La resilienza dei servizi digitali per il mercato finanziario

ABI Supervision risks and profitability 2026
Sessione parallela 1.3 - Pronti a gestire nuovi canali, nuovi prodotti/servizi e nuovi rischi?

9 giugno 2026

Argomenti

1. Contesto di riferimento
2. Digitalizzazione opportunità e minaccia (report BankIT)
3. Il ruolo dell'AI tra protezione e attacco
4. Il caso Mythos e l'impatto per la finanza mondiale
5. Misure a disposizione delle banche per la resilienza dei prodotti digitali

Il Contesto di Riferimento

Le priorità strategiche in ambito Cyber a livello Globale per PwC

La geopolitica come arma informatica

Le tensioni geopolitiche non rappresentano soltanto un rischio di mercato: sono diventate una minaccia operativa diretta alimentando attacchi state-sponsored e generando una frammentazione normativa che complica la conformità e la gestione degli incidenti.

Artificial Intelligence (AI): La Sfida Duale

L'AI è al tempo stesso un motore imprescindibile di innovazione e un potente strumento nelle mani dei Threat-Actor. Ogni vantaggio competitivo che offre introduce nuove vulnerabilità e amplia la superficie di attacco.

Il conto alla rovescia Quantum

La minaccia del calcolo quantistico per la crittografia moderna non è più teorica. La strategia 'harvest now, decrypt later' significa che i dati rubati oggi rappresentano una bomba a orologeria, rendendo la sicurezza dei dati a lungo termine una priorità critica già nel presente.

- Le **priorità strategiche** delle organizzazioni dovrebbero quindi essere le seguenti:

Costruire una resilienza pronta per il futuro

Superare i piani di risposta tradizionali definendo e testando i PlayBook contro minacce combinate, come un attacco AI state-sponsored durante una fase di volatilità dei mercati.

Definire un piano di risposta unificato

Sviluppare un framework unificato per la gestione degli incidenti e la governance dei dati, in grado di affrontare normative frammentate e prevenire conflitti di conformità normativa.

Proteggere il ciclo di innovazione

Per quanto riguarda l'AI prevedere l'integrazione di una governance "secure-by-design" in tutti i nuovi investimenti; in ambito Quantum avviare fin da subito il percorso verso la crittografia post-quantum (PQC) per proteggere i dati a lungo termine.

Digitalizzazione – opportunità e minacce: principali risultati derivanti dallo SREP & priorità della vigilanza 2026-2028

Approfondimento degli ambiti rilevanti in relazione alla gestione dei rischi derivanti dalla digitalizzazione finanziaria

Operational e ICT Risk - Key findings

> Resilience will be at the core of the supervisory priorities 2026-2028

- Il **rischio operativo e ICT** è ancora l'elemento dello **SREP** con i **punteggi medi più bassi**, con la componente di **rischio ICT** che ha ottenuto il **punteggio peggiore in media**.
- **La complessità che le banche devono affrontare** deriva dalle loro **strategie di digitalizzazione**, dalla forte d**ipendenza dall'outsourcing IT** e dall'implementazione dei **requisiti DORA**.
- **Le sfide** da affrontare sono la **governance ICT**, la **gestione del rischio ICT** e il **rischio di sicurezza ICT**, con **crescenti preoccupazioni** relative alla gestione del **rischio dei terzi** (TPRM).
- **Con riferimento alle terze parti** la BCE segnala **rischi di sovranità** attraverso le esposizioni statunitensi per il TPRM.
- Rispetto alla **revisione sull'outsourcing** condotta da BCE nel 2023 e nel 2024 sono ancora presenti **debolezze sulla strategia di outsourcing**, **strategie di uscita** e **gestione della continuità aziendale**. Nel 2026, la revisione coinvolgerà ulteriori 13 banche e si concentrerà sui requisiti DORA per il TPRM, mentre l'outsourcing critico continuerà a essere strettamente monitorato.
- Sono presenti **margini di miglioramento** per quanto riguarda la **scansione e il testing delle vulnerabilità, la gestione delle identità e degli accessi, l'hardening** (rimozione delle potenziali vulnerabilità di un sistema) e la **segmentazione della rete**.

Il ruolo dell'AI tra protezione ed attacco

- L'**Artificial Intelligence** (AI) sta trasformando profondamente il panorama digitale, con applicazioni che spaziano dalla **generazione automatica** di contenuti alla **protezione avanzata** contro **minacce informatiche**. In ambito cybersecurity, l'AI consente di **potenziare** le **capacità** di **rilevamento** e **risposta**, ma introduce anche nuove sfide, come i deepfake e gli attacchi basati su disinformazione. L'integrazione dell'AI nei processi di sicurezza richiede un approccio consapevole e strutturato, capace di bilanciare innovazione e gestione del rischio.

