Regolamento DORA: impatti del regolamento e stato dell'arte del mercato FS

Incontro Acorà
luglio 2023

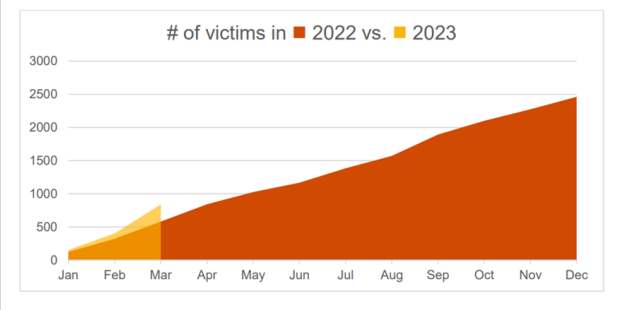
pwc

Agenda

- **Regolamento DORA e roadmap regolamentare: stato dell’arte e prossime milestone**
- **La vista di mercato Italiana ed EU per gli adempimenti DORA**
- **Implementazione del Programma DORA: sfide ed opportunità comuni**
- **L’evoluzione delle pratiche di Vigilanza in ambito Digital Resilience ed il confronto con il mercato Banking**

Premessa: Cyber Resilience e impatto degli attacchi Ransomware

RANSOMWARE



2462 victims leaked in 2022

- Data recovery: spesso è possibile **ripristinare solo in parte** i dati cifrati.
- Il ripristino dei dati da file di backup e di recovery: **può richiedere settimane.**
- Tecniche di attacco: I threat actors **evolvono le tecniche** in funzione delle soluzioni di sicurezza.
- Tempo medio di interruzione: **3 settimane** con conseguente:
  - Perdita di business,
  - Costo delle remediation,
  - Danno reputazionale,
  - Costi legali e sanzioni in caso di violazione dei dati personali

World Economic Forum: The Global Cyber Outlook 2023

Un **evento Cyber catastrofico** è almeno in qualche modo **probabile nei prossimi due anni**.

*L'**instabilità geopolitica globale** ha contribuito a sensibilizzare i leader aziendali e informatici sull'**importanza della gestione del rischio informatico**. Un **evento Cyber catastrofico** è almeno in qualche modo **probabile nei prossimi due anni**.*

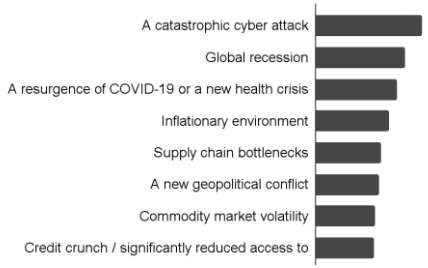
Per aumentare la Resilience, le aziende possono:

- *migliorare le **competenze informatiche** e la consapevolezza,*
- *la **comunicazione***

PwC 2023 Global Digital Trust Insights

Un **evento Cyber catastrofico** è lo **scenario maggiormente temuto** nel 2023 secondo 3,522 chief in ambito business, technology e security.

***PwC ha raccolto** attraverso interviste il punto di vista di CEO, CIO, CISO per comprendere meglio le priorità in tema di Cybersecurity & Privacy e i trend evolutivi tra prima e seconda linea di difesa*



Financial Times - 10 marzo 2023

La ECB lancerà "uno **stress test tematico** sulla resilienza informatica" su tutte le 111 banche che vigila.

***La Banca centrale europea** ha avviato in questi giorni una nuova campagna di Stress Test nella quale chiederà a tutti i principali istituti finanziari della zona euro **di dettagliare** entro il prossimo anno come risponderebbero e si riprenderebbero da un attacco informatico riuscito. **La BCE ha quindi pianificato a partire da gennaio 2024 "uno stress test tematico sulla resilienza informatica"** progettato per fornire "una migliore comprensione della dove sono i punti di forza e di debolezza delle banche".*

ECB Banking Supervision: SSM supervisory priorities for 2023-2025

Rafforzare la Resilience del sistema finanziario è tra le priorità ispettive di ECB.

***L'IT Continuity** è stato inserito tra gli argomenti prioritari di **ispezione da parte dell'Autorità** di Vigilanza in vista dell'adozione di quanto previsto dal Regolamento DORA*

DORA – Contesto ed impatti per il mercato Financial Services

Da più di 2 anni PwC segue l'evoluzione del **Regolamento DORA nel contesto del Digital Finance Package europeo**.

