ABI Banche e Sicurezza 2024

Paolo Carcano
Partner PwC Italia, Cyber Security & Privacy FS

pwc

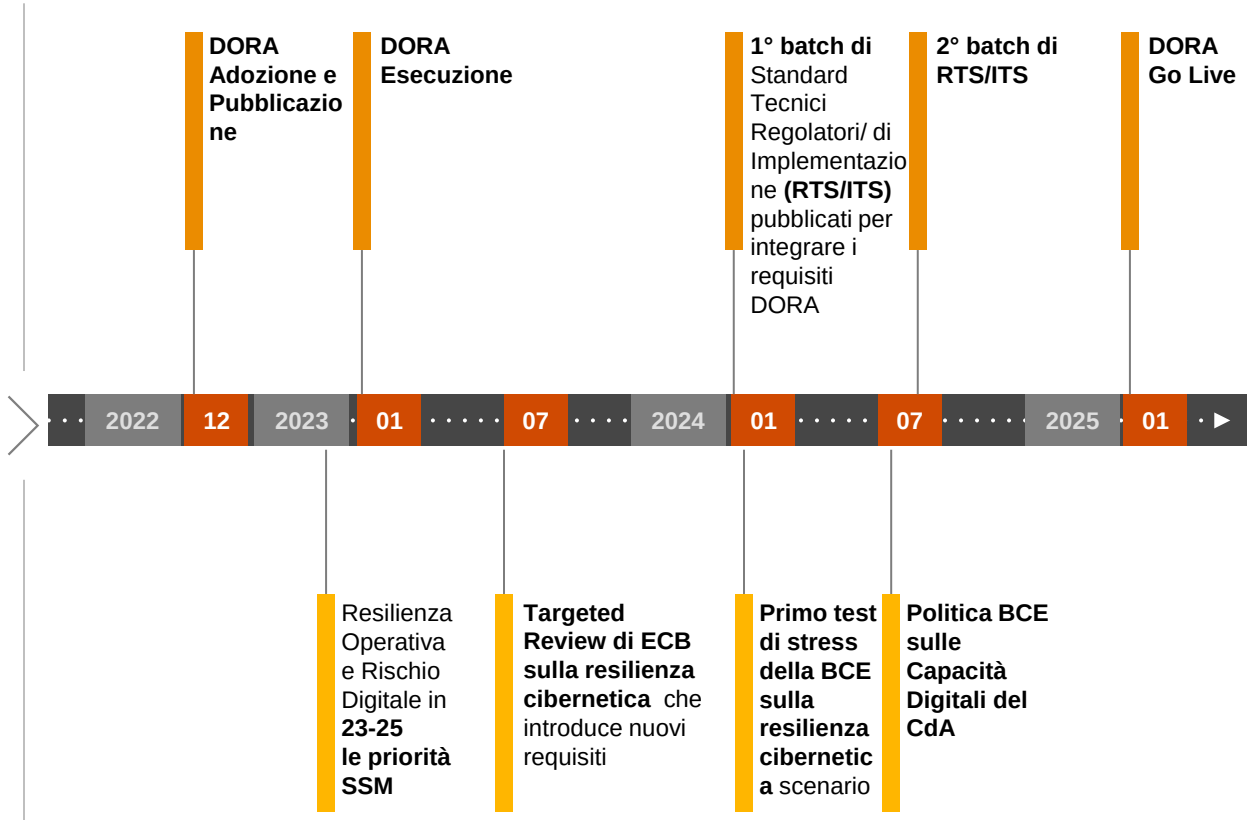
L'UE sta modificando il modo di affrontare i rischi digitali

