

Giornate formative

ICT RISK E RESILIENZA OPERATIVA DIGITALE: DALL'EVOLUZIONE NORMATIVA AI NUOVI MODELLI OPERATIVI

8 e 9 aprile 2024 • Milano, SpazioPola - Aula virtuale



Prima giornata • 8 aprile 2024 (10.00 - 16.30)

► Introduzione ai lavori

OPEN SESSION

LA GESTIONE DEL RISCHIO INFORMATICO: IL FRAMEWORK REGOLAMENTARE E GLI IMPATTI PER IL SETTORE BANCARIO E FINANZIARIO

- **L'attenzione del Regolatore europeo sui rischio ICT: un quadro d'insieme della regolamentazione a livello europeo e nazionale**
- **I building blocks del DORA per proteggere il settore bancario e finanziario dalle minacce digitali: i punti di maggiore attenzione**
 - 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 resilience 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

Luca Cusmano, Dipartimento Vigilanza Bancaria e Finanziaria, Servizio Rapporti Istituzionali di Vigilanza, Capo Divisione Supporto Statistico e Informatico, **Banca d'Italia**

SESSIONE 1

IL REGOLAMENTO DORA: DAI VINCOLI NORMATIVI ALLE PRIORITA' DI INTERVENTO OPERATIVO PER L'ADEGUAMENTO

- **Il rischio ICT nei diversi input normativi e le dimensioni di gestione della resilienza in banca**
 - Il Regolamento DORA vs Circolare n. 285/2013 di Banca d'Italia: gap analysis dei requisiti normativi
 - Business resilience framework: un modello di gestione che comprenda le diverse dimensioni della resilienza in banca

*Relatori confermati***Romano Stasi**, Segretario Generale, **ABI Lab****Piero Piperno**, Senior research analyst, Continuità Operativa e Resilience **CERTFin****Stephane Speich**, Head Business Continuity & Resilience Group Governance **Unicredit**

► Gli impatti del Regolamento DORA e le priorità di azione

- Una vista integrata e sinergica di alcune richieste regolamentari e di Supervisione: DORA; ECB Targeted Review on Cyber Resilience, ECB Cyber Stress Test
- Lessons learnt a seguito del Cyber Resilience Stress Test 2024 promosso da ECB: un esercizio pratico di applicazione dei requisiti DORA
- Le principali evidenze dei Maturity assessment
- Punti chiave, roadmap design principles e best practice per l'implementazione del DORA in ottica risk based

*Relatori confermati***Paolo Carcano**, Partner **PwC****Samantha Trama**, Director **PwC**



SESSIONE 2

L'EVOLUZIONE DEL FRAMEWORK DI GESTIONE DEL RISCHIO ICT E SICUREZZA

► **Impact analysis degli RTS per armonizzare gli strumenti, i metodi e le politiche di gestione del rischio ICT**

- Definizione della Strategia Resilienza Operativa Digitale: la visione integrata del primo e secondo livello di controllo

Francesco Brunetti, Director **PwC**

Priorità e impatti per la seconda linea (CRO)

- Procedure di governo e controllo: ruoli, responsabilità, assetti organizzativi
- L'evoluzione della Funzione Risk management e del Framework di gestione dei rischi ICT e di Sicurezza: i principali impatti operativi e metodologici

Relatori confermati

Nicasio Muscia, Managing Director **Accenture**

Priorità e impatti per la prima linea (CIO; CISO)

- I temi rilevanti derivanti del DORA maturity assessment e gli RTS: le sinergie con le altre priorità di Supervisione
- Impatti delle Funzioni Essenziali o Importanti sulle evoluzioni in ambito Asset & Configuration management
- Come affrontare la sfida delle implementazioni tecnologiche (Crittografia; Sicurezza dei dati, dei sistemi e della rete; Identity Management; Backup)
- Dalla Business Continuity alla ICT Business Continuity: un cambio di prospettiva già sperimentato nel Cyber Resilience Stress Test

Relatori confermati

Samantha Trama, Director **PwC**

Alessio Serafino, Senior Manager **PwC**

Petra Chiste Responsabile della Sicurezza **Volksbank**



Seconda giornata • 9 aprile 2024 (10.00 - 16.30)

SESSIONE 3

THIRD PARTY RISK MANAGEMENT & AGREEMENTS: COME EVOLVE LA GESTIONE DEL RISCHIO TERZE PARTI E LA SORVEGLIANZA PROVIDER CRITICI

► Outsourcing, fornitori e terze parti: gli impatti del nuovo quadro regolamentare

- 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

Relatori confermati

Pasquale Iannelli, Senior Manager **PwC**

Andrea Milani, Senior Manager **PwC**

Gabriele Faggioli, CEO **Digital360 e Partners4Innovation**

Anna Italiano, Partner **Partners4Innovation**

► La governance dei rischi delle terze e quarte parti e la sorveglianza dei provider critici

- 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

Relatori confermati

Maria Cristina Daga, Partner **Partners4Innovation**

SESSIONE 4

ICT MAJOR INCIDENT REPORTING: LA GESTIONE DEGLI EVENTI CRITICI TRA CLASSIFICAZIONE, SEGNALAZIONE, ARMONIZZAZIONE DEI TEMPLATE

► 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
- Impact analysis rispetto a quanto a oggi in essere a livello italiano ed europeo
- 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

Relatori confermati

Lorenzo Ramaccioni, Senior Manager **PwC**

Massimo Messina, senior Advisor



SESSIONE 5

DIGITAL OPERATION RESILIENCE TESTING: LE NOVITÀ E LA RELAZIONE CON TIBER EU/IT

► L'attività di testing da obbligo normativo a opportunità di sviluppo

- I test avanzati di strumenti, sistemi e processi ICT basati su test di penetrazione guidati dalla minaccia (TLPT): la relazione con Tiber EU/IT
- Il framework TIBER EU/IT: le peculiarità dell'approccio dei test di penetrazione guidati dalla minaccia
- 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
- Miglioramento continuo: competenze specialistiche, meccanismi di resilienza e info sharing

Relatori confermati

Dante Niro, Director **PwC**

SESSIONE 6

I MODELLI ORGANIZZATIVI, I PROCESSI, LE PERSONE

- Miglioramento continuo: competenze specialistiche, meccanismi di resilienza e info sharing
- Persone e competenze come requisito per la sostenibilità della roadmap di adeguamento al DORA
- La formazione come leva strategica a tutti i livelli organizzativi