Tale Regolamento presenta **interazioni** con l'attuale **normativa di settore**, nonché **impatti** per il settore dei **Financial Services** e per la relativa **filiera tecnologica**, in considerazione delle sue specificità in termini di gestione dei **rischi ICT/ Cyber e Terze Parti**.

Di seguito riportiamo una **sintesi degli aspetti che riteniamo più rilevanti**:

- **La normativa europea contribuisce attivamente ad aumentare il livello di resilienza del settore FS:**
  “The regulatory umbrella above the world of technology and data is expanding rapidly, bringing previously “wild” sectors under increasingly heavy supervisory scrutiny and control[1]”
- **Adottare un approccio resiliente è l'unico modo per affrontare il contesto attuale**
  “A catastrophic cyber attack is the top scenario in 2023 resilience plans. Such an attack would surely put C-suite alliances to the test.”
- **I rischi Cyber non sono mai stati tanto importanti per il business**
  “Two-thirds of executives consider cybercrime their most significant threat in the coming year. Cybercriminals, increasingly using off-the-shelf tools, can perpetrate and orchestrate a variety of attacks[2]”
- **DORA richiede un approccio multidisciplinare con requisiti complessi che richiedono un forte commitment aziendale tra Risk, Cyber, IT e Legal il cui coordinamento ideale dovrebbe prevedere una sponsorship a livello cross-direzionale**
  “The essence of DORA is divided across 5 core pillars that address various aspects or domains within ICT and cyber security, providing a comprehensive digital resiliency framework for the relevant entities.”
- **Il mercato FS sta vedendo numerose iniziative volte non solo alla compliance a DORA, ma soprattutto alla gestione dei nuovi rischi cyber e IT con approcci volti all'operational resilience e ad una governance integrata**
- **DORA estende lo scope tradizionale dei rischi ICT/Cyber ad aree di rischio nuove ed emergenti** (e.g. concentrazione di terze parti, rischio della catena di fornitura, perdita di dati), **introducendo i concetti di servizio end-to-end e scenario per una visione olistica dei rischi tangibili con, al contempo, un framework per la protezione e reazione concreta dagli stessi**

1 Fonte: 2022 PwC Regulation of Technology report (TechReg)
2Fonte: 2023 PwC Global Digital Trust Insights

DORA: Roadmap Regolamentare

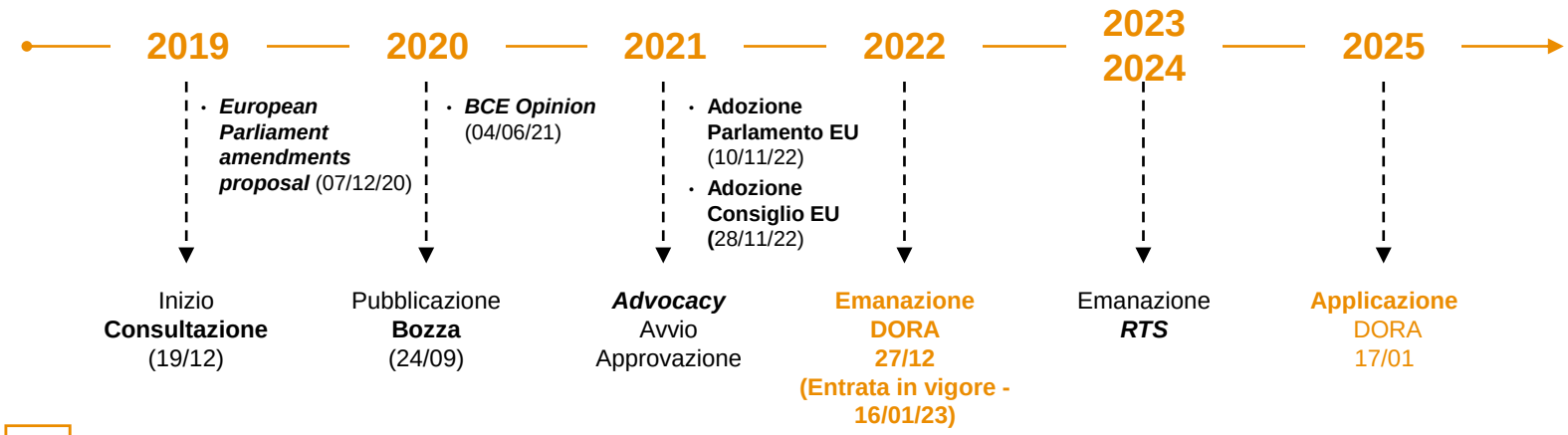
Il carattere fondante della proposta di regolamento UE DORA: un big bang della cyber security per il sistema finanziario comunitario, con obiettivi comuni sfidanti. Un effetto di istantaneo innalzamento dello standard regionale, che rende il sistema finanziario comunitario più forte e con ricadute anche globali.

