BANCA D'ITALIA
EUROSISTEMA

Supervision, Risks & Profitability
Auditorium Bezzi – Banco BPM
Milano, 9-10 Giugno 2026

Evoluzione dei rischi ICT e cyber: attività di vigilanza e profili regolamentari

Relatori: Mauro Belcastro, Giulia Arangio
Banca d'Italia
Servizio Supervisione intermediari finanziari, Servizio Rapporti istituzionali di Vigilanza

mauro.belcastro@bancaditalia.it, giulia.arangio@bancaditalia.it

Introduzione

Trasformazioni geopolitiche e digitali

Le tensioni geopolitiche e la trasformazione digitale influenzano profondamente il contesto economico e finanziario globale.

Settore finanziario digitalizzato

Il settore finanziario è altamente digitalizzato e interconnesso tra operatori, infrastrutture e fornitori tecnologici.

Frammentazione della catena del valore e degli ecosistemi

Il modello è passato da un'integrazione tradizionale a un ecosistema frammentato di operatori specializzati, aumentando complessità operativa e vulnerabilità lungo la catena del valore.

Rischio sistemico e contagio

La natura interconnessa amplifica l'impatto degli incidenti, creando vulnerabilità sistemiche e rischi di contagio.

Attività di vigilanza

Il Piano Strategico 2026-2028 della Banca d'Italia presenta tra gli obiettivi strategici, il presidio sull'evoluzione delle nuove tecnologie nel sistema finanziario.

In particolare, tra le attività svolte dalla Banca d'Italia in tale ambito:

- Supervisione on-going
- Autovalutazioni DORA
- Analisi dei Registri delle Informazioni (RoI)
- Analisi dei gravi incidenti ICT
- Indagine Fintech – focus intelligenza artificiale

4. Il presidio sull'evoluzione delle nuove tecnologie nel sistema finanziario

Le direttrici lungo le quali si declina l'obiettivo strategico n. 4 riguardano: il rafforzamento della vigilanza sugli intermediari e la tutela dei clienti a fronte dei rischi emergenti; il presidio dell'evoluzione del Fintech e delle infrastrutture di pagamento e finanziarie; il potenziamento della resilienza cibernetica della Banca e delle infrastrutture di pagamento e di mercato.

Supervisione on-going: focus sulle attività nei confronti dei fornitori ICT

BANCA D'ITALIA
EUROSISTEMA

Poteri di vigilanza della Banca d'Italia sui fornitori ICT:

- Vigilanza Ispettiva;
- Vigilanza Informativa;
- Convocare amministratori, sindaci e altro personale;
- Applicare sanzioni (solo in casi particolari).

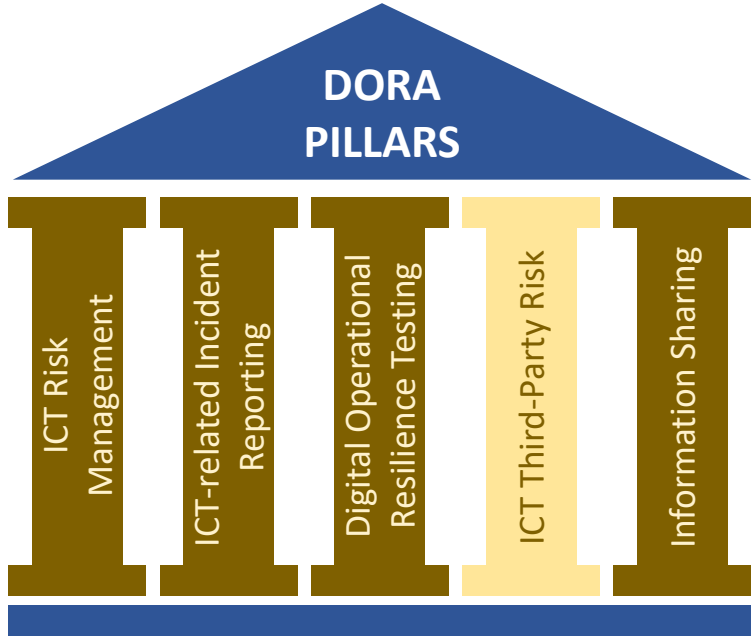
Principali attività di vigilanza:

- Accessi on site;
- Vigilanza cartolare (ad es. thematic review);
- Incontri con l'industria.

