ABISERVIZI ABI FORMAZIONE

ICT RISK & SICUREZZA

Percorso professionalizzante

DIVENTA ICT & SECURITY EXPERT IN BANCA

Moduli propedeutici al percorso professionalizzante

I FONDAMENTI DEL SISTEMA DEI CONTROLLI INTERNI E DEL SISTEMA INFORMATIVO

PROGRAMMI

Aula virtuale

SCHEMA DELL'OFFERTA FORMATIVA

1 PERCORSO PROFESSIONALIZZANTE
DIVENTA ICT & SECURITY EXPERT IN BANCA

Destinatari

- nuova funzione ICT Risk e Sicurezza (percorso intero)
- funzione Risk Management (moduli 1a, 1b e 1d)
- funzione Compliance (moduli 1a, 1c e 1d)

MODULO 1a
PROFILING DELL'ICT RISK E SECURITY EXPERT: EVOLUZIONE REGOLAMENTARE, ASSETTI E RUOLI ORGANIZZATIVI, COMPETENZE RICHIESTE
30 settembre e 1 ottobre 2024

MODULO 1b
ICT RISK MANAGEMENT - LA GESTIONE DELLA SICUREZZA DELL'INFORMAZIONE, DELLE OPERAZIONI ICT, DEI PROGETTI E DEI CAMBIAMENTI ICT, DEI FORNITORI E TERZE PARTI
17 e 18 ottobre 2024

MODULO 1c
COMPLIANCE MANAGEMENT PER IL RISCHIO ICT E SICUREZZA
5 e 6 novembre 2024

MODULO 1d
CYBER RISK MANAGEMENT - METODI E STRUMENTI PER LA PREVENZIONE E GESTIONE
14 e 15 novembre 2024

TEST 4 dicembre 2024

2 MODULI PROPEDEUTICI AL PERCORSO PROFESSIONALIZZANTE
I FONDAMENTI DEL SISTEMA DEI CONTROLLI INTERNI E DEL SISTEMA INFORMATIVO

Destinatari

- Funzioni di controllo di II livello che non hanno esperienza relativa al sistema informativo (modulo 2a)
- funzione IT (I livello) che deve relazionarsi con le funzioni di II livello (modulo 2b)

MODULO 2a
ICT RISK E SICUREZZA: I FONDAMENTI PER ORIENTARSI NEL SISTEMA INFORMATIVO DELLA BANCA
17 e 18 settembre 2024

MODULO 2b
ICT RISK E SICUREZZA: I FONDAMENTI PER ORIENTARSI NEL SISTEMA DEI CONTROLLI INTERNI
19 settembre 2024

1 PERCORSO PROFESSIONALIZZANTE
DIVENTA ICT & SECURITY EXPERT IN BANCA

MODULO 1a · PROFILING DELL'ICT RISK E SECURITY EXPERT: EVOLUZIONE REGOLAMENTARE, ASSETTI E RUOLI ORGANIZZATIVI, COMPETENZE RICHIESTE