Fonte: «Dati e finanza: nuove opportunità e nuove vulnerabilità. La necessità di cambiare paradigma»
Paolo Ciocca, Commissario Consob, 18 novembre 2020

Applicabilità

- Il Regolamento si applicherà a circa **22.000 entità** in ambito ***financial services***
- Il perimetro di applicazione DORA ricomprende le **entità del settore finanziario tradizionale** come **istituti di credito**, **borse** e **stanze di compensazione**, gestori di **fondi alternativi**, **società di gestione**, imprese di **assicurazione**, **istituti di pagamento**, istituti di **moneta elettronica**, nonché **fornitori** di **servizi di cripto-valuta**, **emittenti** di ***cripto-asset*** ed emettenti di ***token***

Iter legislativo



Pillar DORA

2 ***Digital Operational Resilience Governance***

2 ***End-to-end ICT & Cyber Risk Management***

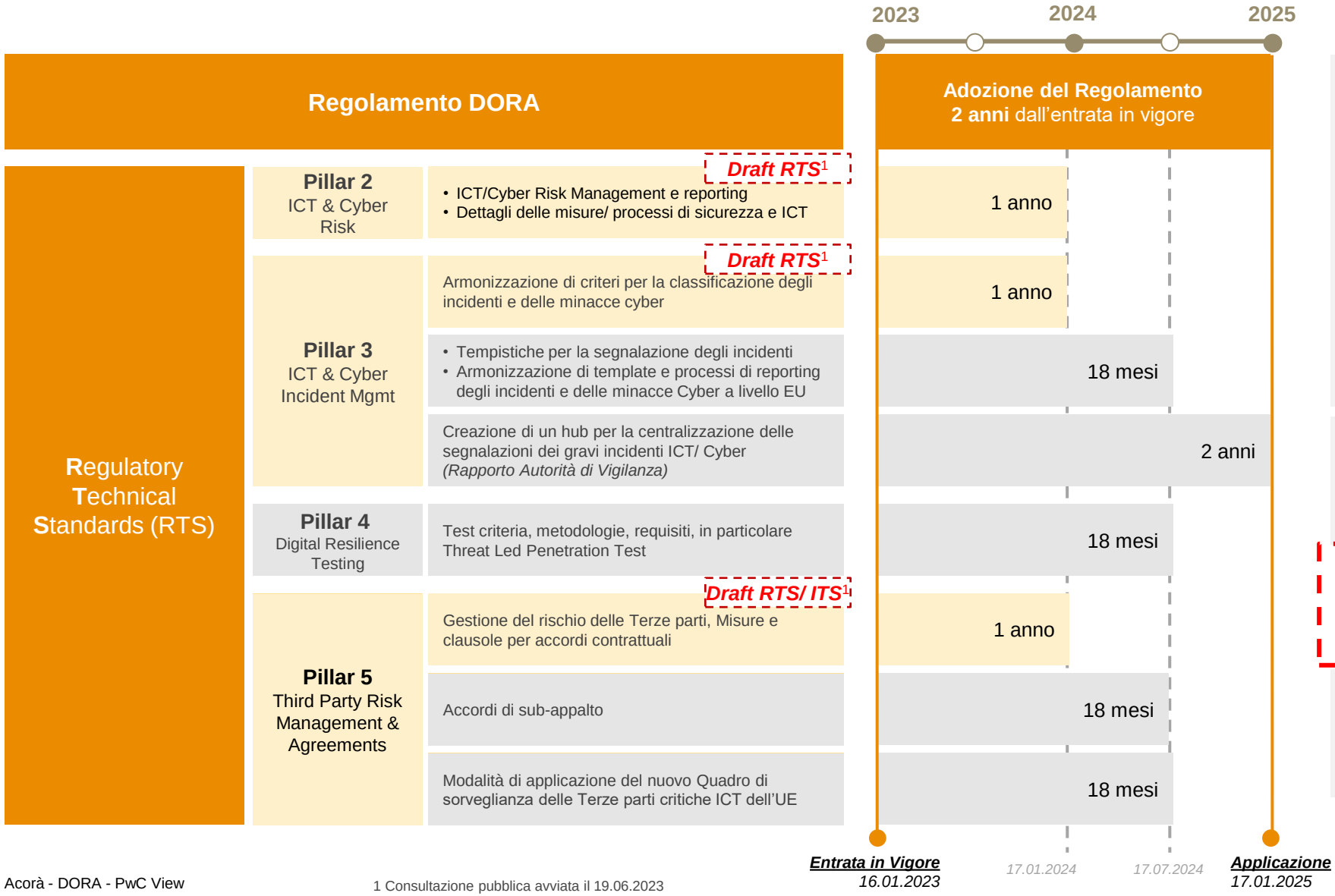
3 ***ICT & Cyber Incident Management***

4 ***Digital Resilience Testing***

5 ***ICT Third Party Risk Management***

6 ***Information Sharing***

Le tempistiche di applicazione



Il Regolamento DORA specifica che fino a quando le RTS non saranno dettagliate e pubblicate, gli Enti Finanziari devono fare riferimento ai seguenti regolamenti e linee guida come standard di riferimento:

- **ESA** (European Supervisory Authority) **Guidelines: EBA; EIOPA, ESMA**.
- **TIBER EU**, con specifico riferimento al Pillar 4 - Digital Resilience Testing.

Focus: *Timeline* di emanazione RTS