Il settore FS avrà un ruolo chiave grazie a DORA e alle soluzioni di resilienza

Agenda Digitale UE

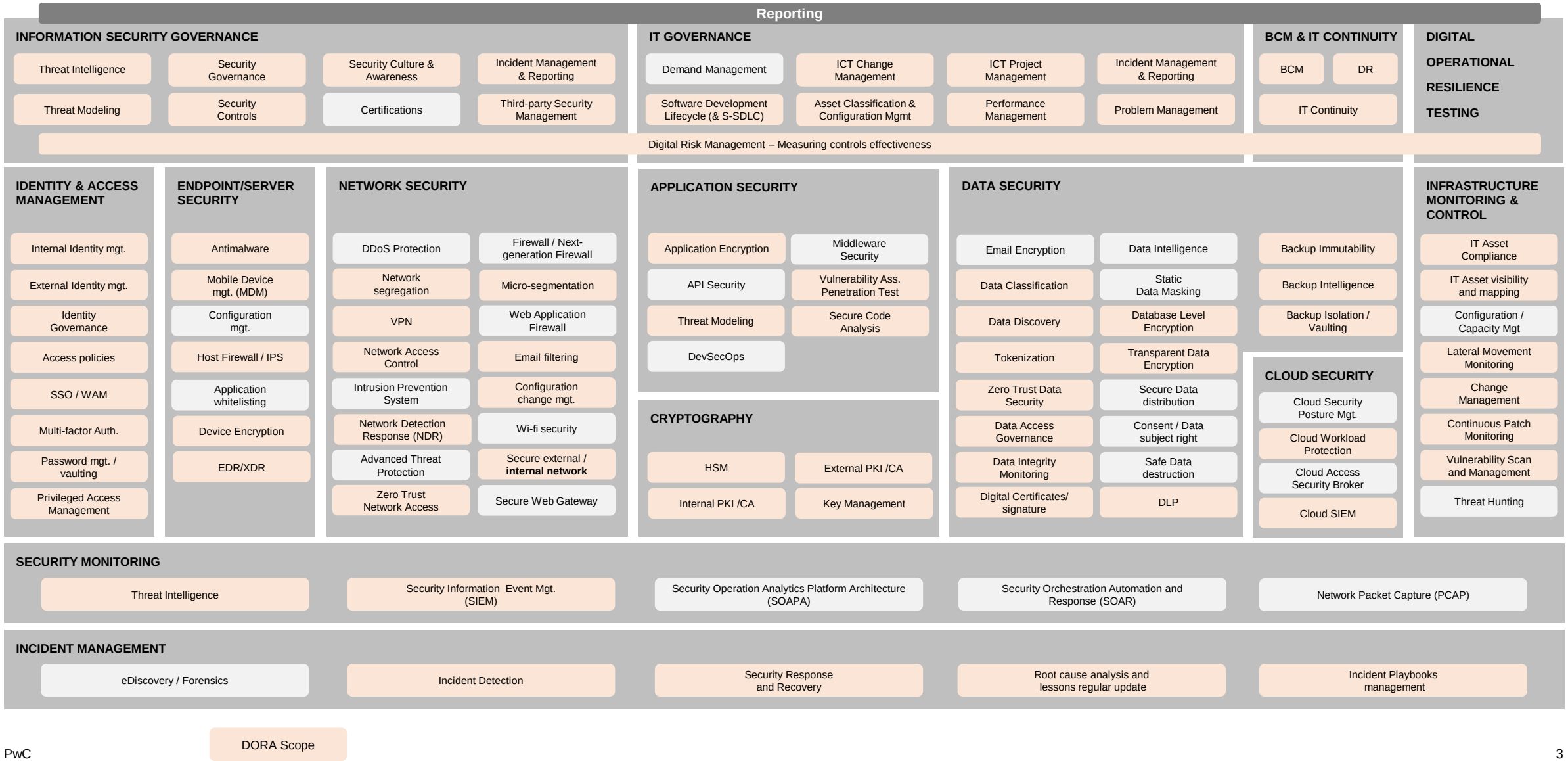
Argomenti Regolatori Chiave	Regolamentazione Pertinente
Resilienza Operativa & Digitale La resilienza operativa è una priorità definita in molti programmi dei regolatori finanziari in tutto il mondo e nelle priorità strategiche per il 2023. Rivedere la strategia di resilienza operativa permetterà di essere in linea con le aspettative in evoluzione dei regolatori e rafforzerà l'integrità del business nel suo complesso.	• **Legge sulla Resilienza Operativa Digitale (DORA)** • Legge sulla Resilienza Cibernetica • Direttiva NIS 2 • Critical Entities Resilience (CER) Directive
Governance e Protezione dei Dati Seguendone l'implementazione, la costante evoluzione in materia di GDPR è stata in linea con lo sviluppo dell'economia dei dati e gli standard di sicurezza necessari per proteggere i dati personali da accessi non autorizzati. Ulteriori iniziative normative sono concentrate sulla creazione di quadri per facilitare la condivisione dei dati e sui diritti di accesso e utilizzo dei dati.	• GDPR • Data Governance Act • Data Act