30 settembre e 1 ottobre 2024

- **Il nuovo scenario tecnologico e digitale: la gestione della sicurezza**
  - Sistema ICT ed evoluzione tecnologica e digitale nel contesto bancario e finanziario
  - Conoscere le minacce e le vulnerabilità che possono influenzare i sistemi informativi aziendali
  - I rischi collegati all'ICT e il cyber risk: le problematiche legate all'identificazione e alla gestione
  - I termini chiave relativi alla sicurezza informatica e alla gestione del rischio ICT
  - L'importanza della sicurezza ICT nel settore bancario a livello sistemico
- **Sistema informativo in banca: organizzazione e processi di gestione**
  - Il modello organizzativo della funzione ICT: soluzioni operative a confronto
  - La fornitura di servizi ICT: la nozione di service management e ICT service management
  - Gli stakeholders dell'ICT service management
- **L'attenzione alla gestione del rischio informatico in banca: l'evoluzione regolamentare**
  - La gestione del rischio informatico nel sistema bancario e finanziario
  - Un quadro d'insieme della regolamentazione a livello europeo e nazionale
  - Il 40° aggiornamento della Circolare n. 285/2013 di Banca d'Italia
  - Il Regolamento DORA: principali novità, raccordi con altre normative stato pubblicazione degli RTS/ITS e prospettive
  - Il Regolamento DORA vs Circolare n. 285/2013 di Banca d'Italia: gap analysis dei requisiti normativi
- **Focus-on: I building blocks del DORA alla luce degli RTS/ITS emanati e in via di pubblicazione**
  - ICT risk management: come evolve il framework di ICT governance e risk management
  - ICT major incident reporting: la gestione degli eventi critici tra classificazione, segnalazione, armonizzazione dei template
  - Digital operation resilence testing: le novità e la relazione con Tiber EU
  - Third Party Risk Management & Agreements: come evolve la gestione del rischio terze parti e la sorveglianza provider critici
- **Profiling delle responsabilità in banca in tema di gestione del rischio ICT e sicurezza**
  - I profili di governance: i ruoli e le responsabilità degli organi aziendali con riferimento ai rischi ICT
  - Le nuove responsabilità l'Organo con funzione di supervisione strategica
  - Il sistema dei controlli interni: tra definizione della nuova funzione e assegnazione delle responsabilità alla funzione risk management e compliance
  - Le peculiarità della funzione di controllo di secondo livello per la gestione e il controllo dei rischi ICT e di sicurezza
- **La definizione della nuova struttura organizzativa a presidio del rischio ICT e sicurezza**
- La struttura organizzativa: il benchmark di mercato con analisi di punti di forza e di debolezza
- Le dinamiche tra primo, secondo e terzo livello di controllo
- La relazione con il CISO e la funzione ICT della banca
- Le peculiarità in caso di intermediari con componente/servizi ICT fortemente esternalizzati
- Ridisegnare i flussi operativi e informativi
- Il ruolo della funzione organizzazione

Testimonianza bancaria

▶ Identificazione e classificazione dei rischi 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
- Il processo di identificazione e classificazione dei rischi ICT
- L'analisi del rischio informatico: la correlazione con le altre tipologie di rischio
- Il framework di gestine del rischio ICT alla luce del DORA

Esercitazione e casi pratici

▶ Le evoluzioni dei modelli di valutazione e gestione dei rischi ICT e di sicurezza

- Il potenziale impatto dei rischi ICT sull'operatività e sulla reputazione della banca
- Le valutazioni del rischio per identificare vulnerabilità e punti deboli nell'infrastruttura ICT della banca
- Le strategie per stabilire le priorità e gestire i rischi in base al loro potenziale impatto e alla probabilità che si verifichino
- La relazione tra rischio ICT e sicurezza e la propensione al rischio della banca: Indicatori quantitativi per il rischio ICT e il raccordo con l'impianto RAF
- Verso la definizione di un framework dinamico e integrato per la gestione del rischio di sicurezza ICT

Testimonianza bancaria

▶ 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

MODULO 1b · ICT RISK MANAGEMENT - LA GESTIONE DELLA SICUREZZA DELL'INFORMAZIONE, DELLE OPERAZIONI ICT, DEI PROGETTI E DEI CAMBIAMENTI ICT, DEI FORNITORI E TERZE PARTI

17 e 18 ottobre 2024

Le modalità operative per la gestione della sicurezza dell'informazione

- La relazione 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, fisica e delle operazioni ICT
- 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

I presidi da attuare per garantire la gestione della continuità operativa

- Le novità in materia di gestione di incidenti e problemi ICT
- La Business Impact Analysis-BIA: gli indicatori da prendere in considerazione e i ruoli coinvolti
- La definizione del piano di continuità operativa, dei piani di risposta e ripristino
- L'attività di monitoraggio, classificazione e segnalazione degli incidenti occorsi
- La definizione del framework dei test di sicurezza e dei test dei sistemi

L'evoluzione dell'Incident Management

- RTS sui criteri per la classificazione degli incidenti ICT-related e soglie di materialità
- Aggiornamento delle modalità dei template di Reporting degli incidenti ICT-related
- Stima delle perdite lorde a seguito degli incidenti ICT-related: il nuovo processo e l'approccio metodologico derivante dall'esercizio dei Cyber Stress Test BCE
- L'importanza del dialogo tra business e linee di difesa in tutte le fasi del processo di classificazione, reporting e valutazione degli impatti degli Incidenti ICT-related
- Come descrivere e comunicare efficacemente le lessons learnt ad Autorità e CdA: una guida pratica
- Meccanismi di condivisione dei dati sulle minacce informatiche secondo il Regolamento DORA

