PERCORSO

CONOSCERE E GESTIRE IL CYBER RISK

MILANO • Copernico Centrale, Via Copernico, 38

1° Mod. • **Introduzione al cyber risk – Cyber risk regulation** *(19, 20 e 21 giugno 2019)*

2° Mod • **Cyber risk management** *(8, 9 e 10 luglio 2019)*

1° MODULO • INTRODUZIONE AL CYBER RISK – CYBER RISK REGULATION

19, 20 e 21 giugno 2019

- IL NUOVO SCENARIO TECNOLOGICO E DIGITALE: LA GESTIONE DELLA CYBERSECURITY
  - L'evoluzione tecnologica e digitale nel contesto bancario e finanziario
  - Conoscere le minacce e le vulnerabilità che possono influenzare i sistemi informativi aziendali per creare un ambiente security confident
  - I rischi collegati all'ICT e il cyber risk: identificazione e gestione
  - La gestione della cybersecurity
- IL TREND DEGLI INCIDENTI E DELLE PERDITE RELATIVE AL CYBER RISK
  - Gli scenari di attacchi cyber
  - Analisi dei principali attacchi al settore bancario: il cybercrime, dark web, hacker profiling
  - Il prezzo della cyber (in)security
  - Gli impatti del cyber crime: proteggere la business continuity, il patrimonio informativo e la reputazione
  - La prevenzione del rischio sanzionatorio: gli impatti di un data breach
- I RISCHI DERIVANTI DALL'INTERNO
  - I rischi interni diretti: le frodi interne
  - I rischi interni indiretti: il social engineering
  - Analisi di scenario delle frodi identitarie: i canali internet, mobile
  - Le strategie per gestire il fattore umano: la cultura del rischio per prevenire le azioni volontarie e involontarie
- LA CYBER RESILIENCE
  - Oltre i sistemi IT: impostare la cyber resilience agendo sulle sull'organizzazione e la cultura del rischio
  - La "Guidance on cyber resilience for financial market infrastructures" del Committee on Payments and Market Infrastructures (CPMI) e del Board of the International Organization of Securities Commissions (IOSCO): le raccomandazioni sui livelli di cyber resilience
- COSTRUIRE IL PROPRIO MODELLO DI COMPLIANCE ICT A PARTIRE DALLA DEFINIZIONE DEL PERIMETRO NORMATIVO
  - L'approccio per l'identificazione del perimetro normativo di riferimento
  - Il perimetro "core" e il perimetro indiretto degli adempimenti IT
- 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
- L'ANALISI DEL RISCHIO DI CONFORMITÀ RELATIVO AI SERVIZI ICT
  - Il processo di classificazione delle risorse ICT 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 CYBERSECURITY ALL'INTERNO DELLE PRINCIPALI NORMATIVE DI RILIEVO (PSD2, GDPR, DIRETTIVA N. 1148/2016...)

- LA CYBERSECURITY ALLA LUCE DEL GDPR
  Requisiti normativi in termini di misure di sicurezza informatica
  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
- IL PANORAMA NORMATIVO NAZIONALE ED EUROPEO PER LA GESTIONE DEL RISCHIO INFORMATICO: LE SOVRAPPOSIZIONI, LE PECULIARITÀ, LE OPPORTUNITÀ DI INTEGRAZIONE DEI DIVERSI REQUISITI
- LE RECENTI ATTIVITÀ DEI REGOLATORI
  - Raccomandazioni EBA/REC/2017/03 del 20 dicembre 2017 - Raccomandazioni sul ricorso in outsourcing a servizi di cloud computing "Recommendations on outsourcing to cloud services providers"
  - Direttiva 1148/2016/(UE) recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi dell'Unione ("Direttiva NIS - Network and Information Security")
  - La Direttiva (UE) 2019/713 del Parlamento europeo e del Consiglio del 17 aprile 2019 relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti
  - Commissione Europea: documento di correzione alla proposta di regolamento del Parlamento Europeo e del consiglio relativo all'ENISA, l'agenzia dell'Unione Europea per la cybersecurity, che abroga il regolamento (UE) n. 526/2013
- I MODELLI DI GESTIONE DELLA SICUREZZA E GLI STANDARD INTERNAZIONALI DI RIFERIMENTO
  - Gli obiettivi dei modelli di gestione della sicurezza e le norme ISO
  - Le norme della famiglia ISO 27000 e approfondimenti sulla 27001
  - Il rischio e le norme ISO27005 e ISO 31000
  - La norma ISO 22301: lo standard internazionale per raggiungere elevati livelli di cyber resilience
  - Il NIST
  - Il confine tra la gestione della sicurezza dell'informazione e gli approcci orientati specificatamente alla protezione contro gli attacchi da internet della cybersecurity
- COSTRUIRE/EVOLVERE IL PROPRIO MODELLO DI COMPLIANCE ICT A PARTIRE DALLA DEFINIZIONE DEL PERIMETRO NORMATIVO
  - Modelli per il governo e il controllo IT e COBIT
  - Il modello organizzativo e i processi della Compliance ICT in BPER BANCA
- FOCUS: I NUOVI SCENARI DI RISCHIO DERIVANTI DALL'APPLICAZIONE DELLA PSD2 CON IMPATTO SU IT/SECURITY
- LA GESTIONE DEL CYBER RISK NELLE ESTERNALIZZAZIONI
- GLI IMPATTI DEI NUOVI ORIENTAMENTI EBA IN MATERIA DI OUTSOURCING: IL "FINAL REPORT ON EBA DRAFT GUIDELINES ON OUTSOURCING ARRANGEMENTS"
- L'EVOLUZIONE DELLA SICUREZZA INFORMATICA NELLA VALUTAZIONE DELL'AFFIDABILITÀ DEI FORNITORI
  - L'esternalizzazione dei servizi IT
  - La protezione dei dati esternalizzati: la conformità al GDPR e l'approccio risk based
  - La gestione dei rischi legati alle cd. fintech
- LA GESTIONE DEI SISTEMI INFORMATIVI IN CLOUD: IL RUOLO DELLE FUNZIONI DI CONTROLLO
  - 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:
    - la definizione degli SLA
    - la cancellazione dei dati alla cessazione del rapporto
    - la proprietà dei dati e il rispetto delle norme sul trattamento dei dati personali
    - la modifica unilaterale delle condizioni contrattuali
    - il diritto di recesso del fornitore
- IL PERIMETRO DI RIFERIMENTO E LE RESPONSABILITÀ DELLA FUNZIONE INTERNAL AUDIT: I CONTROLLI IN CASO DI ESTERNALIZZAZIONE DEL SISTEMO INFORMATIVO E DEI SERVIZI IT
  - I controlli da programmare e porre in essere sui processi esternalizzati
  - I controlli di rispetto degli SLA
  - Modalità per rendere più efficace il controllo dell'esternalizzazione delle funzioni ICT
- TESTIMONIANZE BANCARIE

