BANCA D'ITALIA
EUROSISTEMA

La sfida della governance: i nuovi rischi e l'esperienza di vigilanza

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

Convegno ABI 'Supervision, Risks and Profitability 2024'

Milano, 12 giugno 2024

Introduzione

Riportando indietro l'orologio di cinque anni, pochi avrebbero potuto pensare che in questo breve lasso di tempo la nostra società avrebbe attraversato i profondi mutamenti cui abbiamo assistito: una pandemia, guerre, un ritorno prepotente dell'inflazione con la conseguente decisa risposta delle autorità monetarie, la messa in discussione del sistema di cooperazione multilaterale che tanto ha contribuito alla globalizzazione.

Il mercato sta assistendo a modifiche strutturali nei modelli operativi per cogliere le nuove opportunità di *business*; deve inoltre fronteggiare e limitare l'impatto di nuove tipologie di rischio derivanti dalla maggiore interconnessione con operatori anche non regolamentati, come ad esempio il rischio *cyber*.

Il quadro regolamentare e le aspettative di vigilanza sono cambiate molto per adeguarsi ai mutamenti in corso e la supervisione ha lavorato intensamente per rafforzare la cultura del rischio e per stimolarne la diffusione all'intera struttura aziendale e al complesso dei processi operativi, nella consapevolezza che il ruolo della *governance* è cruciale per orientare le scelte, le azioni e i presidi interni e supportare così modelli operativi sostenibili nel tempo.

Oggi vorrei soffermarmi su tre profili di rischio che stanno assumendo crescente importanza nel sistema finanziario: il rischio organizzativo, il rischio informatico e il rischio cyber. Descriverò poi le aspettative e le azioni di vigilanza intraprese al riguardo.

L'evoluzione del sistema finanziario

La situazione del sistema bancario italiano è migliorata nel corso degli ultimi anni grazie a diversi fattori: gli investimenti effettuati e i conseguenti recuperi di efficienza; l'azione coordinata delle autorità; la fase congiunturale che crea le condizioni per prepararsi a gestire in modo robusto eventuali momenti critici futuri.

I cambiamenti strutturali in corso favoriscono inoltre lo sviluppo del mercato finanziario e agevolano la realizzazione della doppia transizione, 'verde' e 'digitale'. Mutano in misura significativa anche le preferenze e i comportamenti della clientela e, di conseguenza, i prodotti offerti e i relativi canali distributivi. Modelli operativi tradizionali, basati su reti di sportelli, si stanno trasformando velocemente in un ecosistema complesso di servizi digitali, prestati da operatori diversi, eterogenei per caratteristiche, dimensioni e sistemi di controllo. Aumentano conseguentemente anche i rischi informatici e *cyber*, accentuati dal complesso contesto geopolitico.

Il percorso verso nuovi equilibri non è privo di rischi. Nuovi soggetti entrano nel mercato, spesso collocandosi all'esterno del perimetro vigilato, ovvero con regimi prudenziali molto diversi e non di rado disomogenei a livello internazionale. Cresce la collaborazione strategica e operativa tra gli operatori finanziari e tra questi e le imprese non finanziarie, grazie anche allo sviluppo tecnologico, che aumenta la gamma di prodotti e servizi offerti, con benefici in termini di costi e di capacità di soddisfare i bisogni della clientela.

Assistiamo dunque a una progressiva segmentazione della "catena del valore", con la scomposizione dei processi produttivi in attività sempre più elementari, ma strettamente legate tra loro. Cresce così il livello di interconnessione del sistema finanziario e il conseguente grado di dipendenza operativa che ciascun intermediario sperimenta nei confronti di un numero crescente di controparti, finanziarie e non, talvolta anche di dimensioni elevate e legate a una molteplicità di soggetti.

La complessità del quadro di riferimento aumenta in modo trasversale il rischio organizzativo, inteso come la difficoltà degli intermediari di identificare strategie efficaci e di adattare la struttura organizzativa e i relativi processi interni in modo da assicurare, in un contesto mutevole, la sostenibilità del modello operativo nel lungo periodo.

In questo quadro, i rischi informatici assumono crescente rilevanza in quanto possono compromettere il modello operativo; emerge l'esigenza di considerare il rischio IT come un profilo autonomo e centrale per la valutazione della sostenibilità della complessiva attività che richiede l'introduzione di presidi interni, nella consueta articolazione in tre linee di difesa.

Il crescente ricorso all'outsourcing IT da parte di intermediari di tutte le dimensioni, come anche il maggior utilizzo di servizi *cloud* offerti da terzi, spesso in combinazione con altri prodotti, può rappresentare di certo una soluzione efficiente per conseguire risparmi e per l'acquisizione di competenze altrimenti non disponibili. Tuttavia, non può accompagnarsi all'attenuazione dei relativi meccanismi di governo, che vanno mantenuti e adattati al differente perimetro a rischio.

Il segmento degli outsourcer IT presenta inoltre una forte concentrazione, con operatori di dimensioni elevate, anche rispetto alle entità servite; ciò comporta un aumento del rischio di 'terza parte', sia a livello di singola entità (con pochi fornitori che offrono una pluralità di servizi a uno stesso intermediario) sia di sistema (pochi *provider* che supportano molti intermediari).

