ABISERVIZI ABI FORMAZIONE

ICT RISK E SICUREZZA

La proposta formativa 2023 di ABIFormazione

Le banche devono far fronte a crescenti obblighi di conformità associati a leggi, regolamenti e standard relativi alla sicurezza informatica. In particolare, il 40° aggiornamento della Circolare 285/2013 di Banca d'Italia e l'approvazione del Regolamento DORA hanno introdotto rilevanti novità che riguardano la **gestione**, la **governance** e i **compiti** degli organi aziendali, il **sistema dei controlli interni**, l'**outsourcing** e la **continuità operativa**.

Le novità introdotte dal nuovo quadro regolamentare richiedono di affrontare cambiamenti organizzativi, procedurali e metodologici con impatti rilevanti e con un calendario serrato di adempimenti da realizzare e azioni immediate e nel medio-lungo periodo.

Processi, **tecnologie** e **persone** sono i tre fattori che vengono presi in considerazione dalla Regolamentazione per mitigare il rischio di perdita cagionato non solo da una non adeguatezza dei sistemi o delle tecnologie o dei processi ma anche da comportamenti non consapevoli o da mancanza di conoscenza e competenza.

In tal senso, il Regolatore ha individuato nella **formazione uno strumento ineliminabile** per promuovere la più ampia diffusione della cultura della sicurezza, la consapevolezza dei comportamenti, le conoscenze e competenze necessarie, il coinvolgimento e l'impegno di tutti gli attori coinvolti a tutti i livelli.

ABIFormazione ha strutturato un'offerta formativa per accompagnare le banche nel processo di adeguamento alle nuove disposizioni, pensata per i diversi ruoli coinvolti nel presidio del rischio ICT e Sicurezza con uno sguardo alle future evoluzioni in ottica di integrazione tra novità ex Circolare 285/2013 e processi di trasformazione DORA.

ALTA FORMAZIONE PER GLI ORGANI DI VERTICE

Percorso di Alta Formazione per il Consiglio di Amministrazione delle banche
GOVERNANCE DEL RISHIO ICT E SICUREZZA

L'evoluzione digitale che sta caratterizzando la trasformazione del settore bancario offre opportunità di generare nuovo valore e al contempo produce un innalzamento del livello di attenzione dei rischi collegati. Il punto sulla digitalizzazione della banca e sulle nuove e dirette responsabilità del CdA nel presidio dei rischi ICT e di Sicurezza introdotte dal 40° aggiornamento della Circolare 285/2013 di Banca d'Italia

Modulo 1: **L'evoluzione digitale della banca: dalle cryptovalute al metaverso - 21 e 22 settembre**
Modulo 2: **Il sistema informativo in banca: elementi fondamentali, quadro regolamentare e governo del rischio ICT e Sicurezza - 18 e 19 ottobre**

Percorso di Alta Formazione
ESSERE CONSIGLIERE DI AMMINISTRAZIONE IN BANCA

Modulo 4: **Sfide e prospettive - 26 settembre**

Il modulo che supporta i componenti del CdA ad avere una visione organica dei nuovi paradigmi che stanno attraversando il settore bancario focalizzando, in particolare, i due principali driver di cambiamento: sostenibilità e digitalizzazione.

CORSI E PERCORSI

Corso propedeutico

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**
- **funzione IT (I livello) che deve relazionarsi con le funzioni di II livello**

Le novità introdotte dal 40° aggiornamento della Circolare Banca d'Italia comportano l'esigenza di nuovi assetti organizzativi e un nuovo set di competenze. Per favorire il processo di allineamento delle conoscenze delle persone che saranno coinvolte sul processo di presidio del rischio ICT e Sicurezza, è consigliato un corso propedeutico differenziato per target.

Modulo 1.a): **ICT Risk e Sicurezza: i fondamenti per orientarsi nel sistema informativo della banca - 19 e 20 giugno**
Rivolto a esperti di funzioni di controllo che non hanno esperienza relativa al sistema informativo
Modulo 1.b): **ICT Risk e Sicurezza: i fondamenti per orientarsi nel sistema dei controlli interni - 21 giugno**
Rivolto a esperti IT (I livello) che devono interfacciarsi con le funzioni di controllo di II livello.

