BANCA D'ITALIA
EUROSISTEMA

La resilienza digitale: attuazione di DORA e profili di vigilanza

Intervento di Giuseppe Siani
Capo del Dipartimento Vigilanza bancaria e finanziaria della Banca d'Italia

Convegno CSE
'L'evoluzione tecnologica funzionale e normativa nel sistema bancario'

Torino, 26 settembre 2025

1. Introduzione

Ringrazio gli organizzatori per l'invito rivoltomi a partecipare a questo evento, che si concentra su tematiche prioritarie per gli operatori di mercato e per le Autorità.

Come sottolineato di recente dal Governatore[1], la tecnologia è ormai divenuta una leva strategica decisiva per il settore bancario grazie ai possibili effetti sulla reputazione, sulla competitività, sui rapporti con la clientela e sulla stabilità degli operatori.

I risultati reddituali positivi che osserviamo oggi sono sostenuti da un contesto di mercato ancora favorevole, ma non è prudente pensare che questa situazione si mantenga inalterata ancora a lungo. La competizione nel mercato finanziario è destinata infatti a crescere ulteriormente e la capacità di offrire nuovi e più attrattivi servizi caratterizzati da elevati livelli di resilienza digitale rappresenta uno degli elementi centrali per garantire la sostenibilità nel tempo del modello operativo. Gli intermediari devono dunque proseguire a investire in tecnologia sia per migliorare i servizi forniti alla clientela sia per preservare l'integrità e la resilienza dei sistemi informativi.

La vigilanza, a livello nazionale ed europeo, ha prestato attenzione crescente al profilo del rischio IT, tenendo conto del sempre maggior ruolo di questa componente nell'offerta di servizi bancari, della maggiore dipendenza da terze parti e della profonda interconnessione del sistema finanziario, nonché dell'evoluzione degli *standard* di riferimento. Come più volte evidenziato, si tratta di profili prioritari per la supervisione, per gli intermediari bancari e finanziari di ogni dimensione.

Nel mio intervento descriverò le principali evidenze di vigilanza relative al rischio IT, fornirò un aggiornamento sulle riflessioni in corso per l'adeguamento della normativa a seguito dell'attuazione di DORA e anticiperò alcune nostre attività future.

---

1 Intervento del Governatore della Banca d'Italia Fabio Panetta 'Finanza e innovazione per il futuro dell'economia' – ABI, Assemblea degli Associati – Milano, 11 luglio 2025.

2. L'attuazione del Regolamento DORA

La centralità della resilienza digitale ha determinato la stratificazione nel tempo di diverse normative applicabili (ad esempio, il *Digital Operational Resilience Act* (DORA), la Direttiva Network and Information Security (NIS), le Linee guida della Banca Centrale Europea (BCE) e della *European Banking Authority*)[2]: pur perseguendo finalità complementari, esse rendono il quadro regolamentare particolarmente complesso, generando talvolta difficoltà interpretative e potenziale incertezza applicativa.

La complessità della normativa riflette tuttavia la crescente rilevanza a livello globale del rischio ICT e la sua rapida evoluzione, con l'emergere di nuove vulnerabilità precedentemente meno rilevanti. Con particolare riferimento al contesto europeo, il Regolamento DORA assume per il sistema finanziario un ruolo centrale, stabilendo requisiti armonizzati per la gestione del rischio informatico per tutte le tipologie di operatori finanziari e introducendo un regime di sorveglianza sui fornitori 'critici' di servizi IT esterni al settore (cd. terze parti critiche).

Il Regolamento DORA rappresenta quindi il quadro normativo principale che gli operatori devono rispettare al fine di rafforzare la propria resilienza digitale. Esso esamina i profili IT facendo riferimento al più ampio concetto di resilienza piuttosto che a quello di rischio: presuppone quindi la ragionevole certezza (anziché una certa probabilità) del verificarsi dell'evento indesiderato e si concentra sulle contromisure che gli intermediari devono adottare.

