



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

PwC View Operalizzazione DORA e stato di adeguamento del mercato

1

Profilo della Survey

300+

Clienti DORA a livello EMEA

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.

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

Ambiti oggetto di indagine

1. Set Up di Processi, Metodologie e Procedure DORA

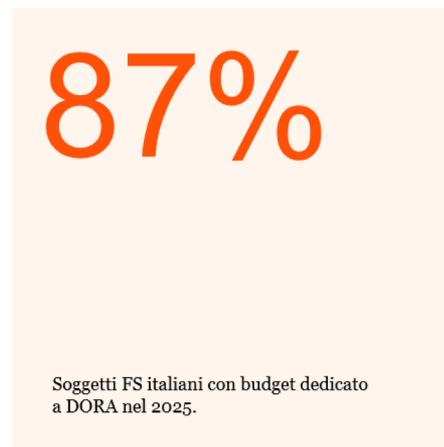
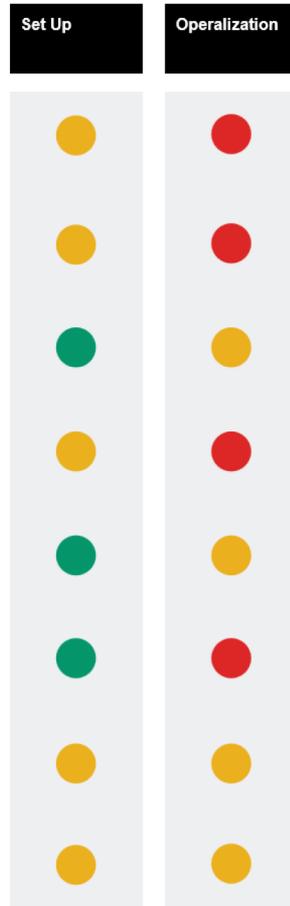
Attività di definizione ed implementazione delle metodologie, processi e procedure previste ed in carico alla singola FSI, anche valorizzando e monitorando quanto eseguito dai fornitori ICT laddove applicabile.

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 Operationalization (1/2)

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

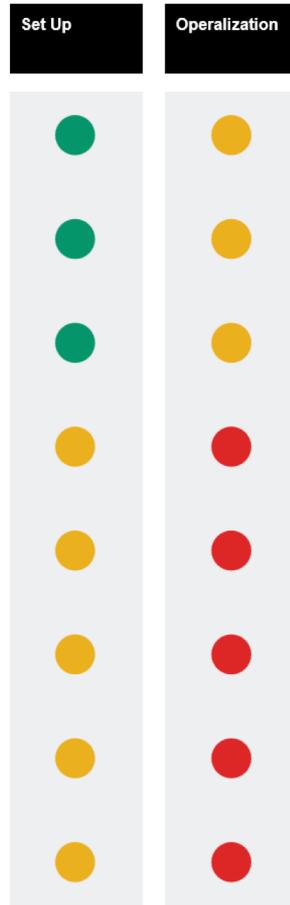


Legenda

- 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 Operationalization (2/2)

A B	Incident Management	Classification & Reporting 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 Execution	Integrazione nei processi BAU Operations	TLPT
A B	Security by Design	Rischi di Sicurezza Requisiti di Sicurezza	Integrazione presidi di Sicurezza	Testing w/SDLC
A B	Identity Governance Access Mgmt	Ricertificazione Profili Inclusione 3 Parti ed ecosistema business	Modelli operativi, ruoli e con di visibilità Adozione/estensione IGA	Adozione/estensione MFA
A B	Secure Endpoint & Vulnerability	Visibility & discovery Cyber Hygiene	Vulnerability scan EDR/Antimalware	Patching
A B	Data Protection	Autenticità del dato Classificazione del dato	Dati in transit Dati at rest Dati in Use	Data Sanitization Integrità, riservatezza disponibilità del dato
A B	Network Security	Segregazione e segmentazione su subnetwork e component	Aggiornamento mappatura architettura di rete e flussi	Ricertificazione regole firewall
A B	Secure Backup	Backup Immutability 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

2025+ La Cybersecurity oltre DORA

2

Cybersecurity verso DORA e oltre (1/2)

