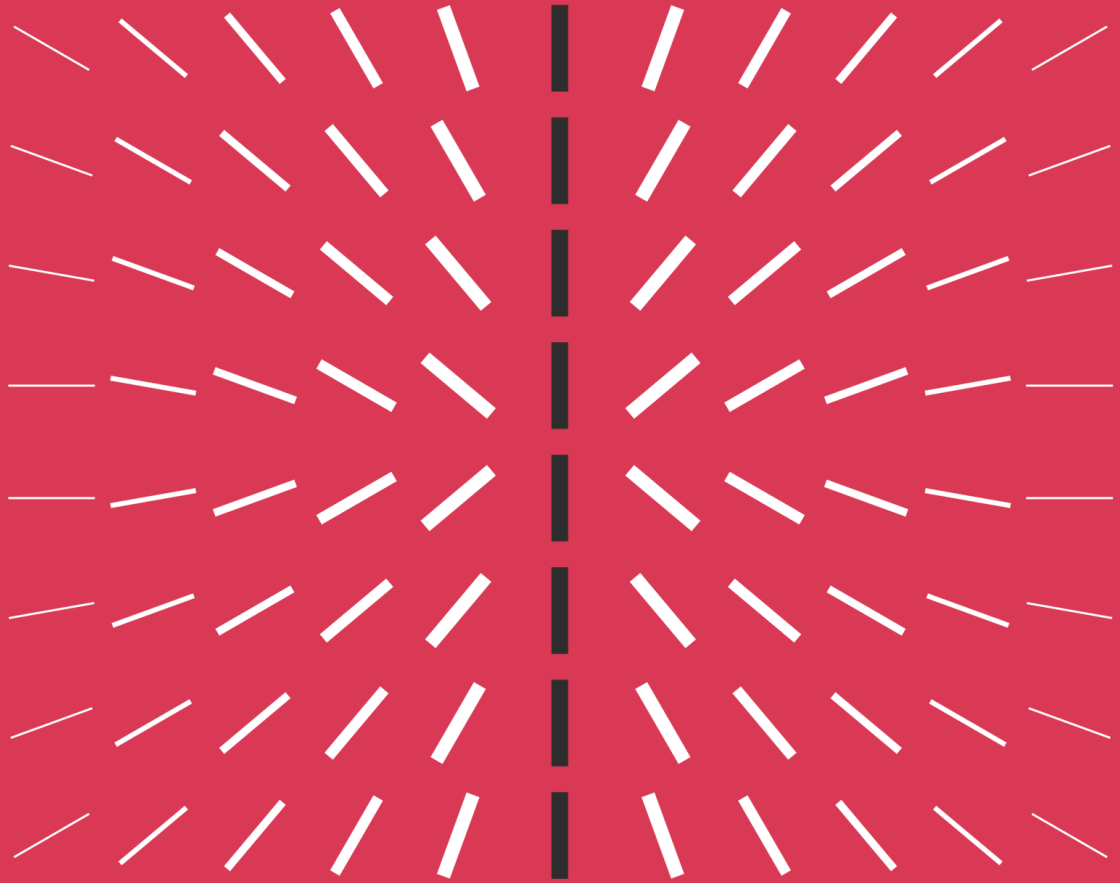
ABI Banche e Sicurezza 2021
Parallela C

Evolvere in Sicurezza: Nuovi strumenti per la Resilienza Operativa

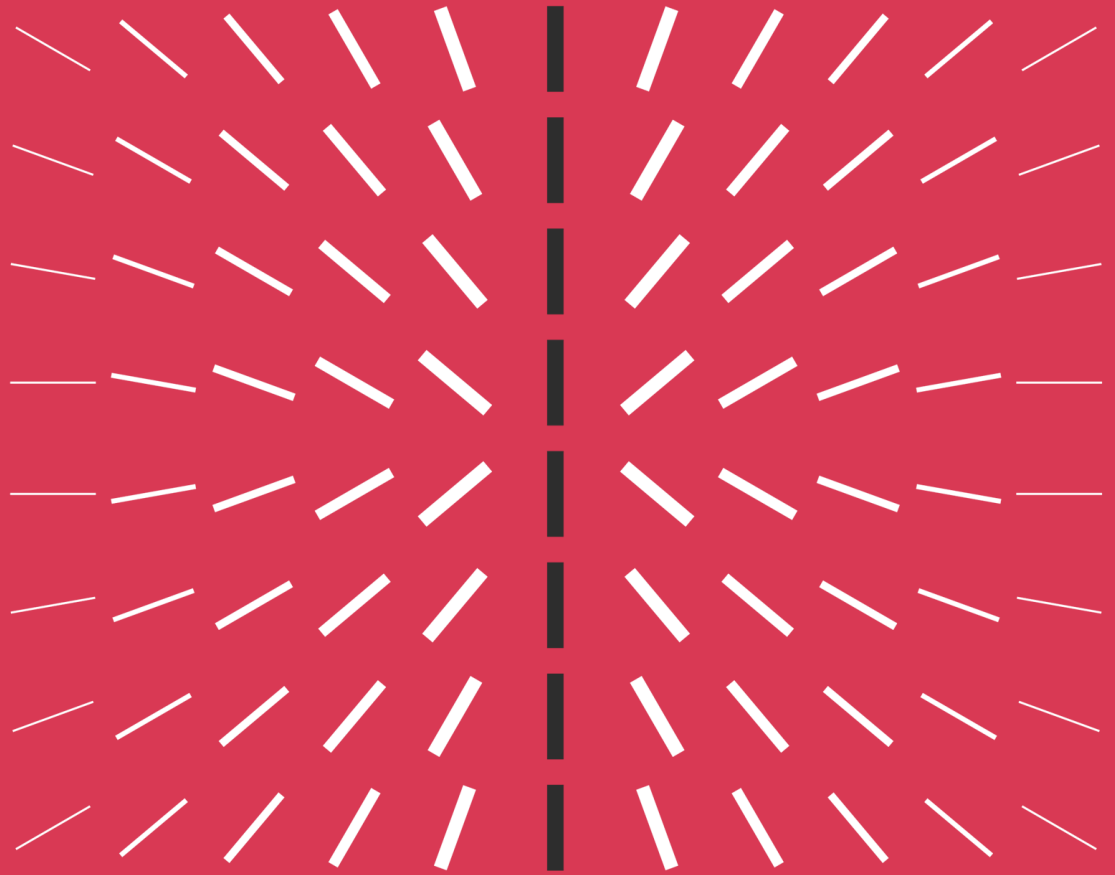
25 Maggio 2021

Samantha Trama, PwC Italia



1

Gli impatti DORA per il Settore Bancario



Il Contesto Regolamentare Digital Operational Resilience Act (DORA)

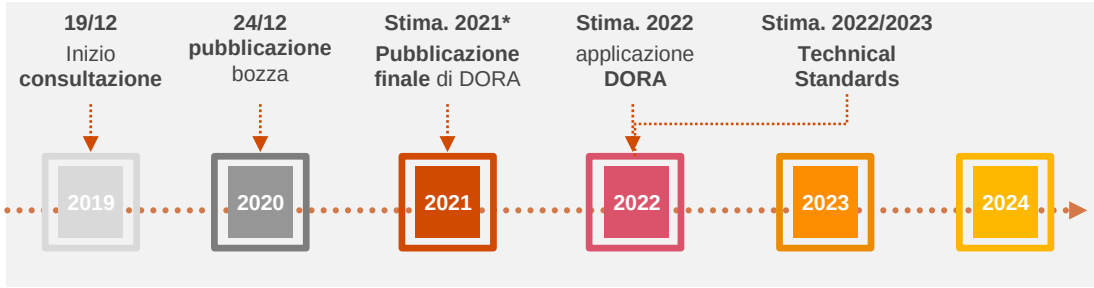
DORA: UNA PRIORITÀ PER IL MERCATO FS

Il Regolamento richiede importanti attività di adeguamento in ambito tecnologico, estendendo l'applicabilità a tutti i soggetti del Mercato FS e relative Terze e Quarte Parti.:

- **migliorare** e **semplificare** la condotta delle entità finanziarie nella **gestione del rischio ICT**
- stabilire meccanismi di **verifica** dei sistemi ICT
- aumentare **l'awareness** delle autorità di vigilanza sui **rischi** informatici/cyber e sugli **incidenti** legati alle TIC
- Introdurre **nuovi poteri per le autorità di vigilanza** finanziaria per sorvegliare i rischi derivanti dalla dipendenza delle entità finanziarie da fornitori di servizi ICT di terze parti

DORA rappresenta una profonda novità in ambito tecnologico, riflesso dell'interesse del Regolatore nel **normare aspetti precedentemente non inclusi**, quali la Resilienza tecnologica e il rafforzamento del presidio degli Outsourcer tecnologici.