Con riferimento al quadro regolamentare, sono stati avviati a livello internazionale e domestico lavori di adeguamento delle regole in vigore; ad esempio, gli aggiornamenti in corso sulle EBA *Guidelines on the sound management of third-party risk*, che sostituiranno le EBA *Guidelines on outsourcing*, introducono numerosi interventi di coordinamento con le previsioni introdotte da DORA e dai relativi atti delegati[3].

La Banca d'Italia è impegnata nello sforzo di semplificazione in atto a livello comunitario, anche per salvaguardare la coerenza complessiva tra le diverse normative. È un impegno che continueremo a portare avanti nella consapevolezza che un quadro regolamentare chiaro è funzionale a sostenere efficacemente la trasformazione digitale del settore finanziario e ridurre i potenziali oneri per gli intermediari, senza compromettere l'obiettivo ultimo della resilienza digitale.

Ad esempio, prima dell'entrata in vigore del Regolamento il 17 gennaio u.s., sono state fornite indicazioni al sistema[4] che hanno confermato margini di flessibilità nella collocazione della funzione di controllo dei rischi ICT nel rispetto del principio di

---

2 Per ulteriori dettagli si rinvia alla pagina del sito web dell'Istituto La Banca d'Italia per la cybersicurezza.

3 Ad esempio, sono stati allineati al Regolamento: le definizioni; l'attuale disciplina sul *sub-contracting* delle funzioni essenziali o importanti; le previsioni sul registro delle informazioni, con l'allineamento tra l'altro del contenuto delle informazioni del registro non ICT a quello previsto da DORA e dai relativi atti delegati (agli intermediari è data facoltà di mantenere un registro unico per servizi ICT e non ICT).

4 Cfr. https://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/regolamento-dora/Comunicazione_Regolamento_DORA_dicembre_2024.pdf

neutralità organizzativa. Inoltre, è stata rivista la modalità di comunicazione alla Vigilanza delle esternalizzazioni di 'funzioni essenziali o importanti', abrogando anche una serie di procedimenti amministrativi previsti dalle normative settoriali previgenti.

È stata altresì abrogata la disciplina relativa alla segnalazione dei gravi incidenti operativi o di sicurezza, facendo rinvio diretto al Regolamento DORA e ai relativi atti attuativi, fornendo alcune precisazioni operative sulle modalità di invio dei flussi informativi. È stato segnalato il rafforzamento dei cc.dd. *Threat-led Penetration Tests* (TLPTs), che con l'attuazione di DORA rappresentano strumenti di vigilanza e devono essere obbligatoriamente svolti almeno con cadenza triennale dagli intermediari identificati dalle competenti autorità. Abbiamo infine avviato il processo per l'adeguamento delle Disposizioni di vigilanza della Banca d'Italia al fine di semplificare la normativa applicabile mediante un chiaro e generale rinvio al DORA per tutti i requisiti in materia ICT, evitando la stratificazione di ulteriori obblighi.

3. L'attività di vigilanza

I rischi informatici e cibernetici, per loro natura, richiedono principalmente valutazioni e interventi di tipo qualitativo, a integrazione dell'eventuale imposizione di requisiti di capitale. È per questa ragione che nel corso degli anni abbiamo sviluppato una gamma di strumenti di vigilanza che comprende verifiche a distanza e ispettive, riferite anche ai fornitori di servizi e, più in generale, alle terze parti, nonché strumenti di confronto orizzontale e analisi di sistema.

La Vigilanza analizza infatti i dati delle segnalazioni relativi a incidenti operativi e attacchi cibernetici di maggiore rilevanza[5], conduce approfondimenti sui rischi derivanti dalle tecnologie emergenti[6], effettua indagini sui temi legati alla *Risk Data Aggregation*[7]. Gli elementi emersi confluiscono nelle valutazioni integrate sul complessivo profilo di rischio ICT degli intermediari vigilati, che tradizionalmente trovano espressione nella valutazione prudenziale annuale di vigilanza (il c.d. *Supervisory Review and Evaluation Process* 'SREP').