Data di emanazione	Consultazione pubblica	Approvazione Comm. EU
17.01.24	Giu/Lug 23 ▼ 15 Set 23	Dicembre 23
17.07.24	Nov 23 ▼ Feb 24	Maggio 24

1 Consultazione pubblica avviata il 19.06.2023

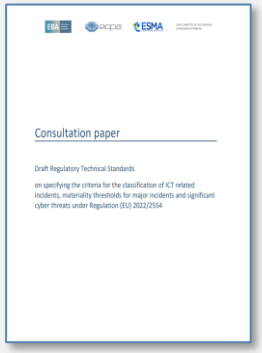
Focus: gli RTS in consultazione

***Draft RTS** to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16 (3) of Regulation (EU) 2022/2554*

- Maggiori specifiche in ambito Governance, Organizzazione ed ICT Risk Management
- Nuovi requisiti di dettaglio per I processi, procedure, protocolli e le tecnologie ICT, Cyber (es. Data & System Security, Vulnerability & Patching, ….), Incident, BCM, ICT continuity
- Applicazione del framework semplificato (proporzionalità): Governance; Organization; ICT Risk Management, requisiti di Sicurezza, ICT, BCM e per la mappatura dei servizi aziendali E-2-E
- Struttura e contenuti del report annuale in ambito ICT Risk Management

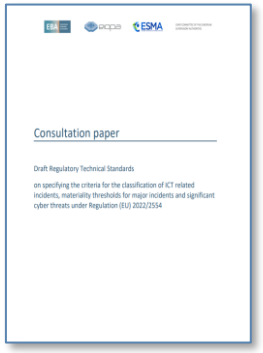
***Draft RTS** on specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under Regulation (EU) 2022/2554*

- Processo per la classificazione degli incidenti, da calare nelle procedure aziendali
- Descrizione qualitativa e definizione delle soglie qualitative dei criteri di classificazione degli incidenti
- Modalità di applicazione pan-europea
- Modalità di reporting per incidenti ricorrenti



***Draft RTS** to specify the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers as mandated by Regulation (EU) 2022/2554*