L'attività di testing nel framework di resilienza digitale operativa

- I test avanzati di strumenti, sistemi e processi ICT basati su test di penetrazione guidati dalla minaccia (TLPT): la relazione con Tiber EU/IT
- La relazione banca/fornitori nella gestione dei test
- Approccio multidisciplinare e integrato per la conduzione sicura e controllata dei test: un caso di applicazione pratica
- Minacce evolute e scenari di attacco convergenti

Esercitazione e casi pratici

La gestione delle operazioni ICT

- Prassi implementative relative alla gestione dei progetti ICT, l'acquisizione e sviluppo di sistemi ICT
- Le peculiarità operative nella gestione dei cambiamenti ICT: i presidi da attuare

Testimonianza bancaria

- **ICT Risk ed esternalizzazioni: gli impatti del nuovo quadro regolamentare**
  - L'esternalizzazione del sistema informativo e il ricorso a fornitori terzi per la prestazione di servizi ICT
  - Le novità relative alle relazione con i fornitori terzi: i nuovi obblighi per gli organi aziendali: gli impatti sulla contrattualistica
  - Focus-on: la Business Impact Analysis-BIA verso i fornitori terzi
  - La definizione di un framework integratodel rischio terze parti: la mappa delle interdipendenze

- **Le disposizioni DORA per la gestione delle Terze Parti ICT: gli impatti operativi**
  - Impact analysis sugli RTS circa le policy delle entità finanziarie sull'utilizzo di servizi ICT forniti da Terzi a supporto di funzioni essenziali o importanti: valutazione (due diligence e risk assessment), ingaggio, monitoraggio e fuoriuscita
  - Impact Analysis sugli ITS sui modelli che compongono il registro delle informazioni in relazione a tutti gli accordi contrattuali sull'uso dei servizi ICT forniti da terzi
  - I nuovi obblighi per gli organi aziendali e gli impatti sulla contrattualistica
  - Come cambia il modello di governo della catena di fornitura e subfornitura: prime indicazioni dal secondo slot di RTS in consultazione
  - Impatti per gli enti finanziari e per i fornitori di servizi ICT critici

- **La gestione dei sistemi informativi in cloud**
  - Il Cloud computing sotto il profilo contrattuale e normativo nazionale ed europeo
  - Cloud: profili legali e contrattuali
  - I vantaggi del cloud computing e i rischi legati al trattamento dei dati
  - Il Cloud computing e la protezione dei dati personali
  - Le criticità legate alla gestione dei contratti

Testimonianza bancaria

MODULO 1c · COMPLIANCE MANAGEMENT PER IL RISCHIO ICT E SICUREZZA
5 e 6 novembre 2024

ICT Risk, Cyber Security ed evoluzione digitale del settore bancario: un framework in costante evoluzione

- Il panorama normativo nazionale ed europeo: le sovrapposizioni, le peculiarità, le opportunità di integrazione dei diversi requisiti
- Oltre la Circolare 285/2013 di Banca d'Italia: la Digital Finance Strategy tra regolamentazione e strategie del settore bancario e finanziario
- I nuovi regolamenti del Digital Finance Strategy
- Regolamento DORA e relazione con la Direttiva NIS
- Il framework Tiber EU
- L'Artificial Intelligence Act europeo: i vincoli posti dal regolatore
- Data Governance Act, Digital Market Act, Digital Service Act, Data Act,: una vista integrata del framework normativo in via di definizione, la timeline implementativa e i principali impatti

Costruire il modello di compliance ICT a partire dalla definizione del perimetro normativo

- L'approccio per l'identificazione del perimetro normativo di riferimento
- L'identificazione dei rischi di conformità relativi ai servizi ICT
- Aspetti definitori: punti di contatto e differenze tra rischio di conformità e rischio informatico
- Il processo di identificazione dei rischi di conformità relativi ai servizi ICT: l'approccio risk-based
- Gli ambiti organizzativo/funzionali interessati: identificazione dei risk e process owner

