della nuova normativa ISO20022

➤ Cloud compliance

- Introduzione al *cloud computing*: modelli di cloud e specificità di ciascuno
- Overview sul mercato bancario in ambito cloud e tipologie di esternalizzazioni
- Il framework dei rischi di compliance in ambito cloud
- *Use case* di progetti di cloud outsourcing: il ruolo della compliance e il confronto con Banca d'Italia

QUARTA GIORNATA • 21 OTTOBRE 2021

➤ I principali standard e best practice di compliance ICT

- I framework di IT management: ITIL e COBIT
- L'impostazione delle verifiche per i processi ICT
- Gli standard ISO che impattano i principali processi ICT: ISO27001, ISO22313, ISO IEC 27031

➤ Use case

- Le verifiche in caso di cloud outsourcing
- Come impattano la compliance i report ISAE3402, SOC1 e SOC2
- Quali rischi chiave e quali tutele da un punto di vista di compliance ICT