BANCA D'ITALIA
EUROSISTEMA

Supervision, Risks & Profitability

Auditorium Bezzi – Banco BPM
Milano, 6-7 Giugno 2023

L'evoluzione regolamentare e la prospettiva dell'Autorità di Vigilanza

Relatore: *Luca Cusmano*
Servizio Rapporti Istituzionali di Vigilanza

luca.cusmano@bancaditalia.it

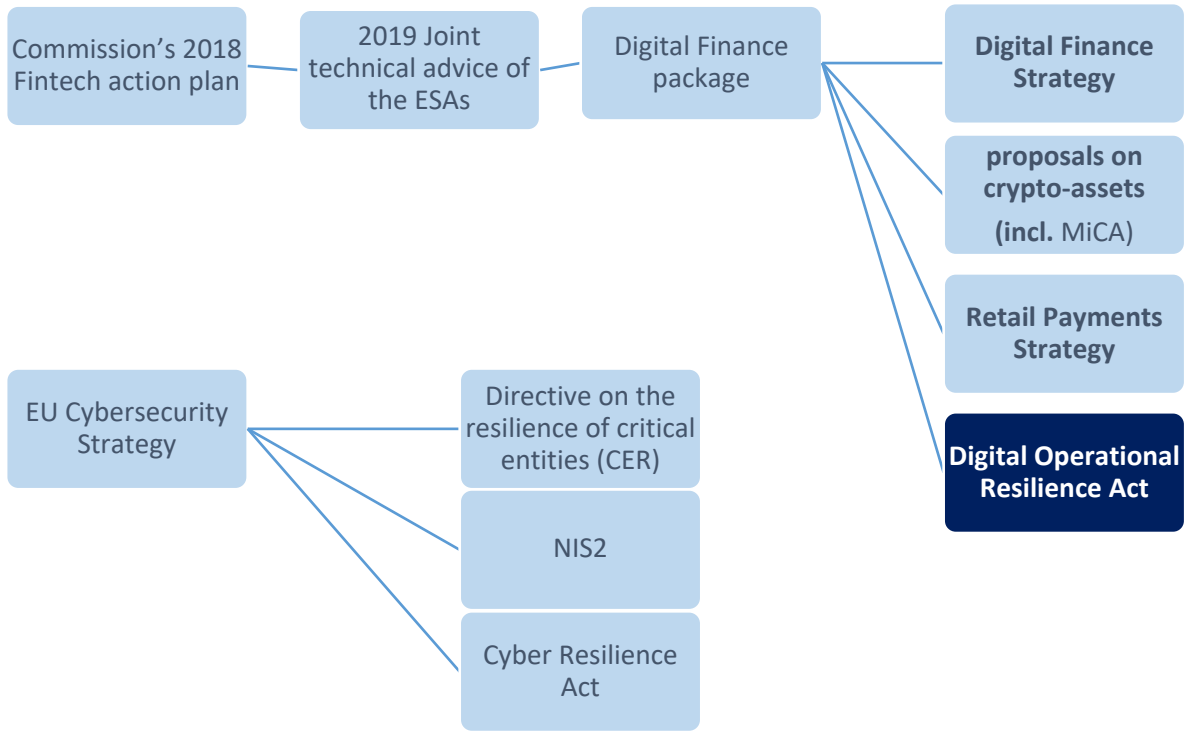
Agenda dell'intervento

1. **L'evoluzione regolamentare**
2. **Stato dell'arte della DORA e lavori di implementazione**
3. **Principali aspetti di discussione in ambito regolamentare**
4. **Le sfide per la Vigilanza**

1. L'evoluzione regolamentare

Il Digital Operational Resilience Act (DORA) mira a rafforzare la componente di cyber resilience del rulebook europeo per il settore finanziario