Intelligenza Artificiale L'IA e l'apprendimento automatico stanno crescendo in termini di complessità delle operazioni e ambito di applicazione. Rimangono diverse preoccupazioni relative al bias involontario o all'overfitting all'interno dei modelli di IA. In considerazione di questo, esistono una serie di strategie e modelli che intendono fornire chiarezza e supporto sia a chi implementa che a chi utilizza i sistemi di IA.	• Legge sull'Intelligenza Artificiale (AI) • Linee Guida Etiche sull'IA • Legge sulla Responsabilità dell'IA
Open Finance e Open Insurance I regolatori dell'UE stanno attualmente cercando di supportare il passaggio verso l'open finance basato sull'adesione ai principi antitrust, di protezione dei dati e dei diritti dei consumatori. L'UE cercherà di incentivare l'innovazione e la collaborazione in questo settore, mentre valuta se l'attuale legislazione e le strutture dell'UE supportano adeguatamente l'industria.	• Direttiva PSD3 • Direttiva FIDA sul Quadro dell'Open Finance • Piano d'Azione FinTech • Euro Digitale
Crypto e DLT Nel settore delle Crypto, l'UE cerca di fornire un chiaro quadro normativo per offrire stabilità e alimentare ulteriori progressi tecnologici nel settore. Per il DLT, un numero di iniziative e progetti pilota dell'UE sono in sviluppo per supportare la crescita e l'innovazione in questo settore di mercato.	• Regolamento sui Mercati di Crypto-Assets (MICA) • Tecnologia del Registro Digitale «DLT»