Le nostre analisi confermano gli sforzi compiuti dagli intermediari per rafforzare la propria resilienza digitale. Tuttavia, identificano anche alcuni punti su cui occorrerà lavorare ulteriormente.

In particolare, gli approfondimenti condotti negli ultimi anni sulle banche meno significative (*less significant institutions – LSI*) hanno fatto emergere progressi sul fronte

---

5 Cfr., da ultimo, il report orizzontale sugli incidenti riferiti al 2024: https://www.bancaditalia.it/compiti/vigilanza/analisi-sistema/approfondimenti-banche-int/Framework-segnaletico-di-Vigilanza-degli-incidenti-operativi-o-di-sicurezza-Analisi-orizzontale-2024.pdf

6 L'Indagine Fintech, ormai giunta alla sua quinta edizione, fornisce ogni due anni una fotografia dello stato dell'innovazione del sistema. Per l'edizione 2025 sono in corso le analisi sulle evidenze raccolte; alcune anticipazioni sono recepite nel recente intervento del Governatore all'ABI (luglio 2025), mentre a breve sarà pubblicato il rapporto di analisi completo.

7 Cfr. https://www.bancaditalia.it/compiti/vigilanza/analisi-sistema/approfondimenti-banche-int/Indagine-su-Risk-Data-Aggregation-e-Risk-Reporting.pdf

della *governance*[8], pur in presenza di carenze sul fronte dei controlli. Appare inoltre elevata l'esposizione al rischio di terze parti[9], cui tipicamente fanno ampio ricorso gli intermediari di minori dimensioni[10]. Restano inoltre da rafforzare i presidi per l'identificazione e la gestione di minacce e vulnerabilità, unitamente alle misure di sicurezza contro la perdita e il furto di dati.

In parallelo, è proseguita l'attività di supervisione nei confronti dei fornitori nazionali di servizi ICT esterni al perimetro degli intermediari vigilati, spesso di grandi dimensioni e operanti in un mercato a elevata concentrazione, nella consapevolezza del loro ruolo strategico per la resilienza operativa del sistema finanziario.

Il ricorso all'esternalizzazione consente infatti anche agli operatori di minori dimensioni di disporre di strutture e competenze specialistiche non presenti internamente. Va tuttavia rammentato che l'intermediario mantiene la piena responsabilità del servizio acquistato, e che il monitoraggio sull'operatività dei fornitori assume un ruolo strategico quando le esternalizzazioni riguardino profili molto rilevanti per la gestione aziendale, soggetti a regolamentazioni via via più stringenti.

L'obiettivo della nostra azione è quello di verificare l'adeguatezza dei processi aziendali degli *outsourcers* e la capacità di rispettare gli obblighi contrattualmente assunti nei confronti degli intermediari vigilati loro clienti. I principali punti di attenzione emersi dalla nostra attività ispettiva e a distanza riguardano (a) l'efficacia dei sistemi di gestione dei rischi, (b) l'adeguatezza delle procedure che assicurano la continuità dei servizi offerti, (c) l'aggiornamento dei sistemi di monitoraggio dei livelli di servizio (anche nei confronti dei subfornitori) e dei relativi presidi di sicurezza. L'esperienza ci dice inoltre che un confronto più aperto tra fornitore e intermediari-clienti circa gli aspetti emersi dalle verifiche di vigilanza possa irrobustire il rapporto e rafforzare il piano delle azioni di rimedio.

Prima dell'applicazione del Regolamento DORA, la Banca d'Italia ha chiesto a tutti gli intermediari direttamente vigilati di condurre un'autovalutazione sull'adeguamento dei presidi interni alle prescrizioni normative[11], unitamente alla pubblicazione di alcuni chiarimenti cui ho fatto cenno in precedenza.