ITER LEGISLATIVO



** Stima basata su un'accelerazione del periodo di finalizzazione standard di 18 mesi*

APPLICABILITA'

Il regolamento si applica a circa **22.000 società** **in ambito FS** e fa parte di un più ampio pacchetto di finanza digitale europea, oltre ad integrarsi con la regolamentazione della strategia Europea in ambto Cybersecurity (NIS).

Il perimetro di applicabilità DORA ricomprende le **entità del settore finanziario tradizionale** come istituti di credito, borse e stanze di compensazione, **gestori di fondi** alternativi, compagnie di **assicurazione**, istituti di pagamento, istituti di moneta elettronica, nonché fornitori di servizi di **criptovaluta**, emittenti di **cripto-asset** ed emettenti di **token**.

Pillar DORA ed impatti per il settore bancario (1/2)

1

GOVERNANCE AND INTERNAL STRUCTURE

- Ruolo dell'**organo di amministrazione**
- Formazione specifica / **Digital Training** per il **Top Management**
- Empowerment delle **responsabilità** per le funzioni **ICT/Cyber**
- **Monitoraggio rischio ICT/Cyber**
- **Reporting continuo** da parte delle funzioni ICT/Cyber sugli **incidenti** e **soluzioni** di rimedio

2

ENFORCE THE ICT RISK MANAGEMENT

2 Livello

- Politiche, Framework e processi di valutazione e gestione del **rischio ICT/Cyber come rischio operativo**
- Definizione di **impact tolerances**, scenari ed **integrazione RAF** (approvazione dell'organo di gestione)
- **Revisione / aggiornamento annuale** o in caso di incidenti

1 Livello

- **Misure tecniche ed organizzative** per protezione e la prevenzione dai rischi ICT/Cyber
- **Threat analysis** & scenario management
- **Monitoraggio predittivo** e **early detection** delle anomalie (incl. test analysis)
- **Continuous improvement**, **root cause** e incident **post-mortem analysis**
- **BC**M, **DR**M, **back-up** strategy

3

INCIDENT REPORTING

- Definizione ed implementazione di processi e procedure per **monitorare, gestire e registrare** gli **incidenti ICT/Cyber**
- **Classificazione** degli incidenti sulla base di **soglie di rilevanza** definite dalle Autorità
- **Segnalazione** alle **autorità** competenti dei soli incidenti TIC sulla base della gravità
- **Trasparenza al mercato**
- Strategie e processi di **comunicazione interna/esterna**

Pillar DORA ed impatti per il settore bancario (2/2)

4

DIGITAL RESILIENCE TESTING

Istituzione, mantenimento ed esecuzione periodica di un **programma di test di resilienza operativa digitale** che tenga conto del profilo di rischio dell'istituto finanziario, includendo:

- valutazioni e scansioni di **vulnerabilità**,
- analisi **open source**
- valutazioni della **sicurezza della rete**
- valutazioni **sicurezza fisica**
- **Threat-led Penetration Testing** su base triennale

5

TPRM, MANAGEMENT & AGREEMENTS

- Adozione, nell'ambito dell'ICT/Cyber Risk Framework, di una **strategia per** il **monitoraggio** e la **gestione dei rischi** derivanti da **fornitori di servizi ICT/Cyber** di terze parti
- Inclusione di **clausole standard nei contratti** con fornitori terzi di servizi ICT/Cyber
- **Mantenimento** e **aggiornamento** di un **registro** con informazioni su tutti gli accordi con fornitori terzi di ICT
- Monitoraggio dello stato di implementazione