Concentrarsi sulle lenti del rischio digitale per i servizi finanziari dell'UE

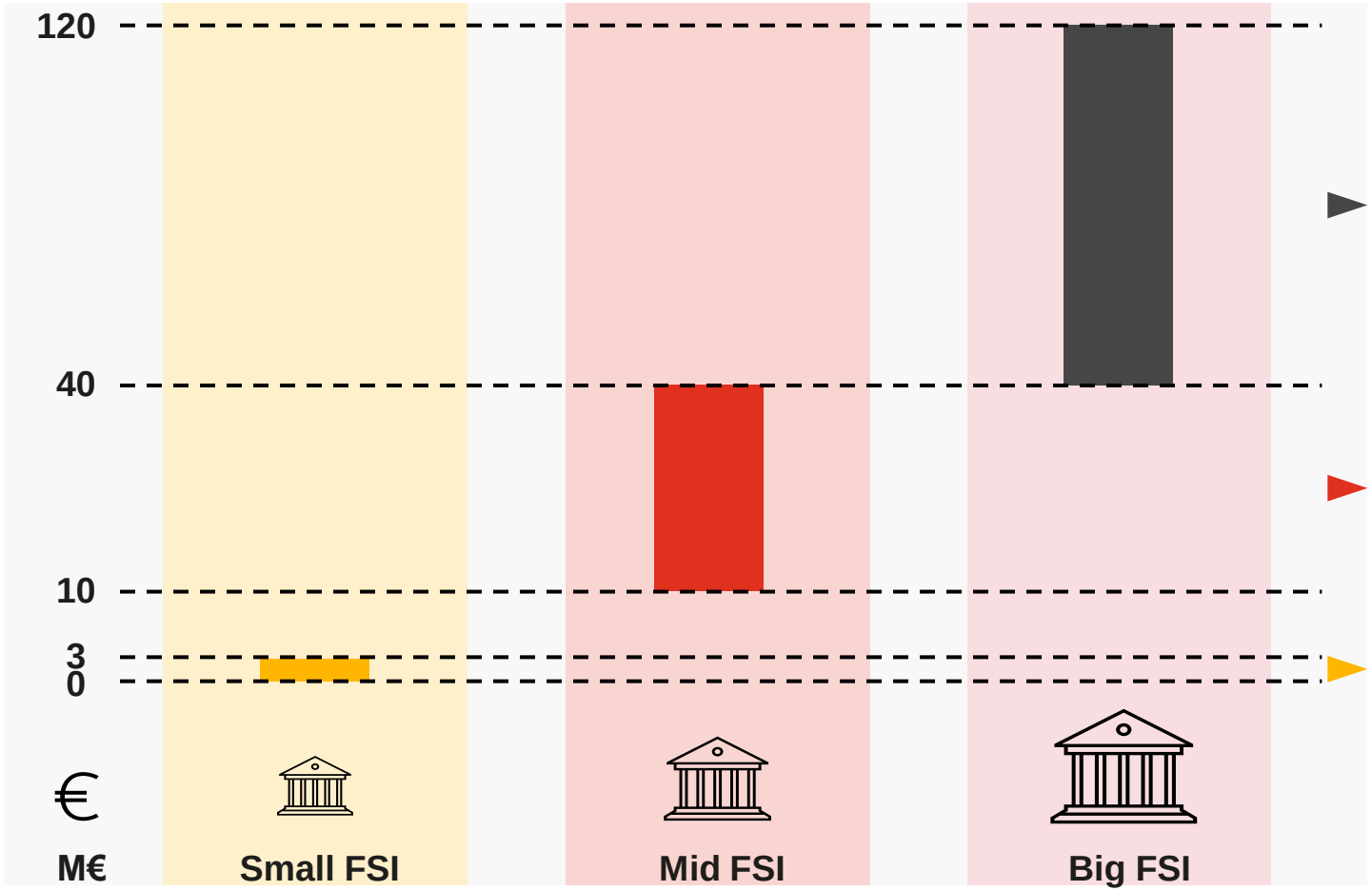


Il **2024 test di stress cibernetico della BCE ha** sfidato**le banche europee** con uno **scenario** di **interruzione del sistema centrale durante in media tre** giorni **, raggiungendo un picco fino a sette giorni**. Questo **scenario richiede** una profonda rivalutazione delle soluzioni di recupero, dove **le funzioni aziendali sono incaricate di definire nuove misure di contingenza capaci di tutelare gli interessi dei clienti. Ne consegue valutazioni d'impatto raggiungono** cifre economiche significative, contro le quali gli**investimenti** in **IT** e **cyber resilienza** richiesti da DORA trovano una profonda**giustificazione aziendale**.