A Europe Fit for the Digital Age



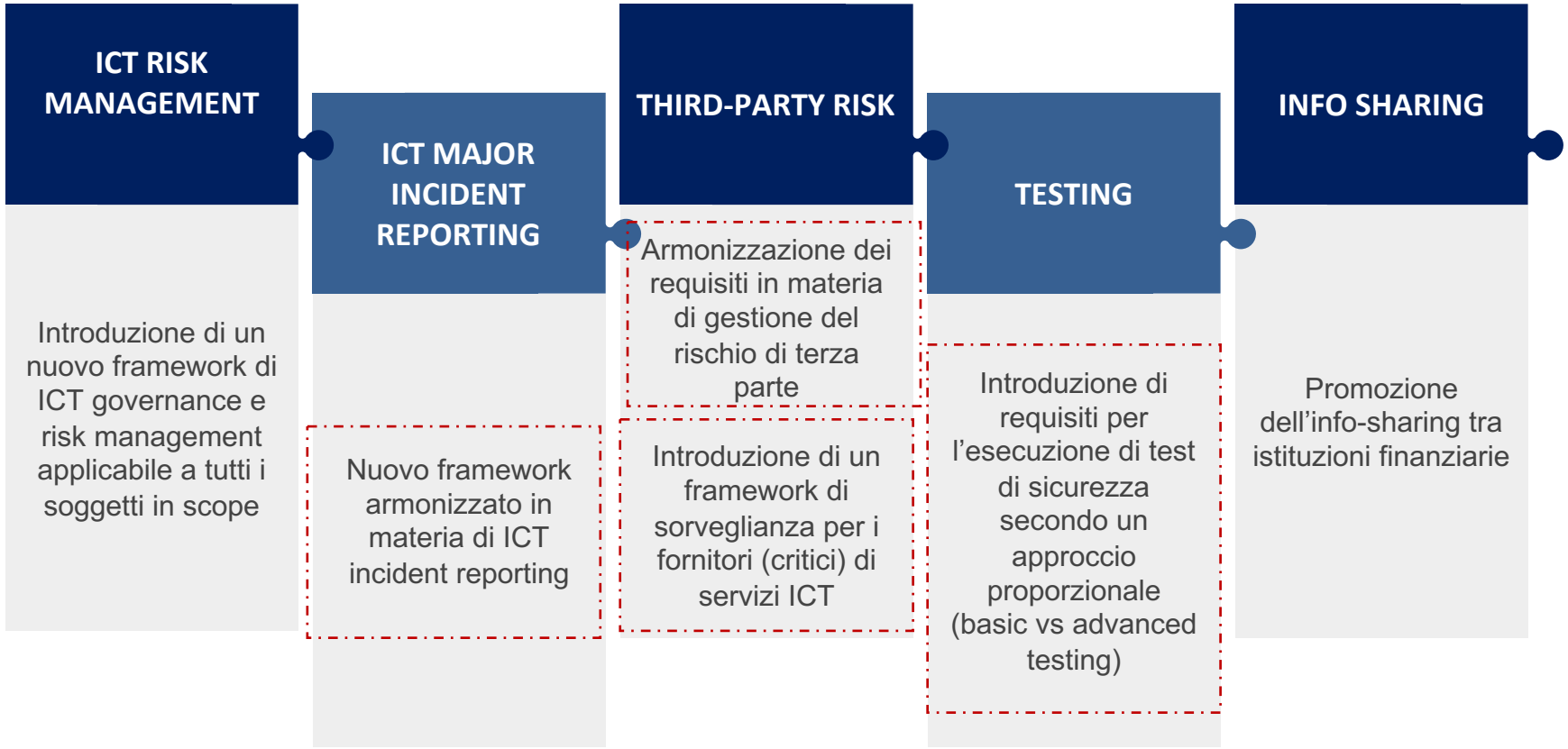
1. L'evoluzione regolamentare

BANCA D'ITALIA
EUROSISTEMA

Building block	Main elements of the buiding block	EU financial services Level 1 and Level 2 legislation												
		Payments (PSD2)	Banks (CRD/CRR)	Investment firms (MIFID)	Trading Venues (MIFID)	CCPs (EMIR)	CSDs (CSDR)	Trade Repositories (EMIR)	Insurance (Solvency II)	Asset Management (UCITS/AIFMD)	CRAs	Data Reporting Service Providers (DRSPs)	Audit	IORPs
ICT risk management	Arrangmenents (policies, procedures and systems) on risks to which the entity is exposed to		art. 74(1)	art. 16(4), (5)	art. 47 (1)	art. 26(1)	L2 - art.48(1)	Art 79		L2 - art. 60(1) - both art. 15(2) - A	Annex I - Section A, (4)			art. 28(3)
	Operational risk framework / policy	art. 95(1)				Art. 28 (risk committee)	L2 - art. 70(1)			L2 - art. 13(1) - A				
	Risk management policy			L2 - art. 23(1)		L2 art.4			art. 41(3)	L2 - art. 38(1) - U				art. 25(1)
	Information security framework/strategy	art. 95(1)		L2 - art. 18 (AT)		L2 - art. 9(3)	L2 - art. 70(9), art. 75(3)							
	Appropriate IT tools, reliable, resilient and secure systems (to ensure security / integrity / confidentiality)	art. 95(1), art. 97(3) L2 - chapter II,IV,V		art. 16(5) L2 - art. 21(2)	art. 48(1) L2 - art. 23(1),(2)	art. 26(6) and L2 art.9	art. 45(1) L2 - art. 75	L2 - art. 79(1)	L2 - art. 258(1)	L2 - art. 57(2) - A		art. 64 (4), 65(5), 66(3) + L2 - art. 9(1)		
	Business continuity policy		art. 85(2)	art. 17 (1) and L2 - art. 14(1) - (AT) L2 - art. 21(3)	art. 48(1)	art. 34(1) L2 - art. 17	L2 - art. 76(1)	art. 79(2)	L2 - art. 258(3)	L2 - art. 57(3) - A	L2 - art. 11 (2)		art. 24a 1(h)	art. 21(5)
	Contingency plans		art. 85(2)		art. 47(1)	part of BCP as referred to in art. 34			art. 41(4)					art. 21(5)