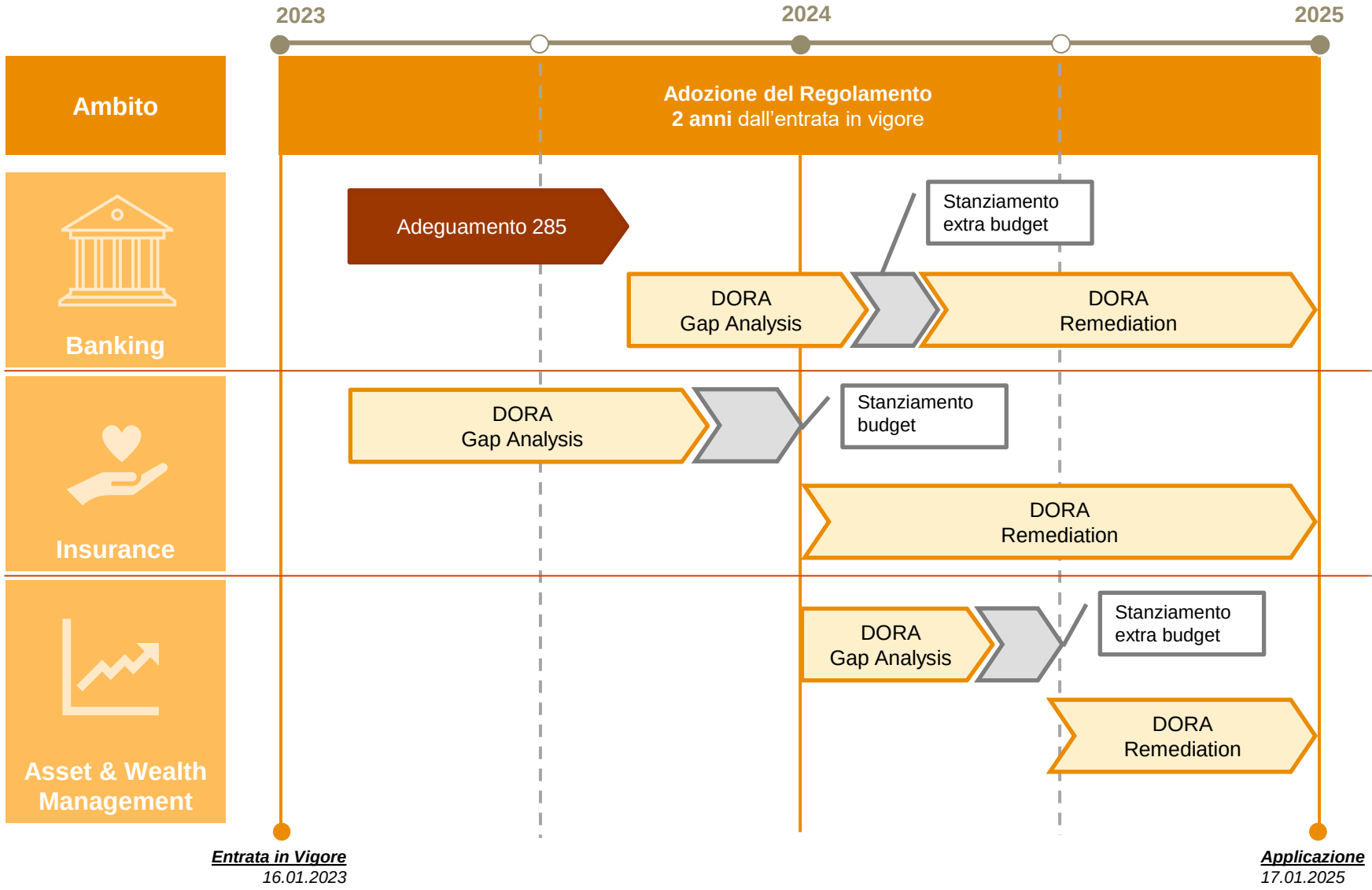
- Ruoli, responsabilità e requisiti per le diverse fasi del ciclo di vita delle terze parti fornitrici di servizi ICT
- Maggiore specifica di ulteriori requisiti in ambito:
  - Due diligence
  - Valutazione dei conflitti di interesse
  - Clausole contrattuali
  - Controlli e Monitoraggio durnate il rapporto contrattuale
  - Exit strategy



***Draft ITS** to establish the templates composing the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers as mandated by Regulation (EU) 2022/2554*

- Struttura del registro delle informazioni per le terze parti a livello di LE
- Struttura del registro delle informazioni per le terze parti a livello subconsolidato e consolidato
- Ruoli, responsabilità e processi di manutenzione / aggiornamento per le LE, subhoding ed holding
- Template del registro delle informazioni per le terze parti, identificativi e descrizione dettagliata dei singoli campi