Gli investimenti Cyber saranno guidati dalla Digital Resilience



Dal nostro osservatorio gli investimenti Cyber sono destinati a crescere proprio per completare il journey verso DORA



Ipotesi di spesa in 3 anni

Ipotesi di spesa in 3 anni

Ipotesi di spesa in 2 anni

Secondo quanto dichiarato da ECB il percorso delle banche europee è più tortuoso del previsto

Fonti informative analizzate da ECB

1 On Site Inspections (OSI)

- IT RISK
- Outsourcing
- Cloud
- Business Continuity
- IT Continuity

2 Self Assessment (Risk Questionnaire)

SUPERVISION NEWSLETTER

IT and cybersecurity: no grounds for complacency

15 Novembre 2023

1 IT Change Risk

2 IT Governance and risk management, with focus on **IT Asset** Management

3 Cyber and IT Security Risk

- **EoL** supporting Critical functions
- **Vulnerability** & **Patching**
- **Hardening**
- **Event monitoring**
- **Identity Management**
- **Network Security**
- **Backup management**
- **Data Classification**

Il Cyber Resilience Stress Test è un grande Table Top Exercise

AUSTRIA
- Addiko Bank AG
- BAWAG Group AG
- Erste Group Bank AG
- RaifCIFsen Bank International AG
- RaifCIFsenbankengruppe OÖ Verbund eGen
- Volksbank Wien AG

BELGIUM
- Belfius Banque SA ; Belfius Bank NV ; Belfius Bank SA
- Crelan SA ; Crelan NV
- Investeringsmaatschappij Argenta NV ; Société d'investissements Argenta SA ; Investierungsgesellschaft Argenta AG
- KBC Group NV
- The Bank of New York Mellon SA/NV

BULGARIA
- DSK Bank AD

CYPRUS
- Agri Europe Cyprus Limited
- Hellenic Bank Public Company Limited

SLOVENIA
- Nova Ljubljanska banka d.d., Ljubljana

FINLAND
- Danske Bank A/S, Finland Branch
- Kuntarahoitus Oyj
- Nordea Bank Abp
- OP Osuuskunta

FRANCE
- **BNP Paribas S.A.**
- BofA Securities Europe SA
- BPCE S.A.
- Bpifrance
- Confédération Nationale du Crédit Mutuel
- Crédit Agricole S.A.
- HSBC Continental Europe
- La Banque Postale
- RCI Banque SA
- SFIL S.A.
- Société Générale S.A.

LATVIA
- AS "SEB banka"
- AS "Citadele banka"
- Swedbank Baltics AS

GERMANY
- Bayerische Landesbank
- Citigroup Global Markets Europe AG
- COMMERZBANK Aktiengesellschaft
- DekaBank Deutsche Girozentrale
- Deutsche Apotheker- und Ärztebank eG
- Deutsche Bank AG
- Deutsche Pfandbriefbank AG
- DZ BANK AG Deutsche Zentral-Genossenschaftsbank
- Erwerbsgesellschaft der S-Finanzgruppe mbH & Co. KG
- Goldman Sachs Bank Europe SE
- Hamburg Commercial Bank AG
- HASPA Finanzholding
- J.P. Morgan SE
- Landesbank Baden-Württemberg
- Landesbank Hessen-Thüringen Girozentrale
- Morgan Stanley Europe Holding SE
- Münchener Hypothekenbank eG
- Norddeutsche Landesbank -Girozentrale-
- State Street Europe Holdings Germany S.à.r.l. & Co. KG
- UBS Europe SE
- Volkswagen Bank GmbH

LITHUAINA
- AB SEB bankas
- Akcinė bendrovė Šiaulių bankas

GREECE
- ALPHA SERVICES AND HOLDINGS S.A.
- Eurobank Ergasias Services and Holdings S.A.
- National Bank of Greece S.A.
- Piraeus Financial Holdings S.A.