L'esame preliminare della documentazione ricevuta ha fatto emergere che quasi la metà degli intermediari soggetti alle disposizioni DORA (banche, IP/IMEL, SGR, SIM, piattaforme di crowdfunding) si valutava mediamente già in linea con larga parte dei requisiti normativi alla data di riferimento (30 aprile 2025); ulteriori progressi

---

8 Sono state rafforzate ad esempio le competenze in materia ICT presenti negli organi sociali delle banche meno significative: quelle completamente sprovviste di tali competenze passano dalla metà del 2022 a circa un terzo alla fine del 2024. Aumentano inoltre in media il numero di personale con competenze ICT nelle funzioni di controllo e la frequenza di informative strutturate inviate al *Board*.

9 Circa il 75 per cento delle LSI adotta modelli di pieno o parziale ICT *outsourcing*.

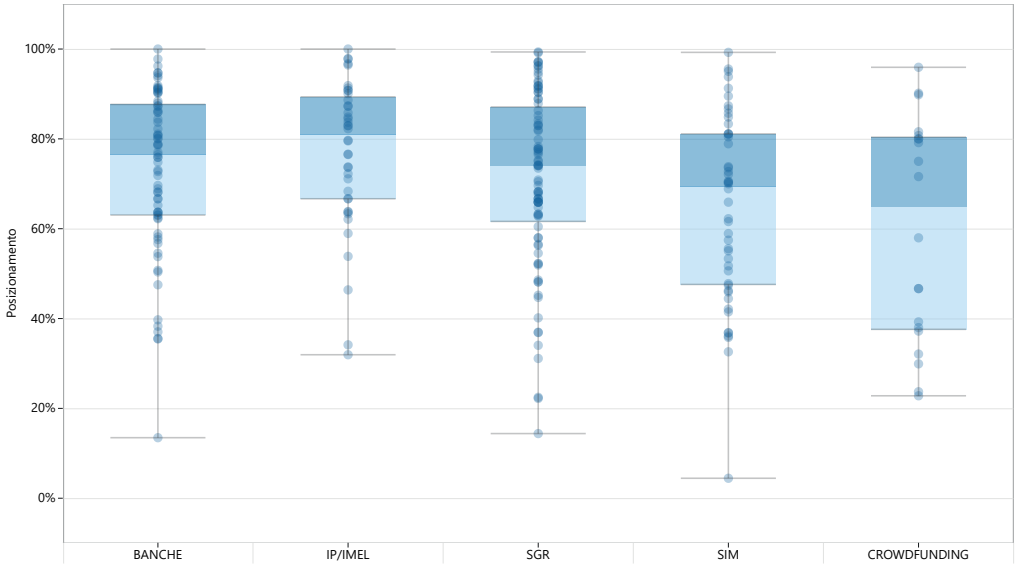
10 Si tratta di profili di tipo strategico, quando attengono ad esempio al ricorso a una pluralità di fornitori (cd ICT *multi-vendor strategy*) o alla definizione *exit strategy* contrattuali, e di tipo operativo, per le difficoltà nel gestire il *change management* e il *security risk*, soprattutto in presenza di sistemi complessi o alla fine del relativo ciclo di vita (c.d. *end of life*).

11 Cfr. https://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/2024.12.23-com-ict/Comunicazione-ICT.pdf

nell'allineamento erano previsti per i mesi successivi. Tuttavia, come emerge dalla figura seguente, il posizionamento relativo delle diverse categorie di operatori, sulla base dell'autovalutazione, risulta alquanto eterogeneo. In particolare, le LSI, gli istituti di pagamento (IP) e gli istituti di moneta elettronica (IMEL) sembrano più avanti nell'attuazione del processo di rafforzamento in corso, anche per effetto delle previsioni e dei requisiti già esistenti[12]. Tempi più lunghi appaiono invece necessari per gli altri intermediari, ad esempio quelli di più recente costituzione come le piattaforme di *crowdfunding*.