Il caso Mythos e l'impatto per la finanza mondiale: Evoluzione delle minacce cyber nell'era dei nuovi modelli AI

I **nuovi modelli** di intelligenza artificiale, come i **Frontier AI**, stanno **portando importanti evoluzioni** nel settore della sicurezza informatica. Queste tecnologie offrono **strumenti avanzati** che permettono di **individuare tempestivamente le vulnerabilità** e di gestire in modo più efficace eventuali attacchi informatici. Tuttavia, se utilizzate per fini malevoli, gli stessi modelli non aumentano solo il volume degli attacchi, ma ne cambiano la struttura stessa, introducendo:

Approccio sistemico	Concatenazione vulnerabilità	Tempo di sfruttamento
I modelli non leggono componenti isolati, ma ragionano sull'intero sistema, ne comprendono le interazioni e fanno emergere **vulnerabilità che sfuggono agli approcci tradizionali**.	Vulnerabilità a bassa severità, che in passato potevano essere considerate gestibili, oggi possono essere combinate in sequenze di attacco critiche, con un effetto **moltiplicatore su impatto e velocità**.	Le capacità dell'AI consentono di generare codice per fare attacchi in tempi drasticamente ridotti. Ciò fa sì che il **tempo di reazione tradizionale non sia più un parametro sufficiente**.

L'aspetto fondamentale consiste dunque in un vero e proprio **cambio di paradigma**: ormai il **vantaggio tra attacco e difesa si è spostato nettamente a favore degli attaccanti**. Durante l'**incontro del 26 maggio con la BCE**🔍, è emersa con forza l'esigenza di **rivedere la gestione del rischio cyber**. Non si tratta più di privilegiare il business a qualsiasi prezzo, ma di **stabilire priorità basate sull'effettivo impatto delle minacce**. Questo nuovo approccio invita a una maggiore consapevolezza e a un'analisi più attenta dei rischi, orientando le decisioni verso una protezione più efficace e mirata.

🔍 *Focus nella slides successive*

Sono in corso confronti sul tema Mythos a livello europeo con tutte le Istituzioni Finanziarie

Il confronto con le Autorità di Vigilanza ha l'obiettivo di comprendere lo stato del mercato rispetto ai rischi derivanti da Mythos

Aprile

Fed (Banca Centrale USA)

Riunione a porte chiuse, con breve preavviso, sul rischio sistemico cyber legato a Claude MythosPreview (Anthropic)

22.05

Incontri con Banca d'Italia

Alcune Banche Significant italiane si sono confrontate con Banca d'Italia sul tema

26.05

ECB Industry meeting

Tutte le Banche significant sono state invitate a partecipare ad un incontro nel quale verranno presentate le priorità della Vigilanza sul tema

Maggio

Incontri One 2 One con il JST

Il JST ha attivato conversazioni con le Banche significant per valutare il livello di attenzione sul tema e la presenza di processi in grado di gestire eventuali aggiornamenti di soluzioni in urgenza

28.05

IVASS

Incontro organizzato da IVASS e dedicato alle Compagnie Assicurative per approfondire il tema

CEO Letter alle Banche Significant

Punti di attenzione e azioni

TO BE CONFIRMED

La BCE invierà una lettera ai CdA delle Banche Significant sulle minacce AI-enabled. I principali punti saranno:

- I modelli AI emergenti **ridefiniscono scala e complessità** delle minacce e accelerano la **scoperta delle vulnerabilità**
- Le banche devono valutare l'impatto **senza ritardo,** preparare un **piano d'azione iniziale** e **rafforzare i controlli**
- I requisiti **DORA** restano pienamente validi e le minacce **post-quantum** saranno trattate separatamente in **Q3 2026**

Azioni a breve termine (3–6 mesi)

1. Proteggere le superfici di attacco prioritarie
2. Accelerare vulnerability e patch management
3. Migliorare monitoring, detection e capacità difensive
4. Rafforzare governance, finanziamenti e supply chain