IRELAND
- AIB Group plc
- BANK OF AMERICA EUROPE DESIGNATED ACTIVITY COMPANY
- Bank of Cyprus Holdings Public Limited Company
- Bank of Ireland Group plc
- Barclays Bank Ireland PLC
- Citibank Holdings Ireland Limited
- Ulster Bank Ireland Designated Activity Company

ITALY
- **Banca Mediolanum S.p.A.**
- **BANCA MONTE DEI PASCHI DI SIENA S.p.A.**
- **Banca Popolare di Sondrio, Società per Azioni (S.p.A.)**
- **Banco BPM S.p.A.**
- **BPER Banca S.p.A.**
- **Cassa Centrale Banca - Credito Cooperativo Italiano S.p.A.**
- **Credito Emiliano Holding S.p.A.**
- **FinecoBank S.p.A.**
- **Iccrea Banca S.p.A. - Istituto Centrale del Credito Cooperativo**
- **Intesa Sanpaolo S.p.A.**
- **Mediobanca - Banca di Credito Finanziario S.p.A.**
- **UniCredit S.p.A.**

LUXEMBOURG
- Atlantic Lux HoldCo S.à r.l.
- Banque et Caisse d'Epargne de l'Etat, Luxembourg
- Banque Internationale à Luxembourg S.A.
- LSF Nani Investments S.à.r.l.
- OTP Luxembourg S.à.r.l.
- Quintet Private Bank (Europe) S.A.
- RBC Investor Services Bank S.A.

MALTA
- Bank of Valletta plc
- MDB Group Limited

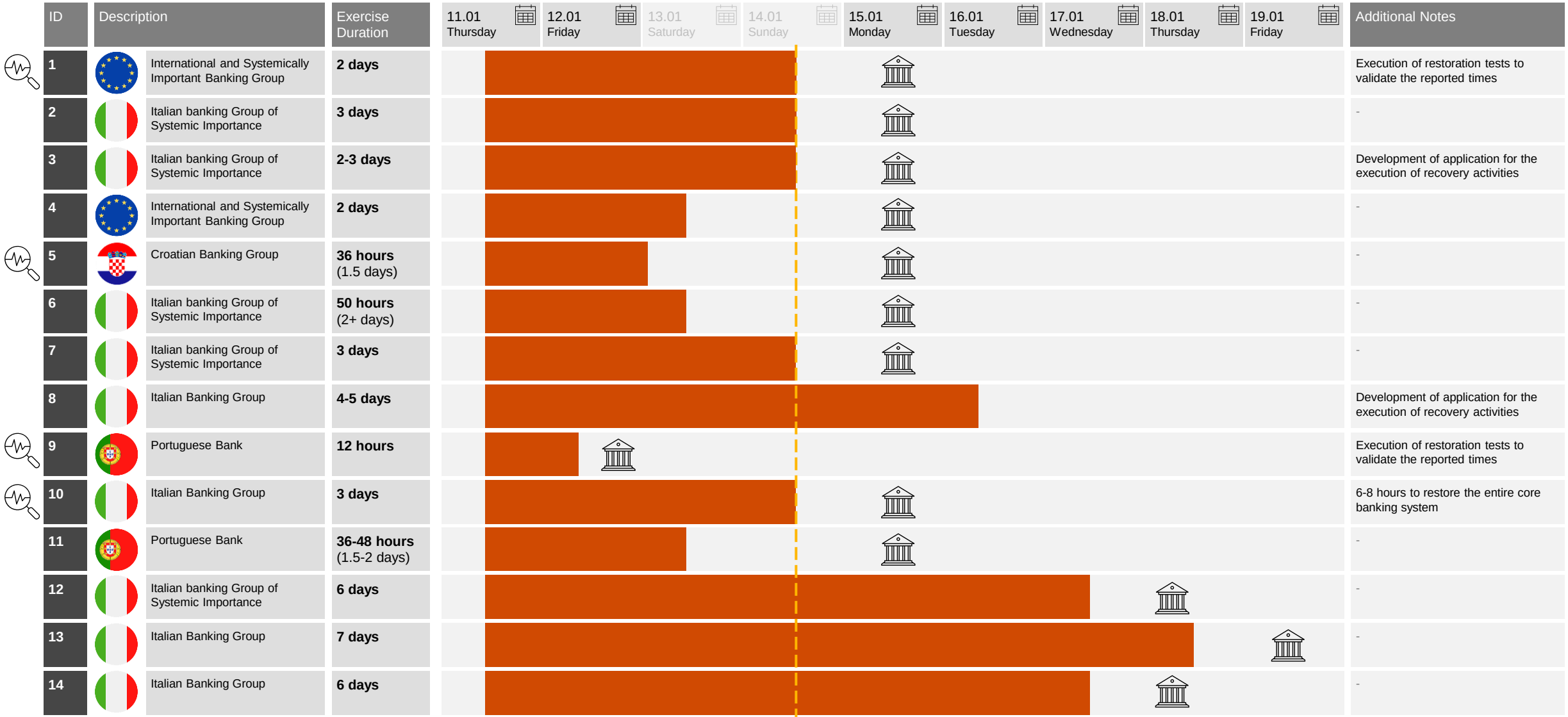
PORTUGAL
- Banco Comercial Português, S.A.
- Caixa Geral de Depósitos, S.A.

