PERCORSO OPERATIONAL RISK EXPERT: MODELLI AVANZATI E GESTIONE DEI RISCHI EMERGENTI IN BANCA



MODULO 1 - Evoluzione dell'Operational Risk: modelli avanzati e integrazione dei novel risk • **30 novembre e 1 dicembre 2026**

MODULO 2 - Operational Risk in pratica: applicazione dei modelli e benchmark di sistema • **14 e 15 dicembre 2026**

Aula virtuale

PIANIFICAZIONE

MODULO 1
Evoluzione dell'Operational Risk: modelli avanzati e integrazione dei novel risk
30 novembre e 1 dicembre

MODULO 2
Operational Risk in pratica: applicazione dei modelli e benchmark di sistema
14 e 15 dicembre

4 mezze giornate – 10:00-13:00

DESCRIZIONE

Il percorso fornisce una visione evoluta e operativa della gestione del rischio operativo, integrando modelli tradizionali e novel risk. Unisce inquadramento metodologico ed esercitazioni pratiche con focus su applicazioni concrete e integrazione nei processi. Il confronto permette di approfondire casi reali, criticità e soluzioni adottate. Un'iniziativa pensata per rafforzare competenze tecniche e capacità operative nella gestione integrata dei rischi.

OBIETTIVI

- Evolvere il framework di Operational Risk verso un approccio integrato con l'Operational Resilience e coerente con il quadro regolamentare e prudenziale
- Applicare metodologie e strumenti di assessment e misurazione, valorizzando loss data, RCSA, KRI e Scenario Analysis
- Integrare novel ed emerging risk nel framework di Operational Risk, considerando le interconnessioni con i rischi ICT, cyber, DORA e AI
- Rafforzare il monitoraggio e la gestione del rischio operativo, attraverso metriche, benchmark di sistema e l'utilizzo dei risultati del risk assessment nei processi decisionali

Copyright © ABISERVIZI SpA. Tutti i diritti riservati. È proibita la riproduzione, anche parziale, in qualsiasi forma senza espresso permesso scritto di ABISERVIZI SpA. - Divisione ABIFormazione. Il ricevente è tenuto ad utilizzare il documento esclusivamente per esigenze di documentazione personale nell'ambito delle proprie esigenze lavorative; non può in alcun modo ridistribuire o comunicare a terzi le informazioni in esso presenti.

PROGRAMMA

MODULO 1 – EVOLUZIONE DELL'OPERATIONAL RISK: MODELLI AVANZATI E INTEGRAZIONE DEI NOVEL RISK

Giorno 1: Dall'Operational Risk Management all'Operational Resilience

- Evoluzione del quadro regolamentare e prudenziale: implicazioni per i framework di gestione del rischio operativo
- L'evoluzione dell'Operational Risk Management: approcci tradizionali, nuovi paradigmi e principali sfide per le banche
- L'Operational Risk Management Framework (ORMF): componenti, responsabilità, processi di identificazione, valutazione, controllo e reporting
- Dall'Operational Risk all'Operational Resilience:
  - Gestione della continuità operativa
  - Focus on - Rischio ICT e la capacità di prevenire, fronteggiare e recuperare eventi avversi
- Integrazione tra framework di Operational Risk e presidi di resilienza operativa: punti di contatto, responsabilità e aree di attenzione

Giorno 2: Modelli di gestione dell'Operational Risk e integrazione dei Novel Risk

- Il modello di Operational Risk Assessment:
  - Criteri di identificazione dei rischi
  - Processi valutativi ed efficacia dei controlli
- Loss Data e Operational Risk Measurement:
  - Raccolta e classificazione delle perdite
  - Analisi delle cause e utilizzo dei dati a supporto della valutazione del rischio
- Key Risk Indicators (KRI):
  - Definizione delle metriche
  - Individuazione delle soglie di attenzione e utilizzo degli indicatori per il monitoraggio e l'escalation
- Novel ed emerging risk:
  - Identificazione dei nuovi fattori di rischio
  - Valutazione degli impatti potenziali e integrazione nei processi e nelle metodologie esistenti
- Interconnessioni tra rischi tradizionali ed emergenti

Copyright © ABISERVIZI SpA. Tutti i diritti riservati. È proibita la riproduzione, anche parziale, in qualsiasi forma senza espresso permesso scritto di ABISERVIZI SpA. - Divisione ABIFormazione. Il ricevente è tenuto ad utilizzare il documento esclusivamente per esigenze di documentazione personale nell'ambito delle proprie esigenze lavorative; non può in alcun modo ridistribuire o comunicare a terzi le informazioni in esso presenti.

MODULO 2 - OPERATIONAL RISK IN PRATICA: APPLICAZIONE DEI MODELLI E BENCHMARK DI SISTEMA

Giorno 1: Applicazione dei modelli di Operational Risk

- Il Risk Control Self Assessment in pratica: perimetro di analisi, identificazione degli scenari di rischio, valutazione dei controlli e determinazione del rischio residuo
- L'identificazione e la misurazione dei KRI: selezione degli indicatori, definizione delle soglie e interpretazione degli scostamenti
- L'utilizzo della Scenario Analysis:
  - Costruzione degli scenari rilevanti
  - Valutazione degli impatti potenziali e utilizzo delle analisi per integrare le informazioni storiche
- Metriche e strumenti di monitoraggio

Esercitazione applicativa: analisi di un caso di rischio operativo con individuazione delle priorità di intervento.

Giorno 2: Integrated Operational Risk Assessment

- Pratiche di sistema per il monitoraggio dei novel risk: approcci metodologici, indicatori e principali criticit applicative
- DORA e rischio ICT: integrazione dei rischi connessi alla resilienza operativa digitale nel framework di Operational Risk
- Cyber risk e AI risk:
  - Identificazione delle esposizioni
  - Valutazione degli impatti e raccordo con i processi di risk assessment e controllo
- Integrated Operational Risk Assessment: lettura trasversale delle diverse componenti di rischio, analisi delle interdipendenze e definizione di una vista integrata
- Dal Risk Assessment alla gestione manageriale:
  - Prioritizzazione dei rischi
  - Definizione delle azioni di mitigazione
  - Reporting e supporto alle decisioni

Copyright © ABISERVIZI SpA. Tutti i diritti riservati. È proibita la riproduzione, anche parziale, in qualsiasi forma senza espresso permesso scritto di ABISERVIZI SpA. - Divisione ABIFormazione. Il ricevente è tenuto ad utilizzare il documento esclusivamente per esigenze di documentazione personale nell'ambito delle proprie esigenze lavorative; non può in alcun modo ridistribuire o comunicare a terzi le informazioni in esso presenti.