Esercitazione e casi pratici

L'analisi del rischio di conformità relativo ai servizi ICT

- Il processo di classificazione delle risorse ICT e Sicurezza in termini di rischio di conformità dei servizi IT
- L'analisi delle misure di mitigazione: conformità a normative esterne e a regolamenti e policy
- Il processo di valutazione dei rischi
- La costruzione di un repository dei controlli
- La relazione con le valutazioni dei rischi operativi e i database delle perdite

La Cyber Security all'interno delle principali normative di rilievo (PSD2, GDPR, …)

- Requisiti EBA sull'IT Risk di compliance all'interno dello SREP
- L'esecuzione della DPIA: approcci e logiche di calcolo del Rischio IT
- Data Breach: l'importanza di prevenire gli eventi e gli impatti sulla Brand Reputation
- Nuovi scenari di rischio derivanti dall'applicazione della PSD2
- I nuovi scenari di rischio derivanti dall'introduzione delle terze parti
- I principali impatti collegati ai servizi innovativi e all'utilizzo di nuove tecnologie (API)

Il ruolo della funzione compliance in relazione alle esternalizzazioni e fornitori terzi

- I punti di attenzione sulla contrattualistica

Testimonianza bancaria

MODULO 1d · CYBER RISK MANAGEMENT - METODI E STRUMENTI PER LA PREVENZIONE E GESTIONE

14 e 15 novembre 2024

Il trend degli incidenti e delle perdite relative al Cyber Risk

- Gli scenari di attacco cyber nell'attuale scenario di crisi geo-politica
- Analisi dei principali attacchi al settore bancario: il cyber crime, dark web, hacker profiling
- Analisi di scenario delle frodi identitarie: i canali internet, mobile
- Il prezzo della cyber (in)security
- Gli impatti del cyber crime: proteggere la Business Continuity, il patrimonio informativo e la reputazione

I rischi derivanti dall'interno

- I rischi interni diretti: le frodi interne
- I rischi interni indiretti: il social engineering
- Le strategie per gestire il fattore umano: la cultura del rischio per prevenire le azioni volontarie e involontarie

Cyber Security e governo del rischio informatico

- Contesto di riferimento delle minacce Cyber: focus su Ransomware & CEO Fraud
- Cyber Risk management & Cyber Resilience
- Cyber Reporting & CEO Dashboard
- Formazione e competenze Cyber

Il controllo e il monitoraggio del Cyber Risk

- La definizione del Risk Appetite Framework per il rischio informatico e cyber risk
- Gli strumenti per il monitoraggio del cyber risk: la definizione degli indicatori di rischio e le analisi di trend e di coerenza
- La definizione di processi di Security Strategy e Security Governance
- Le tecnologie e gli strumenti a supporto del cyber risk management
- Cyber Risk Measurement: come prioritizzare i rischi cyber
- L'implementazione di modelli operativi e organizzativi per la gestione della Business Continuity

Esercitazione e casi pratici

La gestione degli eventi di crisi

- Dalla Business Continuity alla gestione nelle crisi: i processi di gestione nell'ordinario e in stato di emergenza
- L'evoluzione dei processi di gestione emergenze: le funzioni segnalanti e la classificazione degli eventi
- La definizione del piano di Disaster Recovery
- Definizione di soluzioni tecnico-funzionali per implementare un sistema avanzato di Information Security
- La gestione degli eventi di crisi e la definizione del piano di comunicazione

Strumenti di gestione dei rischi cyber e applicazione della Cyber Threat intelligence

- Valutazione periodica dell'esposizione al rischio cyber
- Utilizzo di soluzioni Analytics e Threat intelligence per migliorare analisi dei rischi

La gestione degli impatti operativi derivanti dal framework TIBER-EU

- Dai security Test ai Red teaming: quali impatti nei differenti approcci
- Come evolve la Threat Intelligence

- **Digital Cyber Culture & awareness**
  - Digital cyber culture – why relevant?
  - Main market solution to enhance digital cyber culture & awareness
  - Digital approach to spread out Cyber Culture & Awareness
- **Focus on: monitoraggio e gestione della Brand Reputation**
- **L'uso dei Big Data nella Fraud Detection**