2° MODULO • CYBER RISK MANAGEMENT

8, 9 e 10 luglio 2019

- IL SISTEMA INFORMATIVO IN BANCA: ORGANIZZAZIONE E PROCESSI DI GESTIONE PER LA CYBERSECURITY
  - Come cambia il modello di gestione della sicurezza post Circolare 285 alla luce delle nuove sfide di cybersecurity
  - Modelli data-driven di protezione della sicurezza e delle informazioni, alla luce del GDPR
  - La sicurezza by design: costruzione di un processo/servizio ICT conforme alle policy di cybersecurity sin dall'ideazione all'erogazione e capace di indirizzare tutte le compliance bancarie
  - Information security, cybersecurity, data protection, data governance, enterprise risk management: relazioni tra i diversi processi, opportunità da cogliere, rischi da evitare
- LA GESTIONE DEL RISCHIO IT COME ELEMENTO CENTRALE DELLA SICUREZZA INFORMATICA
  - Il rischio IT e le interrelazioni con le altre tipologie di rischio operativo
  - Le responsabilità delle funzioni aziendali di controllo in banca nella gestione dell'IT risk, cyber risk e cyber crime
  - Modelli operativi, governance, flussi informativi
  - Il framework di gestione del cyber risk: identificazione e misurazione, prevenzione, monitoraggio, mitigazione
  - Risk, threat and vulnerability assessment
  - Dal problem al data breach, passando per "l'incidente rilevante"
- IL FRAMEWORK NAZIONALE PER LA CYBERSECURITY REALIZZATO DAL CIS-SAPIENZA E DAL LABORATORIO NAZIONALE DI CYBERSECURITY
- L'EVOLUZIONE DEL FRAMEWORK DI GESTIONE DEL RISCHIO INFORMATICO: L'ESPERIENZA DI IBL BANCA
  - Gli "Orientamenti EBA sulla valutazione dei rischi ict a norma del processo SREP" (11 maggio 2017): le cinque dimensioni del modello di gestione del rischio informatico (ICT availability and continuity risks, ICT security risks, ICT change risks, ICT data integrity risks, ICT outsourcing risks)
  - Le scelte operative di IBL Banca
- CYBER RESILIENCE E CONTROMISURE PER PREVENIRE IL RISCHIO CYBER
  - Ruolo e responsabilità delle funzioni operative IT e Sicurezza e delle funzioni di controllo Compliance, Risk Management e Audit
  - Modello operativo e coordinamento/flussi informativi tra le funzioni coinvolte
  - Principali aree per la gestione della cyber resilience
  - Strumenti analytics come acceleratore per una più efficace cyber resilience
- IL CONTROLLO E IL MONITORAGGIO DEL CYBER RISK ATTRAVERSO IL RISK APPETITE E INDICATORI DI RISCHIO
  - 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
  - L'uso degli Analytics per svolgere analisi di trend e predittive sul rischio cyber
- LA GESTIONE DEGLI EVENTI DI CRISI
  - Dalla gestione degli incident alla gestione delle crisi
  - 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 incident management
  - La gestione degli eventi di crisi e la definizione del piano di comunicazione
- ESERCITAZIONE: COMUNICARE L'EVENTO DI CRISI
- DIGITAL CYBER CULTURE & AWARENESS
  - Perché rilevante per la cybersecurity
  - Il ruolo delle funzioni operative IT & Sicurezza e di controllo (Risk Management, Compliance e Audit)
  - Principali soluzioni di mercato per incrementare il livello di Culture & Awareness
  - Approccio Digital per la diffusione della Cyber Culture & Awareness all'interno dell'organizzazione a tutti i livelli
- L'UTILIZZO DELLA DATA GOVERNANCE PER MIGLIORARE LA CYBER SECURITY
  - Strumento di supporto e guida per le funzioni IT e Sicurezza e di controllo per Risk Management e Audit
  - Data-Driven Cyber Security by Design
  - Data-Driven Security Development and Testing
  - Cyber Risk Controls utilizzando strumenti di Data Discovery & Data Lineage
- CYBER RISK MEASUREMENT: COME PRIORITIZZARE I RISCHI CYBER (Analisi di dati tratti dal rapporto CLUSIT 2018)
- QUADRO DI RIFERIMENTO ORGANIZZATIVO E METODOLOGICO PER L'ICT AUDIT
  - Le previsioni normative in materia di ICT Audit
  - Perimetro dell'ICT Audit
  - Framework metodologico per la conduzione delle verifiche
  - Caso studio
- TESTIMONIANZE BANCARIE