Percorso professionalizzante

DIVENTA ICT RISK E SECURITY EXPERT

Destinatari:

- **nuova funzione ICT Risk e Sicurezza (percorso intero)**
- **funzione Risk Management (moduli 1, 2a e 3)**
- **funzione Compliance (moduli 1, 2b e 3)**

Favorire lo sviluppo delle conoscenze e competenze necessarie a presidiare e gestire il rischio ICT e Sicurezza secondo quanto previsto dal 40° aggiornamento della Circolare Banca d'Italia e in linea prospettica con quanto delineato dal Regolamento DORA sulla resilienza digitale operativa. È destinato sia a coloro che faranno parte della nuova funzione di controllo sia a coloro che gestiranno tali rischi all'interno delle funzioni Risk Management e Compliance. È richiesta una conoscenza dei fondamenti di gestione dei rischi e dei sistemi informativi trattati nel modulo propedeutico.

Modulo 1: **Profiling dell'ICT Risk e Security Expert: evoluzione regolamentare, assetti e ruoli organizzativi, competenze richieste - 18 e 19 settembre**
Modulo 2a): **ICT Risk Management - La gestione della Sicurezza dell'informazione, delle operazioni ICT, dei progetti e dei cambiamenti ICT, dei fornitori e terze parti - 26 e 27 settembre**
Modulo 2b): **Compliance Management per il rischio ICT e Sicurezza - 5 e 6 ottobre**
Modulo 3: **Cyber Risk Management - Metodi e strumenti per la prevenzione e gestione - 18 e 19 ottobre**
Test: **30 ottobre**

LA GESTIONE DELL'OUTSOURCING, FORNITORI E TERZE PARTI NEL NUOVO QUADRO REGOLAMENTARE: GLI IMPATTI OPERATIVI PER LE BANCHE

10 e 11 ottobre

Il punto sul quadro regolamentare in una visione prospettica delle diverse normative che impattano sul framework delle esternalizzazioni, fornitori e terze parti, le modalità operative per affrontare le maggiori complessità di gestione, le migliori prassi applicative.

CYBER RISK INTELLIGENCE - LABORATORIO DI GESTIONE DEL RISCHIO CYBER

28 e 29 novembre

Un corso operativo destinato a coloro che sono chiamati a presidiare e gestire il framework di Cyber Risk Management. Strutturato su casi pratici e use case in cui i partecipanti sono chiamati a mettere in pratica metodologie e strumenti per la definizione e il monitoraggio di indicatori di rischio che possano offrire una vista prospettica sui Cyber Risk.

SEMINARI E LABORATORI

Seminario

IL REGOLAMENTO DORA: IL PUNTO SUL QUADRO REGOLAMENTARE E GLI IMPATTI COLLEGATI AI 5 PILASTRI DI APPLICAZIONE - 2° semestre

L'analisi degli impatti operativi derivanti dal Regolamento DORA per ciascuno dei cinque ambiti di applicazione: ICT Governance e Risk Management, Terze parti ICT, ICT Threat Intelligence e Info Sharing, Digital Operational Resilience Testing, Incident Management e Reporting.

Laboratori di confronto

GLI STEP DI IMPLEMENTAZIONE DEL PIANO ICT E SICUREZZA IN OTTICA DORA 2° semestre

Un ciclo di incontri finalizzato al confronto operativo tra i partecipanti e gli esperti che condurranno i laboratori, sugli ambiti di maggiore complessità relativi al percorso di adeguamento alle novità normative in ambito ICT Risk e Sicurezza in ottica integrata con il Regolamento DORA.

CORSI ELEARNING ASINCRONI

SUITE CYBERSECURITY - 8 moduli in modalità asincrona

Nessuno oggi può prescindere dal considerare la cybersecurity come elemento strategico per la difesa dei propri dati, aziendali o personali: la questione non è quella di sapere "se saremo attaccati" ma solo "quando". Non importa se siamo grandi o piccoli, privati o aziende: prima o poi ci attaccheranno. Il web è diventato un luogo pericoloso? Possiamo difenderci.

I corsi della suite, multimediali e interattivi, offrono esempi di truffe informatiche e casi pratici di cybersecurity, descrivono i più attuali trend di minaccia cyber e le diverse tipologie di attacchi informatici per favorire la consapevolezza dei rischi, la capacità di riconoscerli e di applicare le precauzioni e i mezzi di difesa più opportuni.

- **Cybersecurity: un gioco di squadra**
- **Perché la cybersecurity è diventata così importante**
- **Le modalità più utilizzate di attacco informatico. Social engineering e phishing**
- **Gli attacchi attraverso la posta elettronica**
- **I ransomware: la minaccia oggi più temibile**
- **Malware su dispositivi mobili**
- **Messaggistica istantanea: ci possiamo fidare?**
- **Imparare a usare le password**

ABISERVIZI

ABI FORMAZIONE

Per ogni ulteriore approfondimento si invita
a contattare ABIFormazione, in particolare:

Barbara Filippella, **b.filippella@abiformazione.it**
Elisa Isacco, **e.isacco@abiservizi.it**