	Crisis management and communications					L2 - art. 22	L2 - art. 70(4)							
	Disaster recovery plan					art. 34(1) L2 - art. 19	L2 - art. 76(1), art. 78	art. 79(2)						
	2h RTO				L2 - art. 15(2)	L2 - art. 17(6)	L2 - art. 78(2)							
Incident reporting	Reporting of operational incidents to CAs	art. 96(1)			L2 - art. 23(3) L2 - art. 83(1)		art. 45(6) L2 - art. 43(h)							
	Procedures to record, monitor and resolve operational incidents						L2 - art. 71(4)						art. 24a 1(i)	
	Breaches in physical and electronic security measures	art. 96(1)		L2 - art. 18(3) (AT)								L2 - art. 9(4)		
Testing	Testing of IT tools, systems and procedures	L2 - art. 3(1)				partly relevant by general provisions art. 49	art. 45(5) L2 - art. 75(6)							
	Penetration testing			L2 - art. 18(4) (AT)										
Third party risk	Outsourcing - the entity remains fully responsible	art. 19(6) art. 20(2)		L2 - art. 4(1) (AT) L2 - art. 31(1)	L2 - art. 6(1)	art. 35(1)	art. 30(1)		art. 49(1)			L2 - art. 6(4)		art. 31(2)
	Outsourcing is governed by a written agreement			L2 - art. 31(3)	L2 - art. 6(4)		art. 30(2)	L2 - art.16			L2 - art. 35			art. 31(5)
	Outsourcing - report to CAs on the outsourcing	art. 19(6)			L2 - art. 6(5), (7)	art. 35 approval by CA required			art. 49(3)	art. 20(1) - A				art. 31(6)
	Identify critical service providers (CSPs) and manage dependencies					L2 - art. 18(3)	L2 - art. 68(1), (2)							
	Inform CAs on dependencies with CSPs						L2 - art. 68(1)					L2 - art. 6(4)		
	Robust arrangements for the selection and substitution of IT third party service providers						L2 - art. 75(3)							
	Due diligence when outsourcing to third party service providers			L2 - art. 31(2)										
	Outsourcing to third party service providers located in a third country			L2 - art. 32										