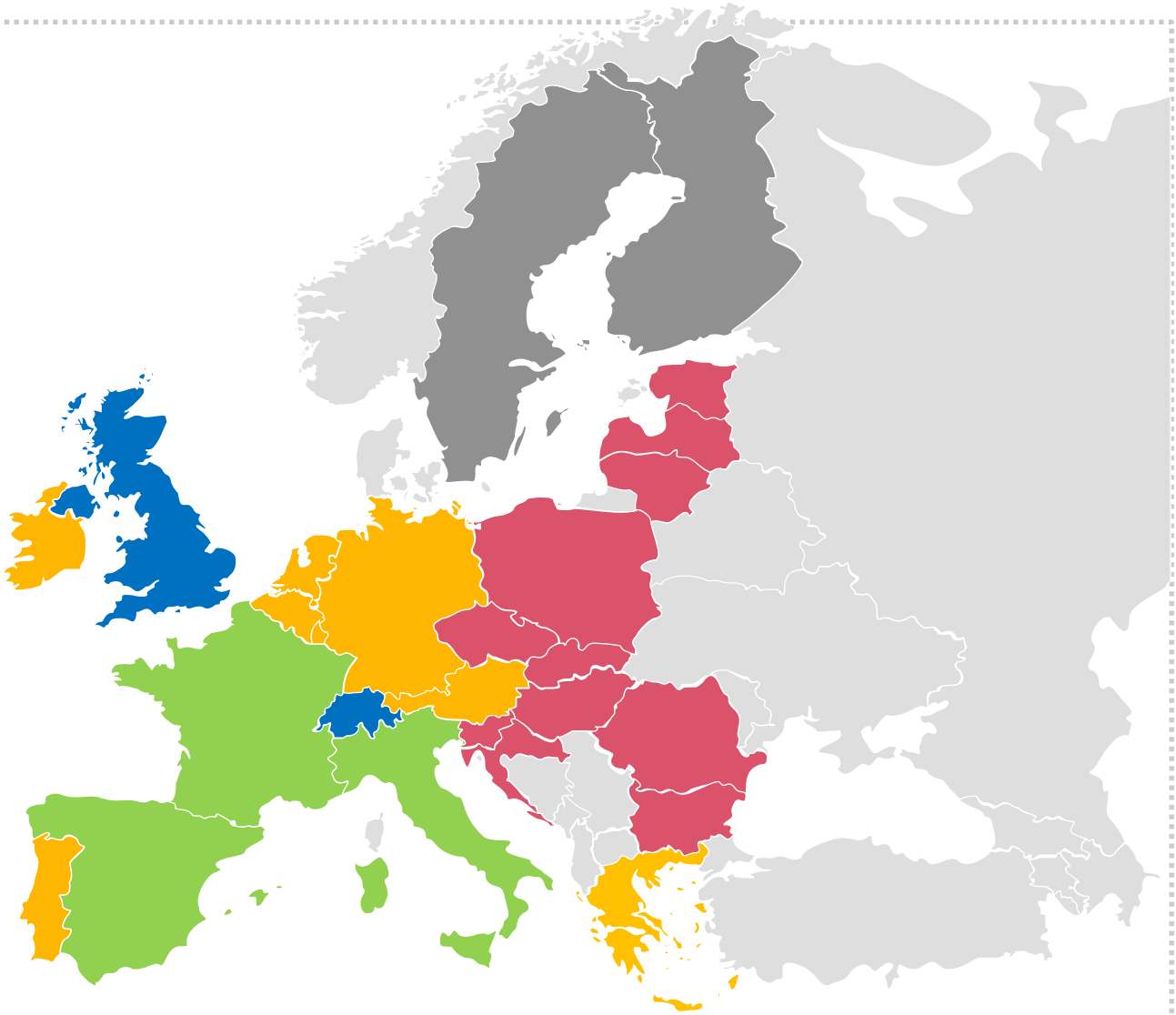
Stato dell'arte e peculiarità del mercato FS in Italia …



