# La Cybersecurity oltre DORA

**Samantha Trama**, Director PwC Italy

ABI Banche e Sicurezza 2025 | Parallela E “DORA in avanti” | 28 Maggio 2025

# Agenda

1. PwC View | Operalizzazione DORA e stato di adeguamento del mercato
2. 2025+ | La Cybersecurity oltre DORA
3. Challenge ed Opportunità per i Security Officer

# 1

# PwC View Operalizzazone DORA e stato di adeguamento del mercato

# Profilo della Survey

**300+**

**Clienti DORA a livello EMEA**

- Banking & Capital Markets
- Insurance
- Asset & Wealth Management
- Payment Institutions
- Altre entità (SGR, IMEL, ICT Service provider,...)

## Obiettivo

Identificare il livello di maturità del mercato EMEA rispetto ai requisiti DORA, coerentemente alle attività ritenute essenziali rispetto alle fasi di adeguamento riconducibili ai piani di remediation tipicamente realizzati dalle istituzioni finanziarie.

## Ambiti oggetto di indagine

### 1. Set Up di Processi, Metodologie e Procedure DORA

Attività di definizione ed implementazione delle metodologie, processi e procedure previste ed in carico alla singola FSI, anche valorizzando e monitorando quanto eseguito dai fornitori ICT laddove applicabile.

### 2. Operazionalizzazione DORA (2025+)

Attività per la messa a terra ed automatizzazione tanto dei processi quanto dei requisiti tecnologici previsti da DORA per le Banche (oltre ai fornitori ICT).

# PwC View: DORA Operalization (1/2)

| | | | | | Set Up | Operalization |
|---|---|---|---|---|---|---|
| A | Resilience Strategy | Policy<br>TOM, Ruoli e Accountability<br>Framework | Flussi Informativi<br>Calendarizzazione | Integrazione cross-funzionale | 🟡 | 🔴 |
| A<br>B | Manutenzione mappatura FEI | Accountability e Processi<br>Manutenzione | Processi e Tecnologie Asset Management & Visibility | Integrazione 3 e 4 Parti<br>Tool di Orchestrazione | 🟡 | 🔴 |
| A | End-to-End ICT & Cyber Risk | RAF<br>Scenari | Impact Tolerance<br>Resilience Strategy | Integrazione con BCM evoluta e Stress Testing | 🟢 | 🟡 |
| A | DORA Integrated Controls | Modello dei controlli interni vs. Impianto documentale | Sintesi indicatori<br>Integrazione indicatori | Flussi Informativi<br>Rappresentazione CdA | 🟡 | 🔴 |
| A | TPRM | Registro Terze Parti<br>Processi di manutenzione e workflow | Contract Review<br>Controlli I e II linea<br>Verifica SLA | Automatizzazione processi e controlli tramite tool | 🟢 | 🟡 |
| A | BCM Evo / ICT Continuity | Metodologia BIA<br>Contingency | Nuovi modelli e procedure operative vs. scenari definiti | Tempi di ripristino per scenari ICT Continuity | 🟢 | 🔴 |
| A<br>B | Threat Intelligence | Attività Threat Intelligence<br>Threat Profiling | Analisi e definizione scenari<br>Monitoraggio 3 e 4 Parti | Formazione CdA | 🟡 | 🟡 |
| A<br>B | Landscape Tecnologico | Analisi di soluzioni tecnologiche processi e procedure | Priorità di intervento | Roadmap e programma di monitoraggio implementazioni (incl. Outsourcer) | 🟡 | 🟡 |

**100%**

Soggetti FS italiani Soggetti che hanno in corso attività di operalizzazione e di implementazione di processi e tecnologie DORA.

**87%**

Soggetti FS italiani con budget dedicato a DORA nel 2025.