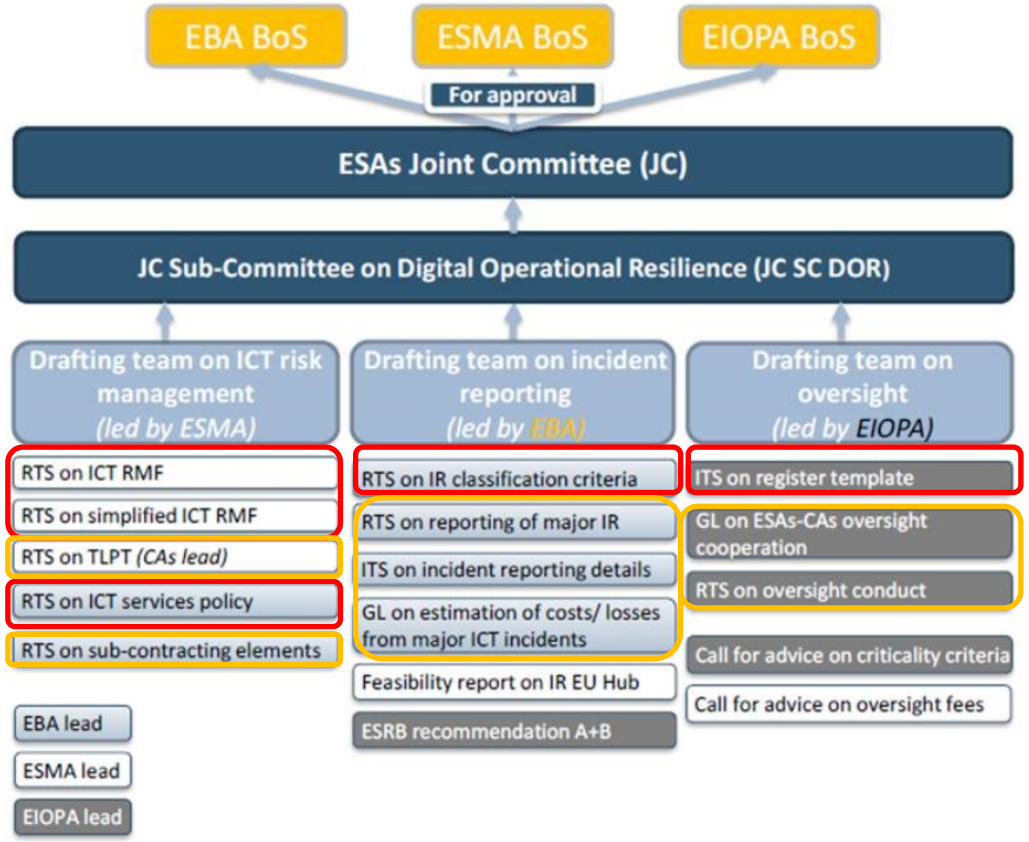
Table 7 – Mapping of existing (qualitative) provisions on digital operational resilience in the EU financial services L1 and L2 legislation. The different elements of the building blocks (column 2) are illustrative and non-comprehensive. Legend: white= provisions missing in the EU financial services legislation; green cells = provisions exist in the EU financial services legislation; L2 = level 2 legislation. Source impact assessment* EUR-Lex - 52020SC0198 - EN - EUR-Lex (europa.eu)

2. La DORA



- ✓ *Data di entrata in vigore della DORA: 16.01.2023*
- ✓ *Date di applicazione: + 24 mesi (17.01.2025)*