Supervisione on-going: attività nell'ambito del DORA Oversight Framework sui CTPP

Partecipazione alle attività di vigilanza sui Critical Third Party Provider (CTPP) nell'ambito del DORA Oversight Framework:

- **Oversight Forum**: Organo di coordinamento che assicura coerenza, proporzionalità e qualità delle attività di supervisione sui fornitori ICT critici, favorendo il confronto e l'allineamento tra le autorità di vigilanza europee (EBA, ESMA, EIOPA).
- **Joint Examination Teams** (**JET**): gruppi operativi coordinati ciascuno da un Lead Overseers (EBA/ESMA/EIOPA), che svolgono operativamente le attività di vigilanza sui CTPP (ad es. general investigations, on site inspections, ecc.).



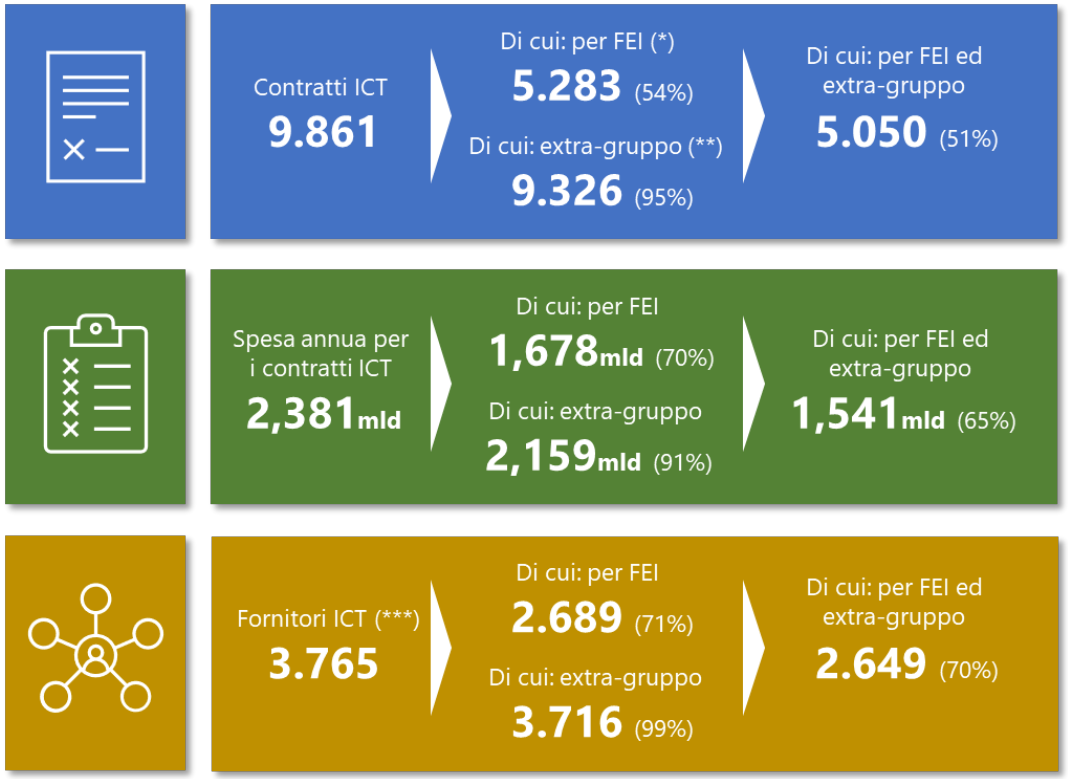
Attività di supervisione: analisi RoI

DORA ha introdotto i Registri delle Informazioni (RoI) con tre funzioni:

- Parte del framework di gestione del rischio ICT per le financial entities
- Strumento di supervisione per la vigilanza
- Base informativa per l'identificazione dei fornitori critici da sottoporre all'Oversight Framework

Dall'analisi 2025 è emerso:

- forte incidenza della componente extragruppo, sia per numero di contratti (95% del totale), sia per spesa complessiva (91%), sia per numero di fornitori (99%)
- alta concentrazione per costo dei contratti sui primi 5 fornitori di servizi ICT (40% del totale)
- Oltre l'80% dei contratti a supporto di FEI vengono erogati dall'Italia, e circa il 30% dei contratti prevede la conservazione di dati con sensibilità «alta», nella grande maggioranza dei casi conservati nell'UE



Attività di supervisione: gravi incidenti ICT

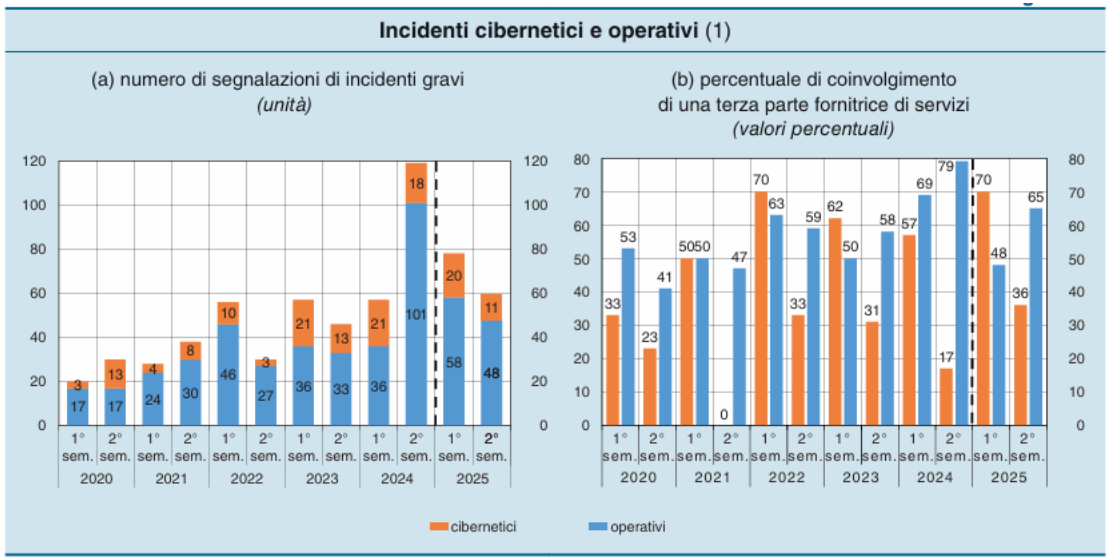
DORA ha introdotto un *framework* armonizzato di *incident reporting* che:

- estende l'obbligo di segnalazione a nuovi soggetti
- prevede un meccanismo di condivisione degli incidenti cross-border
- prevede la segnalazione su base volontaria delle minacce cyber

La Banca d'Italia raccoglie e analizza i report dei gravi incidenti ICT. Ne deriva anche un analisi orizzontale che annualmente viene pubblicata sul sito ufficiale.

Dall'analisi è emerso che:

- Poche segnalazioni da parte di entità che non erano soggette al *framework* pre-DORA
- Importanza della catena di fornitura
- Rilevanza del *change management*



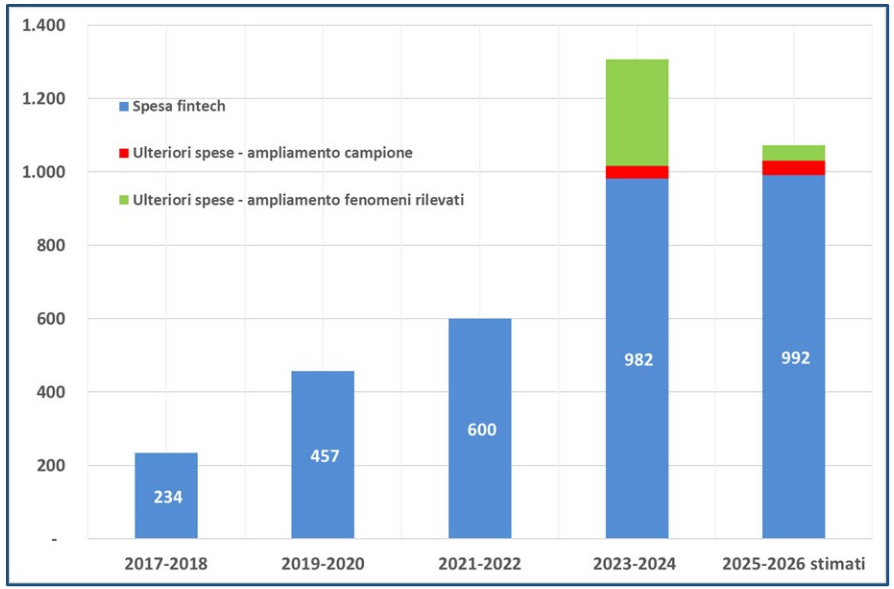
Fonte: Rapporto di Stabilità Finanziaria RSF_1_2026.pdf