- **L'adeguamento al 40mo aggiornamento della 285** ha anticipato alcuni temi organizzativi in linea con quanto previsto da DORA ma ha anche **procrastinato le attività di gap analysis** e di definizione dei piani di remediation. In molti casi i risultati degli assessment potrebbero arrivare successivamente al processo di budgeting con **possibili ritardi nell'implementazione delle misure**
- **Gap analysis DORA attivate già dai primi mesi del 2023** (in alcuni casi anche prima) con la possibilità di **pianificare gli investimenti per il 2024 in linea con i processi di budget ordinari**, assicurando così una corretta pianificazione delle attività implementative nel 2024. I **tempi sono comunque molto sfidanti** per gli adeguamenti. L'analisi degli RTS integrerà la pianificazione delle attività in modo dinamico.
- **Una ridotta sensibilità verso il DORA** comporta mediamente un **ritardo di oltre 6 mesi rispetto all'attivazione delle attività di Gap Analysis**. Ciò comporta una **maggiore complessità** da gestire per l'esecuzione delle **iniziative di remediation** entro la scadenza del provvedimento. Diverso il caso di Gruppi Bancari o Assicurativi con rami di business che includano l'Asset & Wealth Management. In questi casi le pianificazioni sono quelle della parent company

… mantenendo la vista Europea

PwC si impegna nel **mantenere, aggiornare** ed **estendere** costantemente un benchmark che coinvolge un **panel internazionale** di **organizzazioni** sia **pubbliche** che **private**, operanti nell'ambito dei **Financial Services**, supportando i clienti nell'identificazione di **aree** di **miglioramento** e nell'**indirizzo** di **iniziative** all'interno di Programmi strategici pluriennali.



- AREA **MEDITERRANEA**
- AREA **CENTRALE**
- AREA **SETTENTRIONALE**
- **CEE** COUNTRIES
- **UK**
- **SVIZZERA**

Sponsorship e coinvolgimento funzioni aziendali

- Le principali **funzioni aziendali impattate** della Regolamentazione DORA risultano essere l'Organizzazione/Operations, la Sicurezza Informatica e Risk Management
- Il progetto di adeguamento ai requisiti DORA viene **tipicamente guidato dall'Area COO** (Organizzazione / Operations, Sicurezza Informatica); in alcune progettualità si rileva **co-ownership** nella guida del progetto fra **Area COO e Area CRO**
- Le funzioni **Compliance**, per il loro ruolo di trasversalità rispetto agli adempimenti del Regolamento DORA, a partire da Dicembre 2022 hanno avuto ruolo di promotore di iniziative di **endorsement cross-funzionali** e avvio **attività di Gap Analysis & Roadmap.**

DORA: Cosa Significa per *il mercato FS?*

Le peculiarità del Regolamento

Quick-win	Big Challenge	Innovation
X **Gap** Analysis	2 **Mappatura** dei **Servizi** e **filiera** tecnologica	4 **TIBER-EU / IT**
X **Remediation** Plan	2 Evoluzione modelli di gestione[2] in ottica **scenario-based**	2 Processi di **comunicazione automatizzata**
1 Assegnazione nuove **responsabilità** DORA	2 **Segregazione** della **Rete**	6 **Collaborazione** e sharing a livello di **mercato**
3 Processo di **Incident Mgmt**	2 Nuovi modelli di **protezione dei dati** (backup)	X **Dashboard** per il **governo integrato** dei Rischi ICT/Cyber
2 **Threat Intelligence**	2 **Implementa-zione** logiche **Zero-Trust**	
5 Revisione **contratti** delle **Terze Parti ICT**	5 **Negoziazione** e governo dei **contratti** con le **Terze Parti ICT**	
	5 **Gestione** delle **Terze Parti ICT**	

n Identificativo Pillar associato all'iniziativa

X Attività cross-Pillar

Punti di Attenzione Comuni

Governance e Responsabilità

- Responsabilità diretta del CdA gestione dei rischi ICT e Cyber lungo l'intera catena del valore (incl. terze parti).
- Necessità di definizione di nuove responsabilità ed accountability
- Rafforzamento delle Funzioni di Controllo in ambito Digital Resilience
- Introduzione di nuovi flussi informativi
- Rafforzamento competenze specialistiche ed upskilling

Strategia Digital Operational Resilience

- Nuovi strategia e framework, trasversali all'azienda, integrati con i processi esistenti
- Indicatori, monitoraggio, dashboarding

Visibilità End-to-End sulla value chain di erogazione dei servizi

- Mancanza di governance sui processi di integrazione e manutenzione delle informazioni
- Necessità di potenziare la governance della Supply Chain tramite TPRM e efficaci modelli di controllo

Adeguatezza degli investimenti per minacce concrete e rischi tangibili

Necessità di evolvere le valutazioni del rischio informatico per comprendere le minacce attuali e l'evoluzione degli scenari di rischio.