**Legenda**

A Interventi in ownership alla singola FSI

B Interventi in compartecipazione con il fornitore/department ICT

🟢 In larga parte completato

🟡 In corso

🔴 Da avviare

# PwC View: DORA Operalization (2/2)

| | | | | | Set Up | Operalization |
|---|---|---|---|---|---|---|
| A B | Incident Management | Classification & Reporting<br>Skill, capacity, SOC | Evoluzione End-to-End da early warning a follow up (incl. Tecnologie) | Integrazione log, SIEM | | |
| A B | Resilience Testing | Metodologia e processi<br>Execution | Integrazione nei processi BAU Operations | TLPT | | |
| A B | Security by Design | Rischi di Sicurezza<br>Requisiti di Sicurezza | Integrazione presidi di Sicurezza | Testing w/SDLC | | |
| A B | Identity Governance Access Mgmt | Ricertificazione Profili<br>Inclusione 3 Parti ed ecosistema business | Modelli operativi, ruoli e coni di visibilità<br>Adozione/estensione IGA | Adozione/estensione MFA | | |
| A B | Secure Endpoint & Vulnerability | Visibility & discovery<br>Cyber Hygiene | Vulnerability scan<br>EDR/Antimalware | Patching | | |
| A B | Data Protection | Autenticità del dato<br>Classificazione del dato | Dati in transit<br>Dati at rest<br>Dati in Use | Data Sanitization<br>Integrità, riservatezza disponibilità del dato | | |
| A B | Network Security | Segregagazione e segmentazione su subnetwork e component | Aggiornamento mappatura architettura di rete e flussi | Ricertificazione regole firewall | | |
| A B | Secure Backup | Backup Immutability<br>Backup Isolation | Backup analysis to prevent ransomware/wiper spread | Cyber Recovery procedures | | |

96%

Soggetti FS italiani in cui la governance DORA non ha partecipato allo sviluppo di requisiti funzionali per le tecnologie DORA nè hanno partecipato alla costruzione di una roadmap in logica Segregation of Duties.

80%

Soggetti FS italiani che hanno strutturato una procedura per i Test di Resilienza, ma l'esecuzione è limitata solo ad alcuni ambiti o sistemi critici. Non includono ad esempio le terze parti ICT.

**Legenda**

A Interventi in ownership alla singola FSI

B Interventi in compartecipazione con il fornitore/department ICT

In larga parte completato

In corso

Da avviare

2

# 2025+ La Cybersecurity oltre DORA

# Cybersecurity verso DORA e oltre (1/2)

| Obiettivi Strategici dei CSO/CISO dal 2025+ | | Impatti e Correlazioni con altri Processi/Funzioni Aziendali | Impatti e Governo della Supply Chain (Outsourcer e 3 Parti) |
|---|---|---|---|
| **Resilience Governance** | • Dashboard di sicurezza (KPI/KRI) vs. Funzioni Essenziali/Importanti<br>• Orchestrazione Funzioni Essenziali/Importanti<br>• Razionalizzazione investimenti tecnologici | • ICT/Cyber Risk management<br>• Organizzazione<br>• Funzioni Business<br>• ICT / Security Operations<br>• Sicurezza Fisica | • Integrazione 3 Parti ed ecosistema tramite monitoraggio indicatori TI e osservazione tecnologica |
| **Scenario Modelling** | • Continuo aggiornamento vs. evoluzione contesto (es. blackout)<br>• Interpretazioni Threat Intelligence e declinazione scenari plausibili<br>• Declinazione operativa (no scenari astratti) | • ICT/Cyber Risk management<br>• Outsourcing Management/TPRM<br>• Sicurezza Fisica<br>• ESG<br>• BCM / Crisis Management | • Strutturazione scenari 3 Parti con componenti di sicurezza ibrida (cyber-fisico), geopolitica e ESG |
| **BCM Evo vs. Resilience** | • Correlazione impatti vs. business<br>• Impatti degli scenari tecnologici e nuovi RTO/RPO<br>• Valutazione multi-scenario ed «effetto domino»<br>• Integrazione AI | • ICT/Cyber Risk management<br>• Organizzazione<br>• Funzioni Business<br>• ICT / Security Operations | • Migliore valutazione degli scenari ed effetti di disruption sui servizi forniti da 3 Parti<br>• Contingency solution dedicate |
| **Security By Design** | • Presidio funzionale ed architetturale<br>• Dialogo nel continuo con funzioni Business<br>• Gestione rischi cyber su spinte di innovazione tecnologica (e.g. AI; Quantum)<br>• Evoluzione delle architetture di riferimento in ottica resiliente | • Funzioni Business<br>• Demand Management<br>• Change Management | • Presidi SbD nei confronti delle 3 Parti rilevanti (es. Outsourcer ICT)<br>• Analisi funzionale e requisiti ex ante<br>• Monitoraggio nel corso della roadmap implementativa<br>• Testing |