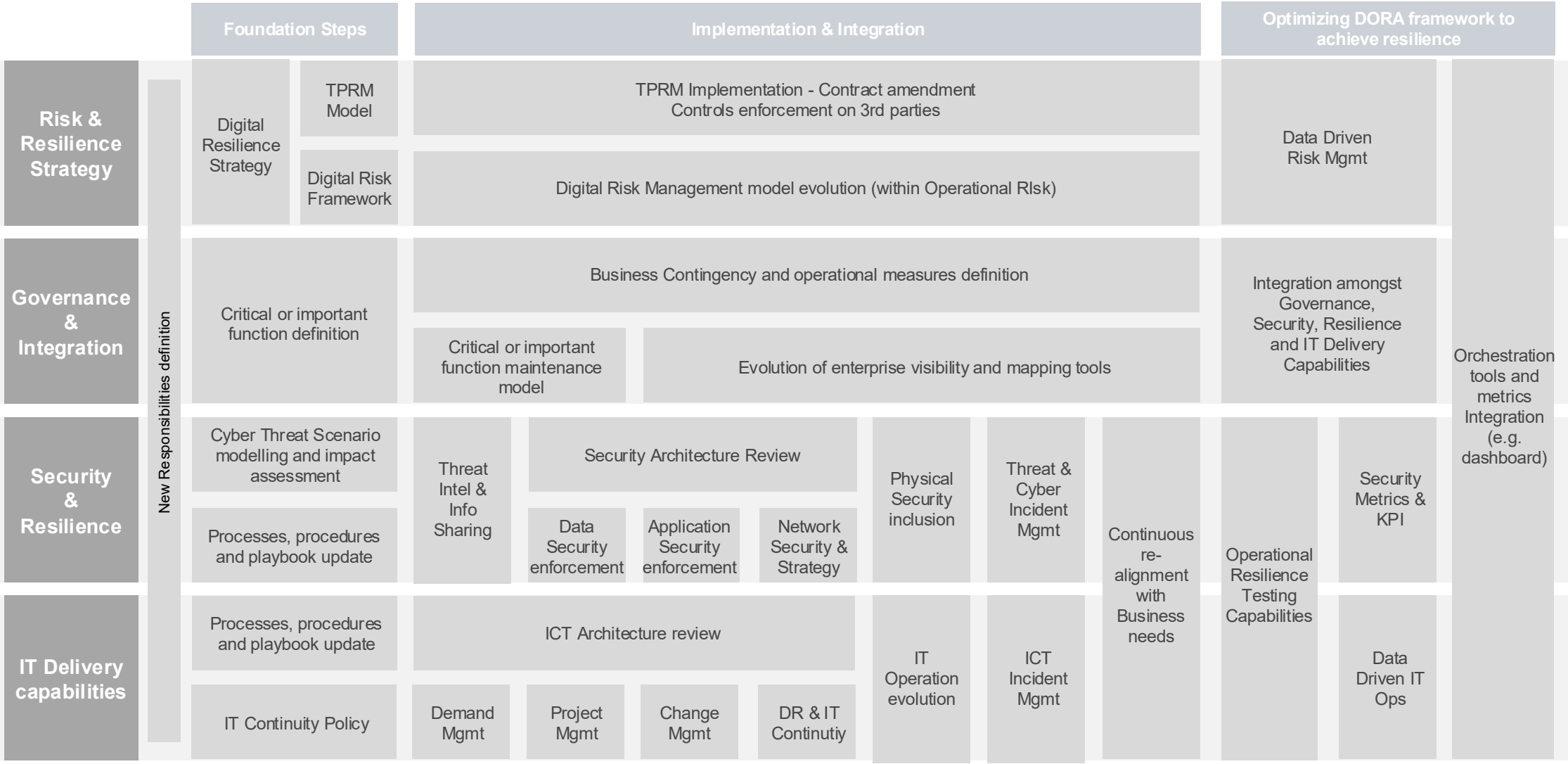
Misure strutturali

5. Rafforzare defence-in-depth e cyber hygiene, modernizzare l'infrastruttura
6. Migliorare resilienza operativa, gestione delle crisi e information sharing

Follow-up della Vigilanza:

- Le banche preparano un **action plan iniziale**
- I **JST** dialogano con le banche e monitorano i progressi
- I **findings ICT/security aperti** vanno chiusi, soprattutto se legati alle aree chiave
- Findings non collegati alle aree chiave possono essere **deprioritizzati** su richiesta
- Scadenza dell'**Annual IT Risk Questionnaire prorogata** da settembre 2026 a **febbraio 2027**

Misure a disposizione delle banche per la resilienza dei prodotti digitali: il valore del programma di trasformazione DORA per il mercato FS



Implementare DORA è una trasformazione a medio-lungo termine con priorità chiave, che devono essere affrontate come base del Programma:

- **Governance e Responsabilità**
- **Visibilità End-to-End** e Orchestrazione / Manutenzione
- **Adeguatezza** degli **investimenti vs.** minacce e **rischi tangibili**
- Governance della Supply Chain e **TPRM**
- **Investimenti** Cyber ed IT

Grazie

pwc.com