Figura 1

Livello di adeguamento a DORA



Fonte: elaborazione della Banca d'Italia sul posizionamento delle entità finanziarie in base alle autovalutazioni ricevute, dove si evidenzia la percentuale di completamento degli interventi necessari, da 0 per cento a 100 per cento.

In particolare, i profili di maggior attenzione riguardano:

a. per il rischio ICT, i sistemi di controllo e di monitoraggio della sicurezza delle infrastrutture informatiche, i meccanismi automatizzati per isolare i patrimoni informativi colpiti in caso di attacchi informatici, i processi di apprendimento organizzativo dei risultati emersi a seguito di incidenti ICT[13] e dei test interni;

b. per il rischio di terza parte, l'adeguamento dei contratti con i fornitori.

---

12 In particolare, la *European Banking Authority* è stata molto attiva nell'emanare linee guida volte a fornire un quadro di riferimento armonizzato sulla gestione dei rischi ICT (v. ad esempio le *EBA Guidelines on ICT and Security Risk Management*, le *EBA Guidelines on outsourcing*, *EBA Guidelines on major incidents reporting under PSD2*).

13 Le evidenze a disposizione della Vigilanza confermano una progressiva crescita degli incidenti, soprattutto di tipo informatico, e un aumento del numero di intermediari coinvolti nel singolo evento così come di fornitori terzi, a conferma dell'elevata interconnessione del sistema (cfr https://www.bancaditalia.it/media/notizia/framework-segnaletico-di-vigilanza-degli-incidenti-operativi-o-di-sicurezza-analisi-orizzontale-2024/). Le tendenze esposte nel report 2024 risultano confermate dai primi dati riferiti al 2025.

Le evidenze emerse dall'autovalutazione sono in linea con quanto da noi rilevato nell'ambito della ordinaria attività sugli intermediari vigilati. Analogamente, gli approfondimenti condotti sui principali fornitori evidenziano differenti gradi di allineamento alla normativa, confermando che il processo di adeguamento a DORA richiede ulteriori progressi anche da parte loro.

In estrema sintesi, l'azione svolta finora dalla Vigilanza ha consentito:

a. agli intermediari vigilati, di beneficiare di informazioni aggiuntive utili ai fini di valutazione della propria politica di esternalizzazione e del servizio reso dai propri fornitori;

b. ai fornitori di approfondire i margini di miglioramento esistenti dal punto di vista organizzativo, della *governance* e della gestione dei relativi rischi, oltre che delle responsabilità contrattuali, nonché di intraprendere il superamento delle residue criticità.

4. Le attività future

L'innovazione tecnologica è ormai inarrestabile e ha modificato i profili di rischio e i tradizionali criteri di valutazione dell'esposizione complessiva al rischio, dei relativi presidi di controllo, e dei possibili maggiori rischi di contagio a causa della crescente interconnessione del sistema. I cosiddetti 'anelli deboli' della catena del valore possono infatti rappresentare un fattore critico nel favorire attacchi malevoli, con effetti di contagio potenzialmente tanto più ampi quanto più elevata è l'interconnessione nel sistema.

Il ruolo dei fornitori è cruciale in questo percorso verso la resilienza digitale. Nell'ambito dell'*oversight framework* introdotto da DORA, le Autorità di vigilanza europee interagiranno direttamente con i *providers* a maggior rilevanza. L'iter per l'individuazione di questi fornitori è in corso presso le tre Agenzie europee incaricate del regime di sorveglianza (*European Banking Authority*, *European Securities and Markets Authority, European Insurance and Occupational Pensions Authority*)[14] e si concluderà entro la fine del 2025.

Il nuovo quadro regolamentare prevede, in particolare, che le terze parti critiche debbano attenersi alle raccomandazioni formulate dalle autorità responsabili, che in caso di inottemperanza da parte dei fornitori sono tenute a informare gli intermediari-clienti circa i connessi potenziali rischi, e ad adottare le iniziative più opportune per sollecitarli a riconsiderare le politiche di esternalizzazione.