6

INFORMATION SHARING

Programma (su base volontaria) di **condivisione di informazioni** relative a **minacce informatiche** all'interno della **community** delle **entità finanziarie** soggette DORA al fine di:

- migliorare la **resilienza operativa** digitale del mercato europeo FS
- aumentare la **consapevolezza** delle minacce informatiche
- **contenere la diffusione** delle minacce informatiche
- **rafforzare le capacità di difesa** delle entità finanziarie

7

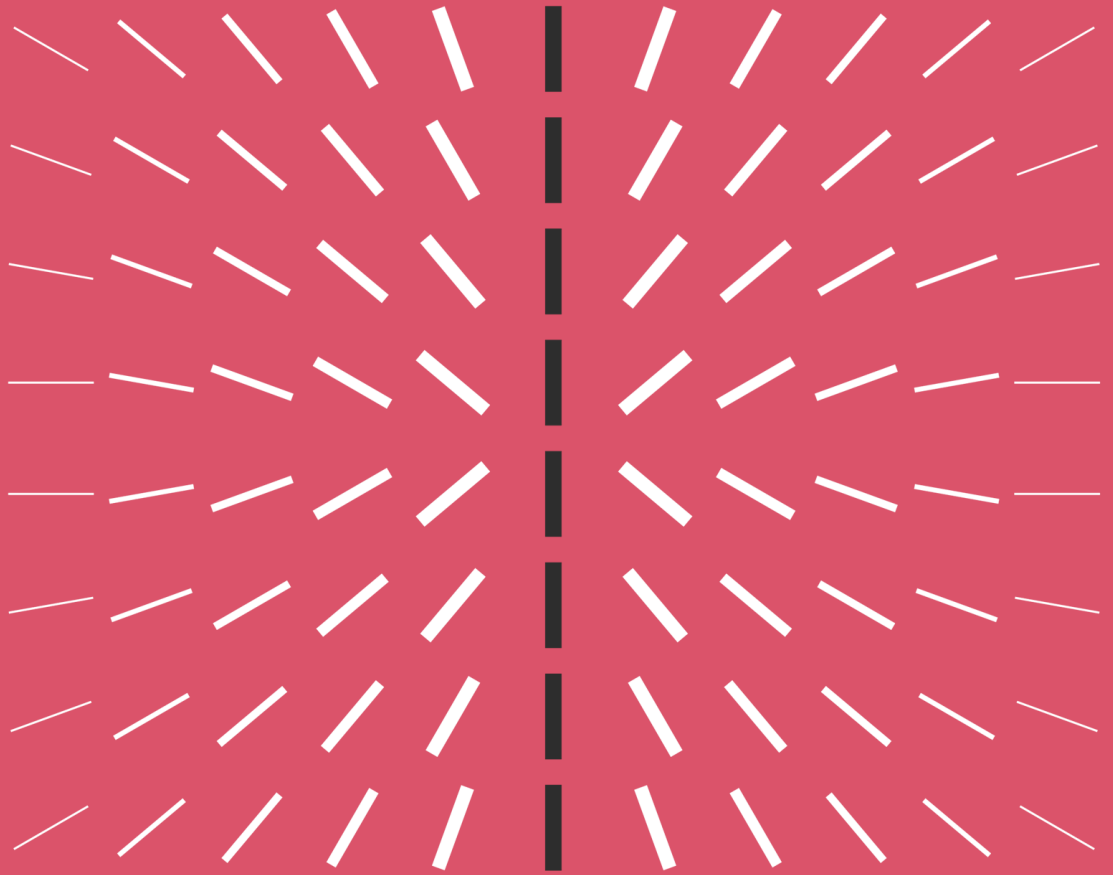
COMPETENT AUTHORITIES

Le AEV, attraverso Comitati congiunti e in collaborazione con le Autorità Competenti, la BCE e il CERS, possono introdurre meccanismi di **condivisione di pratiche efficaci** e di meccanismi **esercitazione** a livello EU per:

- migliorare la **situational awareness** ed identificare **rischi e vulnerabilità** informatici **comuni** a tutti i settori
- promuovere la **cooperazione** tra diversi settori
- consentire lo **scambio di pratiche di vigilanza**
- sviluppare **canali di comunicazione** e **promuovere modalità di risposta coordinata** a livello UE