Esercitazione: scenari di incidenti informatici simulati

Testimonianza bancaria

MODULI PROPEDEUTICI AL PERCORSO PROFESSIONALIZZANTE

2 I FONDAMENTI DEL SISTEMA DEI CONTROLLI INTERNI E DEL SISTEMA INFORMATIVO

MODULO 2a · ICT RISK E SICUREZZA: I FONDAMENTI PER ORIENTARSI NEL SISTEMA INFORMATIVO NELLA BANCA

17 e 18 settembre 2024

- **Il sistema informativo negli intermediari finanziari**
  - Introduzione ai sistemi informativi: le evoluzioni nel tempo
  - Le peculiarità dei sistemi informativi del settore bancario
- **La classificazione del sistema informativo in banca**
  - I sistemi informativi interni ed esterni
  - I sistemi informativi direzionali ed operativi
  - La suddivisione per aree funzionali della banca e la vista per processi
- **I principali mezzi tecnici caratterizzanti i sistemi informativi**
  - Le caratteristiche peculiari delle architetture hardware e software
  - Le reti e i processi di knowledge management
  - Dati a Database aziendali: architetture dei database e i modelli logici
  - I datawarehouse e i flussi informativi
- **La funzione sistemi informativi in banca**
  - La funzione Sistemi Informativi come centro di fornitura di servizi agli utenti: I principali compiti e responsabilità
  - Il posizionamento della funzione Sistemi Informativi in banca
- **L'outsourcing dei sistemi informativi bancari**
  - Le motivazioni alla base delle esternalizzazioni dei sistemi informativi: le scelte strategiche e di efficientamento
  - Le modalità operative di gestione delle attività in outsourcing e i punti di controllo
- **Le sfide per l'ICT in banca**
- La business continuity e la continuità operativa
- Il processo di evoluzione tecnologico e digitale
- **L'evoluzione tecnologica e digitale del settore bancario**
  - Il punto sull'evoluzione digitale del settore bancario: dalla fase sperimentale alla messa a sistema
  - Digital Transformation: a che punto siamo
- **Le principali tecnologie evolutive nel settore bancario**
  - Il Machine learning e Intelligenza artificiale
    - Gli utilizzi dell'AI e machine learning in banca: i principali ambiti di applicazione e le prospettive di evoluzione
    - IA artificiale generativa: le opportunità per il settore e i rischi da gestire
  - Cloud
    - Le possibilità offerta dal cloud con l'attenzione alla gestione dei rischi collegati
    - La tendenza a interpretare il Cloud come driver strategico
  - Distribuited ledger tecnologies, Blockchain e Cryptovalute
    - La tecnologia alla base della blockchain e le principali applicazioni
    - L'evoluzione delle cryptocurrencies e i punti di attenzione per la banca

MODULO 2b · ICT RISK E SICUREZZA: I FONDAMENTI PER ORIENTARSI NEL SISTEMA DEI CONTROLLI INTERNI

19 settembre 2024

- **I fattori di rischio della banca**
  - I fattori di rischio rilevanti della banca
  - Il framework normativo di Vigilanza Prudenziale che regola i rischi in banca
  - Le principali tipologie di rischio in banca: le specificità e i punti di connessione
- **L'architettura complessiva del sistema dei controlli interni**
  - Il quadro normativo di riferimento: dalla Circolare 285/2013 di Banca d'Italia agli Orientamenti EBA sulla governance interna
  - Completezza, adeguatezza, funzionalità e affidabilità del sistema dei controlli interni
  - L'architettura dei controlli in banca: il primo, secondo e terzo livello
  - La corretta interazione e il coordinamento fra le funzioni aziendali di controllo: mission, ruolo e attività delle funzioni compliance, risk management, ICT e Sicurezza, Internal audit
  - I principali flussi informativi delle funzioni di controllo verso gli organi aziendali
- **Il processo di Risk Management in banca: individuazione, valutazione, monitoraggio, controllo e metodi di attenuazione dei rischi**
  - Identificazione, classificazione e processo di gestione dei rischio in banca
  - Le interrelazioni tra i rischi e il processo di integrazione del sistema dei controlli interni
  - Il Risk Appetite Framework: inquadramento generale e processo di definizione
  - La valutazione del RAF e il sistema dei controlli interni
- **Focus-on: le peculiarità di gestione di alcune categorie di rischio**
  - Il rischio di compliance
  - Il rischio operativo
  - Il rischio informatico