Questo meccanismo può favorire un potenziale ribilanciamento del potere contrattuale tra le due parti del rapporto di fornitura, oggi spesso sbilanciato a favore di

---

14 Per maggiori dettagli sul processo previsto, si rinvia alla *roadmap* resa nota in un comunicato congiunto da parte delle autorità europee: https://www.eba.europa.eu/publications-and-media/press-releases/esas-provide-roadmap-towards-designation-ctpps-under-dora

grandi operatori del settore ICT, con potenziali benefici in termini di sicurezza informatica, trasparenza contrattuale e resilienza complessiva del sistema.

Il percorso verso la resilienza digitale è già stato avviato, seppur con velocità differenziate. Rimangono aree di attenzione sia nei sistemi di controllo degli intermediari, sia nell'operatività dei fornitori, che rappresentano per noi profili prioritari di intervento, per favorire il progressivo allineamento al nuovo quadro di riferimento.

Il patrimonio di informazioni e di analisi a disposizione della vigilanza sui profili di resilienza digitale è dunque ampio e agevola un approccio proporzionale basato sul rischio. Resta fermo che, nei confronti degli operatori che presentano disallineamenti più significativi, unitamente al perdurare di debolezze già emerse dalle analisi di vigilanza pregresse, saranno adottati gli opportuni interventi per accelerare le azioni di rimedio.

È nostra intenzione continuare a promuovere un dialogo costruttivo con le 'terze parti' e con i soggetti vigilati, attraverso un percorso di crescente consapevolezza che tenga conto delle nuove sfide di mercato, dei maggior presidi chiesti dal nuovo quadro normativo e dell'esigenza di favorire soluzioni sostenibili e proporzionali per la gestione del rischio IT.

5. Conclusioni

L'innovazione tecnologica rappresenta ormai una leva strategica per espandere e migliorare i servizi prestati alla clientela, per salvaguardarne la fiducia e preservare quindi la sostenibilità dei modelli operativi degli intermediari. L'innovazione tecnologica, se ben governata, rappresenta quindi un'opportunità per migliorare l'efficienza, la trasparenza e la competitività del sistema finanziario.

È quindi essenziale che gli intermediari adottino un approccio strategico, capace di coniugare innovazione e solidità. I risultati economici favorevoli degli ultimi anni sono anche il riflesso dei benefici derivanti dall'innovazione, ma non sarebbe appropriato considerarli necessariamente sostenibili nei prossimi anni e perseguibili da tutti gli intermediari.

In un contesto a crescente competitività, la resilienza digitale diviene quindi un fattore strategico che non può prescindere da una solida cultura del rischio in tutti i livelli aziendali. Occorre pertanto continuare a investire non solo in tecnologie, ma anche nella formazione continua del personale e nella consapevolezza organizzativa.

L'innovazione tecnologica sta modificando anche l'attività della supervisione, nello sviluppo di strumenti più sofisticati per il monitoraggio dei rischi, nella ricerca di maggiore semplificazione delle regole e delle prassi di vigilanza, nell'esigenza di integrazione e collaborazione fra professionalità e competenze di diversa estrazione, nell'utilizzo di tutte le basi informativi disponibili.

Il rafforzamento della resilienza digitale deve essere visto quindi come un obiettivo comune, da perseguire attraverso un ecosistema integrato, in cui tutti gli attori – pubblici

e privati – sviluppino e perseguano buone pratiche, adottino metriche comuni e sistemi di controllo omogenei. Le regole e l'attività di vigilanza favoriscono proprio lo sviluppo dell'eco-sistema verso queste direttrici, mediante anche l'adozione di misure di prevenzione e di risposta condivise.

La Banca d'Italia continuerà a svolgere un ruolo proattivo nel guidare il sistema finanziario verso una maggiore maturità digitale, promuovendo un approccio collaborativo tra operatori, fornitori e autorità, volto a rafforzare la fiducia nel sistema.

Grafica a cura della Divisione Editoria e stampa della Banca d'Italia