SPAIN
- ABANCA Corporación Bancaria S.A.
- Banco Bilbao Vizcaya Argentaria, S.A.
- Banco de Crédito Social Cooperativo, S.A.
- Banco de Sabadell, S.A.
- Banco Santander, S.A.
- Bankinter, S.A.
- CaixaBank, S.A.
- Ibercaja Banco, S.A.
- Kutxabank, S.A.
- Unicaja Banco, S.A.

THE NETHERLANDS
- ABN AMRO Bank N.V.
- BNG Bank N.V.
- Coöperatieve Rabobank U.A.
- de Volksbank N.V.
- ING Groep N.V.
- Nederlandse Waterschapsbank N.V.

ESTONIA
- AS LHV Group
- AS SEB Bank
- Luminor Holding AS

2024 ECB Cyber Resilience Stress Test: Survey sui tempi di ripristino



ID	Description	Exercise Duration	Additional Notes
1	International and Systemically Important Banking Group	**2 days**	Execution of restoration tests to validate the reported times
2	Italian banking Group of Systemic Importance	**3 days**	-
3	Italian banking Group of Systemic Importance	**2-3 days**	Development of application for the execution of recovery activities
4	International and Systemically Important Banking Group	**2 days**	-
5	Croatian Banking Group	**36 hours** (1.5 days)	-
6	Italian banking Group of Systemic Importance	**50 hours** (2+ days)	-
7	Italian banking Group of Systemic Importance	**3 days**	-
8	Italian Banking Group	**4-5 days**	Development of application for the execution of recovery activities
9	Portuguese Bank	**12 hours**	Execution of restoration tests to validate the reported times
10	Italian Banking Group	**3 days**	6-8 hours to restore the entire core banking system
11	Portuguese Bank	**36-48 hours** (1.5-2 days)	-
12	Italian banking Group of Systemic Importance	**6 days**	-
13	Italian Banking Group	**7 days**	-
14	Italian Banking Group	**6 days**	-

In-depth exercise

Re-opening of branches

Business RTO (incl. Data reconciliation activities)