2

DORA: le sfide per gli operatori bancari



DORA richiede il rafforzamento Security Risk, Governance ed Operations

Risk Management

- Modello Operativo, ruoli e responsabilità 1 e 2 Livello di Controllo
- Integrazione Rischi Operativi, ICT/Cyber e TPRM: RAF ed impact tolerances
- Business View
- Threat analysis e valutazioni scenario-based
- Monitoraggio, reporting e strumenti

Security Governance

- Cybersecurity Maturity & Strategy
- Cybersecurity Culture & Awareness
- Modello dei Controlli (1.5 Livello)
- Reporting e Comunicazione

Security Operations

- Identity Governance, Access Management & Zero Trust Architecture
- Network Security Segmentation
- EDR technolgies
- Threat-led Cyber Incident Testing

Cyber Incident Mangement

- Misure predittive
- Trend e test analysis
- Post-incident review
- Procedure e Cookbook
- Comunicazione

Gestione IIIe e IV Parti

- Strategia e Policy
- TPRM
- Clausole contrattuali
- Controlli IIIe e IV parti
- Correlazione processi
- Monitoraggio e auditing

BCM, DR & Emergency

- Strategia e policy ICT disruption
- Integrazione BIA/ Impact tolerances
- Estensione scenari
- Misure di contingency
- Scenario-based test methodology
- Comunicazione

Fix the Basis

Security Baseline	ICT Service Management	Capacity Management	CMDB & Configuration Management	Change Management

DORA: le sfide per gli operatori bancari

Points for Management Attention

Mandato Operativo Digitale

Istituire un mandato operativo digitale con una forte sponsorizzazione del Top Management

Gestione dei Rischi

Comprendere chiaramente i rischi sottostanti e stabilire un'adeguata propensione al rischio

Oltre la Business Continuity & IT

Partire da un approccio End-to-End basato sui Business Services

Modello Operativo Integrato

Costruire un modello operativo forte e integrato, con obiettivi di controllo e KPI per il monitoraggio del programma

Customer View

Tener conto del punto di vista del Cliente per identificare ciò che è più importante

Evolvere il Modello AS-IS

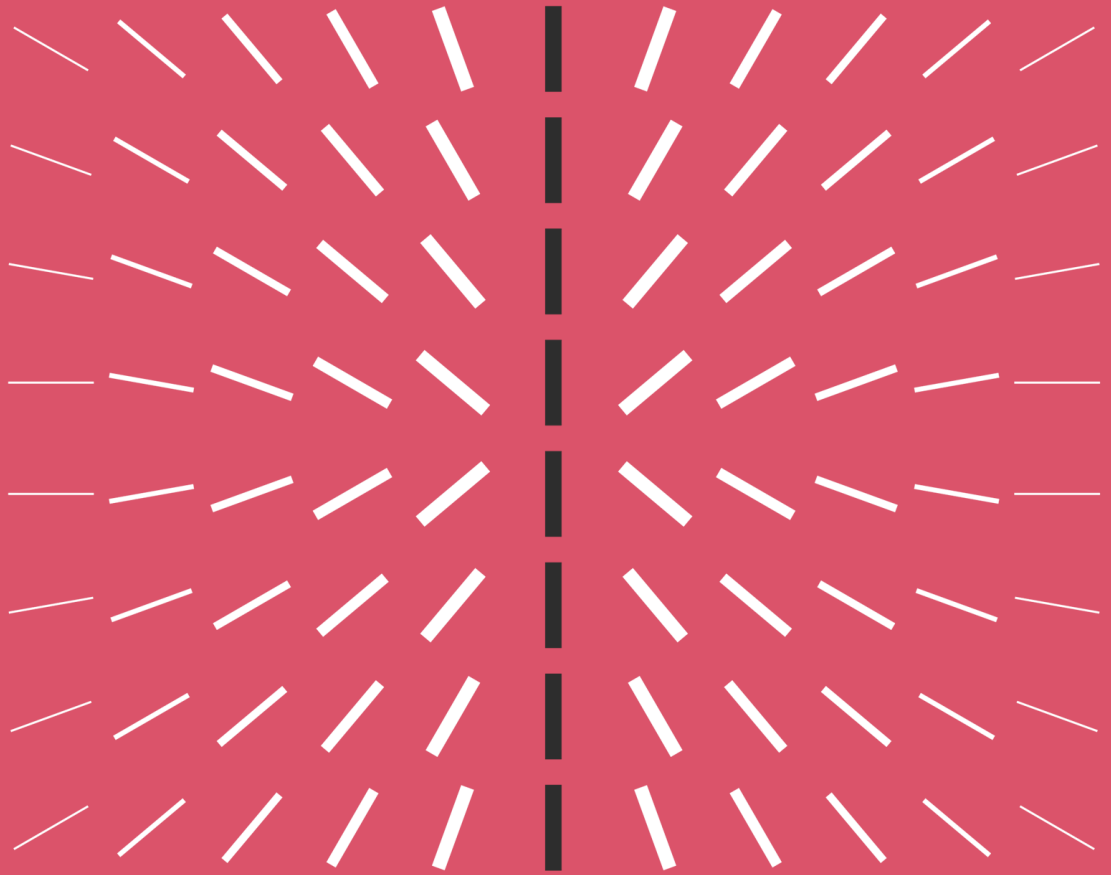
Rimediare alle attuali lacune sulla Resilienza Operativa Digitale, facendo leva su un approccio di miglioramento continuo