Indagine Fintech: focus AI

La Banca d'Italia svolge un'indagine sugli investimenti in tecnologie innovative nel sistema finanziario italiano.

Tra i principali risultati emersi:

- Investimenti di quasi un 1 mld di euro in entrambi gli ultimi due bienni nel sistema finanziario italiano
- GenAI guida investimenti nel prossimo biennio, ma poco diffusa nei servizi core business, dove prevalgono tecniche di ML più tradizionali
- L'AI è ormai parte integrante della strategia digitale degli intermediari, soprattutto quelli di grandi dimensioni
- L'adozione tecnologica procede più velocemente della governance
- Tra le sfide del prossimo biennio rileva l'implementazione regolamentare (AI Act).



2025-indagine-fintech-intermediari.pdf

Riordino della normativa

Contesto: a partire dal 17 gennaio 2025 si applica il Regolamento DORA che mira a favorire l'armonizzazione dei requisiti di resilienza digitale per tutto il settore finanziario europeo.

⇒ Necessario riordino della normativa preesistente al fine di garantire la coerenza del quadro regolamentare ed evitare duplicazioni e sovrapposizioni con i nuovi requisiti direttamente applicabili.

In particolare, sono stati revisionati:

- **A livello europeo** le EBA Guidelines on ICT and security risk management (EBA/GL/2019/04)
- **A livello nazionale**, la normativa secondaria della Banca d'Italia applicabile alle banche, agli IP e agli IMEL (nello specifico per la banche la Circolare 285).

Revisione delle EBA Guidelines

A seguito dell'entrata in vigore del Regolamento DORA, le EBA *Guidelines on ICT and security risk management* sono state oggetto di revisione nel 2025 al fine di garantire la coerenza del quadro regolamentare ed evitare duplicazioni e sovrapposizioni con i nuovi requisiti direttamente applicabili.

Modifiche

- In particolare, la revisione ha comportato la rimozione delle disposizioni riguardanti l'ICT.

- Rimangono alcune disposizioni riguardanti profili non coperti dal Regolamento e riferiti ai servizi di pagamento ai sensi della PSD2, con specifico riguardo alla gestione del rapporto con gli utenti, alla sicurezza delle comunicazioni e alla protezione dei dati, assicurando continuità regolamentare in tali ambiti.

Cap. IV – Il sistema informativo

- Sono state eliminate tutte le previsioni relative al sistema informativo, in quanto già disciplinate da DORA.
- Sono state mantenute le disposizioni specifiche relative ai rapporti con gli utenti dei servizi di pagamento in attuazione della PSD2.

Cap. V – La continuità operativa

- A livello generale viene mantenuta l'organizzazione precedente a tre sezioni: Sezione I (Disposizioni di carattere generale) – Sezione II (Requisiti per tutte le banche) – Sezione III (Requisiti particolari per i processi a rilevanza sistemica).
- Le Sezioni I e II sono state aggiornate come segue:
  - Rimozione previsioni sulla continuità operativa in ambito ICT -> Rimando a DORA.
  - Coerenza con framework DORA (es. funzioni essenziali o importanti in luogo dei processi critici).
- La Sezione III non ha subito modifiche, in quanto sono in corso approfondimenti di più ampia portata.

Grazie per l'attenzione