# Cybersecurity verso DORA e oltre (2/2)

| Obiettivi Strategici dei CSO/CISO dal 2025+ | | Impatti e Correlazioni con altri Processi/Funzioni Aziendali | Impatti e Governo della Supply Chain (Outsourcer e 3 Parti) |
|---|---|---|---|
| **Data Protection** | • Protezione dato end-to-end<br>• Migliore visibilità su tipologia e modalità di gestione del dato anche sulla Supply Chain<br>• Limitazione e monitoraggio accesso ai dati | • Audit<br>• Compliance / DPO / Legal<br>• Risk Management<br>• Organizzazione<br>• IT / Data Governance<br>• Funzioni Antifrode / Controlli Interni | • Monitoraggio eventi di accesso ai dati anche sui sistemi della terza parte<br>• Anonimizzazione/ protezione dei dati<br>• Cancellazione end to end |
| **Continuous testing** | • Test su declinazione Scenari DORA<br>• Continuous testing per ITSM e Cyber Operations<br>• Nuove soluzioni tecnologiche a supporto<br>• Simulazione scenari plausibili (Digital Twin e Stress Testing)<br>• Evolutive TLPT | • Audit<br>• Compliance / Legal<br>• Risk Management<br>• Organizzazione<br>• IT / Data Governance | • Condivisione delle esigenze di test tra clienti di uno stesso fornitore ICT<br>• Pooled testing |
| **Incident Management** | • Utilizzo efficace Threat Intelligence<br>• Analisi integrate log eventi<br>• Competenze e skill<br>• Migliore comprensione e preparazione tramite processi strutturati di analisi post incident | • ICT/Cyber Risk management<br>• Funzioni Business<br>• ICT / Security Operations<br>• BCM / Crisis Management<br>• Compliance / DPO | • Collaborazione bi-direzionale<br>• Monitoraggio TI<br>• Monitoraggio indicatori su eventi / incidenti su terze parti<br>• Aumento qualità servizi forniti |
| **Infosharing** | • Modelli strutturati analisi dei rischi<br>• Prodotti assicurativi cyber efficaci | • Risk Management | • Logiche di condivisione info near real time (log management estesi) |

3

# Challenge ed Opportunità per i Secuity Officer

# Two content

## CISO | CSO Ambition

Come evolverà il ruolo della Sicurezza?

↑ Estensione responsabilità in ambito governance
e modellizzazione scenari di rischio ed impatti.

↓ Responsabilità di messa a terra dei programmi di messa a terra delle tecnologie, evitando commistione con ruoli di governo.

## Make or Buy?

CISO End-to-End
Vs. Cyber Managed Services

**Specializzazione** su temi ad alto valore aggiunto, governo di fornitori esterni per servizi standardizzati e ripetibili.

**Rafforzamento** e specializzazione organizzazione e competenze per la fase run post implementazione.

## Data Security Owner

Chimera o obiettivo strategico?

**Accountable** di un security data lake proprietario e di cui la sicurezza è responsabile della qualità e correlazione efficace delle informazioni*.

**Cliente** fruitore di dati provenienti da altre fonti (tecnologie, strutture organizzative).

## Chief of Resilience

Governance o sovrastruttura?

**Passaggio** da approccio progettuale a quello di lungo periodo mantenendo accountability puntuali senza coordinamento centrale.

**Creazione** di struttura di governo del TOM Resilience specializzata sul lungo periodo.

**Raccolta e correlazione log, Threat Intelligence, classification, incident, frodi, test, controlli*

# Grazie

pwc.com