Non reinventare la ruota

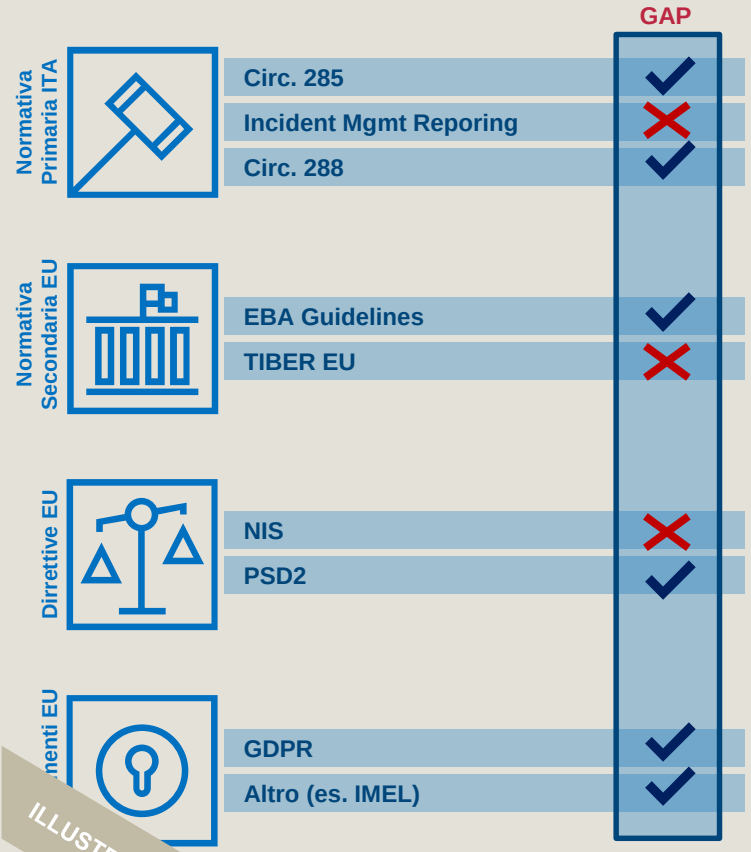
Le fondamenta del modello Digital Operational Resilience dovrebbero essere già presenti nell'Organizzazione

3

Priorità per la Digital Operational Resilience Journey



Priorità per la Digital Operational Resilience Journey



ILLUSTRATIVO

1 Digital Operational Resilience Maturity Assessment

2 Prioritizzazione e definizione del Programma DOR

3 Definizione modello operativo e Framework per la gestione dei Rischi

4 Business Case ed esecuzione Pilota

Framework Enhancement

5 DOR Embedment

Process Enhancement

www.pwc.com/it

190624-142613-AS-OS