2. I lavori di implementazione della regolamentazione di II Livello



16 Mandati

Principali milestone

Scadenza 12 Mesi:
- Consultazione pubblica: Lug – Sett 23
- Pubblicazione: Gennaio 2024

Scadenza 18 Mesi:
- Consultazione pubblica: Nov 23 – Feb 24
- Pubblicazione: Luglio 2024

Principi che ispirano i lavori: Momentum, qualità, pragmatismo

3. Alcuni aspetti di discussione in ambito regolamentare

ICT Risk Management

- Allineamento con i framework esistenti (es. EBA/ESMA/EIOPA guidelines), per facilitare la sintonia, ridurre i costi di implementazione, garantire la continuità con l'attività di vigilanza
- Approccio Technology-neutral & future-proof
- Principio di proporzionalità

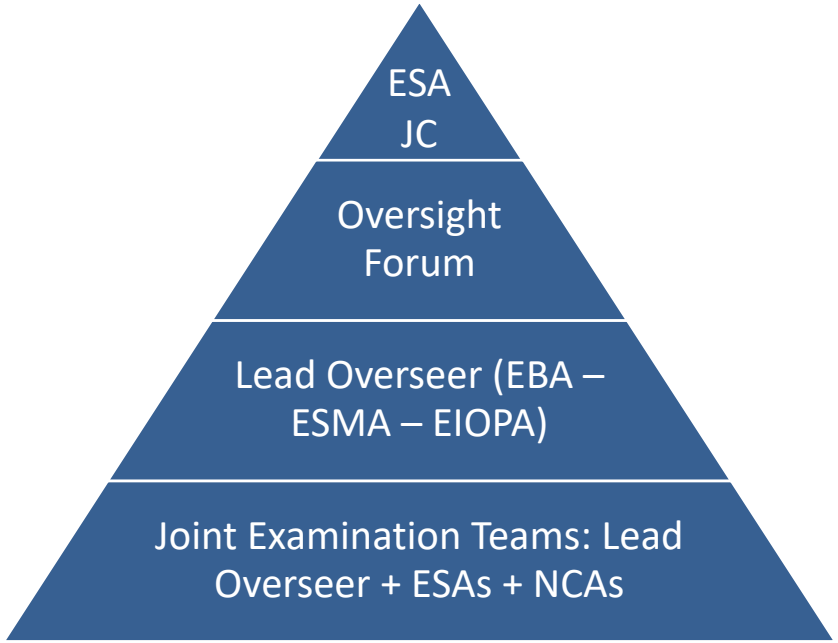
Incident Reporting

- Armonizzazione con i framework esistenti e prassi già consolidate (es. PSD2)
- Inclusione dei Cyber threat nella valutazione delle NCA (non più solamente I cyber threat)
- Single Hub a livello europeo per i Major ICT Incident

TLPT

- allineamento con TIBER;
- identificazione delle entità finanziarie soggette a TLPTs

3. La novità per i service provider: l'Oversight Framework



Union Oversight framework for critical ICT third-party service providers

- ESAs as Lead Overseers
- Financial entities shall only make use of the services of a CTPPs established in a third if it has a subsidiary in the Union
- Possibility to impose a periodic penalty payment (up to 1% of the average daily worldwide turnover)
- CA shall inform relevant financial entities of the risks identified in the recommendations addressed to CTPPs
- CA may request to suspend use of service or terminate contractual arrangement.