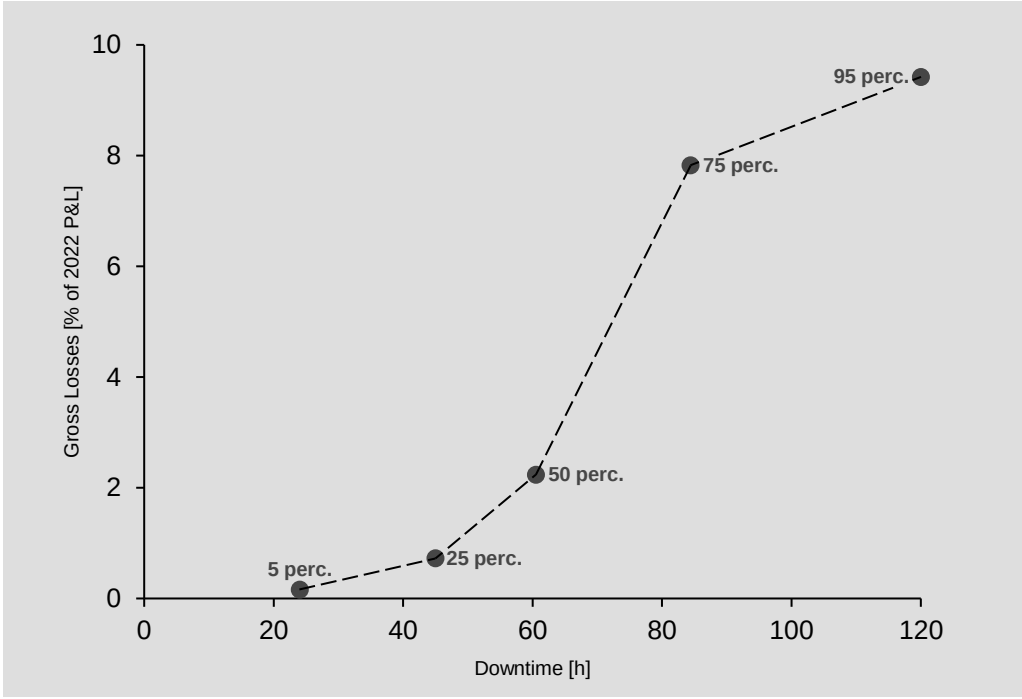
La valutazione degli impatti di business pone le basi per una nuova concezione del ritorno degli investimenti in ambito Cyber

I downtime e le perdite stimate mostrano tendenze che possono essere associate a una **relazione monotona.**

Le banche più mature in termini di **misure di contingency** e di **business resilience**, e quindi in grado di **limitare il perimetro della clientela** interessata dall'interruzione del Core Banking System o che sono caratterizzate da un particolare modello di business, **segnalano impatti più contenuti**.

Le perdite dirette stimate dalle banche sono, in media, **inferiori a quelle indirette**. Le perdite dirette comprendono generalmente le perdite dovute a discontinuità operativa, guasto del sistema informatico e mancata esecuzione dei processi bancari.

Le perdite indirette comprendono generalmente le perdite relative al risarcimento per operazioni fraudolente, inadempienze nei confronti di clienti/fornitori o outsourcer e sanzioni normative.



Le analisi riportano una distribuzione polarizzata tra il **50°** e il **75°** percentile, con **valori di perdita** compresi tra il **2 e l'8%** del Fatturato netto 2022 e **tempi di inattività** compresi **tra 60 e 85 ore**

Crescono le competenze ma anche il fabbisogno a livello globale

-4 M (+12%)

Sono i profili cyber che mancano a livello globale su 5.5M€ attualmente esistenti

Di cui 347.000 in Europa (+10%)

25%

Presenza femminile nell'intero settore Cybersecurity

Nel 2017 erano solo l'11%

13,2%

Tasso medio di turnover per profili Tech

Il mercato FS si attesta sulla media assoluta del 10,8%

67%

È la percentuale di aziende che ha problemi a trovare profili Cyber

+10%

Aumento medio nel 2018

Rispetto ad un settore IT che cresce del 3%

Fonte: ISC2 Cybersecurity Workforce Study 2023

L’esigenza di competenze specifiche include anche i membri del Board

SUPERVISION NEWSLETTER

New policy for more bank board expertise on ICT and security risks

21 Febbraio 2023

1. Top Management must **adequately understand** IT/Cyber risks
2. **The current level of competence/experience** of the Board members **is inadequate**
3. **At least one non-executive board member** with **adequate skills and experience** in ICT and Cyber risk
4. **Regular training** on these topics
5. Starting **from 31 March 2024** assessments will be carried out **on the board members**

Grazie

Paolo Carcano
Partner PwC Italia, Cyber Security & Privacy FS
+39 334 689 6335
paolo.carcano@pwc.com