Sfide ICT e Cyber

- TLPT come Cyber Business Case
- Mapping, Configuration & Asset Management
- Governo dei sistemi EoL e Legacy Systems
- Segregazione della Rete
- Nuove Strategie e Tecnologie per Backup e Restore

Non solo DORA: Stress test in ambito Cyber Resilience

EIOPA

Cyber Stress Test

Discussion Paper on Methodologies of Insurance Stress Testing - Cyber component

Closing Date: 28 February 2023

Consultation paper on methodology for assessment of insurers' resilience under severe but plausible cyber incident scenarios, focusing mostly on their financial consequences and specifically on:

- **Cyber resilience,** intended as the capability of an insurance undertaking to sustain the financial effect of an adverse cyber-event. The economic impacts should be informed by more operational oriented data on a firm's capability to restore its operations at a sufficient level and in a time horizon which do not generate potential systemic effects on the financial sector and eventually to the real economy;
- **Cyber underwriting risk**, intended as the capability of an insurance undertaking to sustain the financial impact by a capital and solvency perspective of the materialization of an extreme but plausible adverse cyber scenario impacting the insurance coverages contained in the liability portfolios.

EBA (SREP add-on)

SSM Priorities 2023 - 2025

Targeted review on EU Banking Systems vulnerabilities - Operational resilience frameworks, namely IT outsourcing and IT security/cyber risks

July – August 2023

Within SSM supervisory priorities, ECB Banking is committed to focus their activities on prioritized vulnerabilities, including Operational resilience frameworks, IT outsourcing and IT security/cyber risks:

- **Specific assessment on Cyber**: **140** questions drilling down *identification, protection & prevention measures;*
- **SREP 2024**: targeted review will be feeding the outcome of the next SREP cycle, contributing to the supervisory priorities for 2024.

Targeted OSIs of outsourcing and cyber security management for EU Significant banks

2023 – 2025

Cyber Stress Test

ECB runs a stress test for SREP purposes once a year. For 2024, the ECB annual stress test will be a cyber resilience stress test

From January 2024

Estimation and reporting of impact and consequences of a cyber scenario, while assessing Banks capability to be operationally resilient in terms of emergency/contingency procedure activation and business operations restoring:

- **Stress test assessment based on a common pre-defined Cyber scenario: 450** questions drilling down *respond & recovery capabilities*
- **In-depth exercise** for **selected** EU significant banks, l**ighter assessment** for other EU significant banks;
- **SREP 2024**: cyber stress test outcomes will be feeding the 2024 SREP outcomes.

Stay Tuned

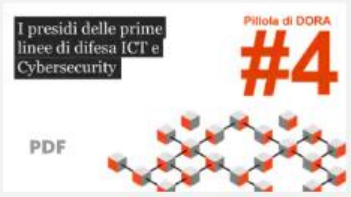
https://www.pwc.com/it/it/services/consulting/digital-operational-resilience.html

Governo e gestione delle Terze Parti

DORA si ispira ai principi TPRM nel presidio delle Terze Parti, introducendo inoltre nuovi poteri per le Autorità di Vigilanza

Digital Operational Resilience Testing

DORA definisce un programma onnicomprensivo di test di resilienza operativa digitale comprendendo gli aspetti Cyber ed inclusivo delle logiche Tiber EU.



I presidi delle prime linee di difesa ICT e Cybersecurity

Le Responsabilità delle 1e Linee di Difesa Cybersecurity ed ICT nel presidio End-to-End dei Rischi introdotto dal Regolamento EU DORA

La Gestione degli Incidenti ICT e Cybersecurity

DORA evolve la gestione degli incidenti IT e Cyber, richiamando le best practice, ed introducendo novità per la comunicazione e segnalazione alle Autorità.

Operational Resilience e le interconnessioni con il framework di Risk Management

Visione End-to-End del modello di Gestione dei Rischi Operativi, ICT e Cyber come game changer del Regolamento EU DORA.

Contesto di mercato ed implementazione del Regolamento

La view PwC sul contesto del Regolamento EU DORA, una priorità per i Financial Services date le novità in ambito Rischi Operativi, ICT e Cybersecurity.

Thank you

pwc.com/it