Preparatory work for ESAs and NCAs:

- *ESAs will need to designate critical third-party providers of ICT services (CTPPs)*
- *To gain a first understanding of the market and to gain practical experience in this area, ESAs (with NCA input) launched a joint exercise covering a sample of financial entities*

3. Attualmente in consultazione

Call for advise on criticality criteria and oversight fees

- Le ESAs designeranno i fornitori ICT critici sulla base di alcuni criteri (impatto sistemico del disservizio del fornitore; carattere sistemico delle entità finanziarie servite; dipendenza delle entità finanziarie dai servizi prestati dal fornitore; grado di sostituibilità di quest'ultimo).
- L'RTS specificherà maggiormente i criteri stabiliti dalla norma primaria, introducendo anche delle soglie quantitative. La metodologia per l'individuazione dei fornitori critici sarà successivamente realizzata dalla Commissione EU.
- L'RTS illustrerà anche come calcolare le fees da applicare ai provider soggetti alla sorveglianza. Tale fees, dovranno tenere conto di diversi aspetti e costi che si dovranno sostenere per la gestione del framework..

4. Le sfide per la Vigilanza

- Crescente importanza del Rischio IT. Rischio operativo o trasversale?
- Il ruolo dei service provider e le implicazioni in termini di rischio sistemico -- > SSM cyber stress test
- L'importanza di avere risorse qualificate per valutare la variabile tecnologica (opportunità di revisione dei modelli di business ed esposizione/gestione del rischio)

4. La nostra esperienza sui service provider

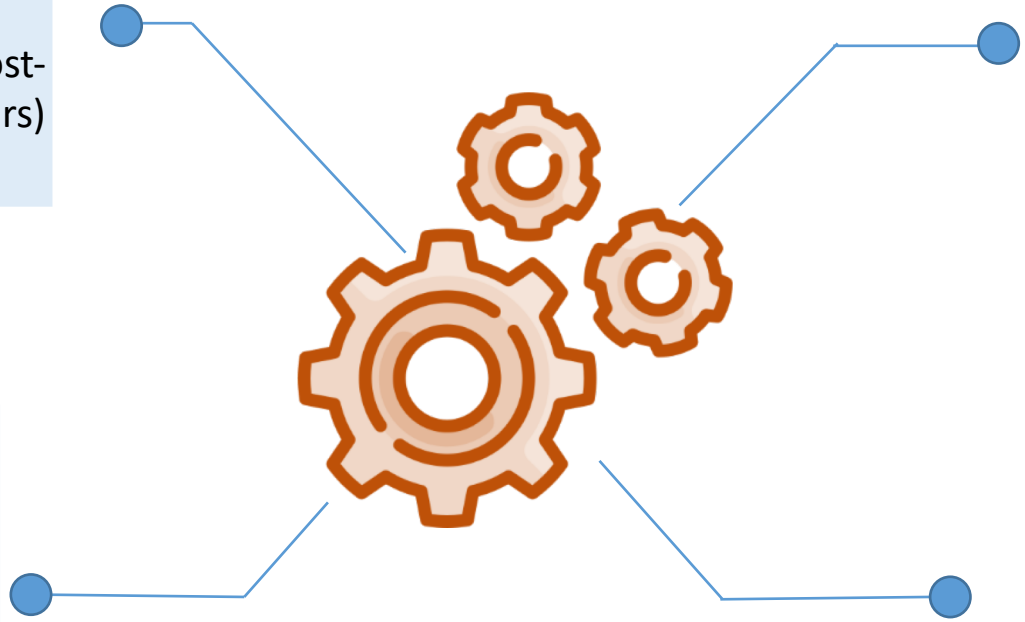
- Approccio strutturato e anticipatorio rispetto all'implementazione della DORA
- Attività off-site e on-site sui principali providers (anche non IT)
- Modifiche organizzative interne

Interventi Diretti

Analisi e attività off-site (e.g. post-incident follow up con i providers) e on-site

Supporto alle attività di supervisione

Creazione di una dashboard con informazioni quantitative e qualitative sui service provider



Sviluppo di metodologie e tools

Sviluppo di metodologie di analisi

Partecipazione nelle discussioni internazionali

Presenza su vari tavoli

BANCA D'ITALIA
EUROSISTEMA

Supervision, Risks & Profitability

Auditorium Bezzi – Banco BPM

Milano, 6-7 Giugno 2023

Domande ??