Obiettivi Strategici del CSO/CISO dal 2025+

Resilience Governance

- Dashboard di sicurezza (KPI/KRI) vs. Funzioni Essenziali/Importanti
- Orchestrazione Funzioni Essenziali/Importanti
- Razionalizzazione investimenti tecnologici

Scenario Modelling

- Continuo aggiornamento vs. evoluzione contesto (es. blackout)
- Interpretazioni Threat Intelligence e declinazione scenari plausibili
- Declinazione operativa (no scenari astratti)

BCM Evo vs. Resilience

- Correlazione impatti vs. business
- Impatti degli scenari tecnologici e nuovi RTO/RPO
- Valutazione multi-scenario ed «effetto domino»
- Integrazione AI

Security By Design

- Presidio funzionale ed architetturale
- Dialogo nel continuo con funzioni Business
- Gestione rischi cyber su spinte di innovazione tecnologica (e.g. AI; Quantum)
- Evoluzione delle architetture di riferimento in ottica resiliente

Impatti e Correlazioni con altri Processi/Funzioni Aziendali

- ICT/Cyber Risk management
- Organizzazione
- Funzioni Business
- ICT / Security Operations
- Sicurezza Fisica

- ICT/Cyber Risk management
- Outsourcing Management/TPRM
- Sicurezza Fisica
- ESG
- BCM / Crisis Management

- ICT/Cyber Risk management
- Organizzazione
- Funzioni Business
- ICT / Security Operations

- Funzioni Business
- Demand Management
- Change Management

Impatti e Governo della Supply Chain (Outsourcer e 3 Parti)

- Integrazione 3 Parti ed ecosistema tramite monitoraggio indicatori TI e osservazione tecnologica

- Strutturazione scenari 3 Parti con componenti di sicurezza ibrida (cyber-fisico), geopolitica e ESG

- Migliore valutazione degli scenari ed effetti di disruption sui servizi forniti da 3 Parti
- Contingency solution dedicate

- Presidi SbD nei confronti delle 3 Parti rilevanti (es. Outsourcer ICT)
- Analisi funzionale e requisiti ex ante
- Monitoraggio nel corso della roadmap implementativa
- Testing

Cybersecurity verso DORA e oltre (2/2)

Obiettivi Strategici del CSO/CISO dal 2025+

Data Protection

- Protezione dato end-to-end
- Migliore visibilità su tipologia e modalità di gestione del dato anche sulla Supply Chain
- Limitazione e monitoraggio accesso ai dati

Continuous testing

- Test su declinazione Scenari DORA
- Continuous testing per ITSM e Cyber Operations
- Nuove soluzioni tecnologiche a supporto
- Simulazione scenari plausibili (Digital Twin e Stress Testing)
- Evolutive TLPT

Incident Management

- Utilizzo efficace Threat Intelligence
- Analisi integrate log eventi
- Competenze e skill
- Migliore comprensione e preparazione tramite processi strutturati di analisi post incident

Infosharing

- Modelli strutturati analisi dei rischi
- Prodotti assicurativi cyber efficaci

Impatti e Correlazioni con altri Processi/Funzioni Aziendali

- Audit
- Compliance / DPO / Legal
- Risk Management
- Organizzazione
- IT / Data Governance
- Funzioni Antifrode / Controlli Interni

- Audit
- Compliance / Legal
- Risk Management
- Organizzazione
- IT / Data Governance

- ICT/Cyber Risk management
- Funzioni Business
- ICT / Security Operations
- BCM / Crisis Management
- Compliance / DPO

- Risk Management

Impatti e Governo della Supply Chain (Outsourcer e 3 Parti)

- Monitoraggio eventi di accesso ai dati anche sui sistemi della terza parte
- Anonimizzazione/ protezione dei dati
- Cancellazione end to end

- Condivisione delle esigenze di test tra clienti di uno stesso fornitore ICT
- Pooled testing

- Collaborazione bi-direzionale
- Monitoraggio TI
- Monitoraggio indicatori su eventi / incidenti su terze parti
- Aumento qualità servizi forniti

- Logiche di condivisione info near real time (log management estesi)

3

Challenge ed Opportunità per i Security 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.

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).

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.

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