L'attuale contesto geopolitico determina la crescente importanza anche della resilienza cibernetica[1], cioè la capacità degli operatori di garantire la continuità operativa, adattandosi alle possibili minacce e sviluppando le misure necessarie a superare gli eventi *cyber*, contenendone impatti e costi.

Assistiamo infatti all'espansione della superficie soggetta al rischio *cyber*, la cui gestione si articola in varie fasi (*identify; protect; detect; respond; recover)*[2], ognuna delle quali richiede soluzioni tecniche e organizzative specifiche. Aumenta pertanto il possibile impatto sull'integrità dei dati e sui processi operativi degli intermediari derivante da interruzioni di fornitura, per debolezze operative o per incidenti *cyber*, tenuto anche conto delle difficoltà di gestire eventuali sostituzioni del fornitore colpito in tempi (e a costi) ragionevoli. Il numero di incidenti gravi segnalati dagli intermediari nazionali è aumentato in misura rilevante, denotando esigenze di rafforzamento dei presidi, di aggiornamento di procedure e sistemi informativi e di investimenti nelle competenze del personale.

L'azione di vigilanza

Il ciclo di valutazione SREP riferito al 2023 ha posto in evidenza alcune tendenze comuni: pur dando atto dei miglioramenti indotti dall'attuale fase congiunturale e dei progressi raggiunti sui profili tecnici quantitativi, la qualità della *governance* resta un punto di attenzione nelle valutazioni e nell'azione di vigilanza.

È questa probabilmente la principale lezione emersa dalla supervisione: la crisi di un intermediario è spesso riferibile a debolezze negli assetti di governo e controllo, nonché alla inadeguata gestione dei conflitti di interesse. Tali situazioni influenzano negativamente, talvolta con un certo ritardo, la situazione economico-patrimoniale degli intermediari, riflettendosi ad esempio in un peggioramento della qualità dei crediti erogati ovvero nel deterioramento dei profili tecnici per l'ingresso in mercati complessi senza la necessaria consapevolezza dei rischi potenziali e delle implicazioni operative e di controllo.

L'attenzione della vigilanza sui profili di *governance* è sempre stata molto elevata, al fine di stimolare la diffusione di un'adeguata cultura del rischio nell'organizzazione aziendale. La capacità di definire livelli di appetito al rischio coerenti con gli obiettivi di lungo periodo individuati dall'alta Direzione, di adeguarvi i meccanismi incentivanti così come anche i sistemi di controllo interno, formano infatti da tempo oggetto del dialogo di vigilanza, sia con gli intermediari maggiori che con quelli di più ridotte dimensioni. Grazie anche a una rigorosa disciplina sulle parti correlate, la dimensione dei conflitti di interesse che possono generarsi nelle relazioni d'affari tra esponenti e intermediari è oggetto di attento scrutinio, sia nella valutazione dell'adeguatezza quali-quantitativa degli organi apicali, sia con riferimento a specifiche situazioni per le quali è stato necessario richiedere l'adozione di *policy* dedicate.

---

1 FSB Cyber Lexicon – 2023 update.

2 NIST - Cybersecurity Framework's five Functions.

La centralità degli assetti di governo e controllo è anche confermata dalla numerosità e dalla frequenza delle misure qualitative adottate nell'ambito delle decisioni SREP. Nella quasi totalità dei casi, le banche *significant* italiane hanno visto applicate misure della specie; circa il 20 per cento di queste riguarda espressamente profili di *governance*, quali ad esempio la composizione e il funzionamento degli organi di governo e controllo; il rafforzamento del *risk management*; la verifica di adeguate *policy* interne e di codici di condotta.

Analoga evidenza riguarda intermediari bancari e finanziari sottoposti alla nostra diretta supervisione: misure qualitative hanno riguardato oltre la metà delle situazioni, e hanno avuto a oggetto il rafforzamento dei controlli di secondo livello, del funzionamento di Collegio Sindacale e dell'Internal Audit, il miglioramento del *reporting* verso l'organo di gestione e/o il Comitato Rischi.

Abbiamo inoltre promosso iniziative a livello nazionale volte a rafforzare la consapevolezza dell'industria su tali temi, ad esempio, sulla composizione e sul funzionamento degli organi amministrativi e sui requisiti degli esponenti[3]. Abbiamo a questo proposito programmato a breve un ulteriore confronto con l'industria nell'ambito degli approfondimenti in materia di valutazioni sui requisiti di professionalità e onorabilità.

Una *governance* efficiente è necessaria anche per gestire i rischi tecnologici. Mi riferisco in particolare ai controlli richiesti dalla normativa sull'operatività in cripto-attività e in materia di rischi IT, nonché ai temi di *data governance*.

Il primo esempio riguarda la nuova disciplina prevista dal Regolamento europeo sul mercato delle criptoattività (MiCAR) e, in particolare, le norme di secondo livello in via di completamento a cura dell'EBA e dell'ESMA. Ci aspettiamo che gli intermediari siano in grado di identificare, misurare e monitorare efficacemente i rischi associati a nuove attività e servizi, dedicando particolare attenzione alle relazioni con fornitori fortemente specializzati.

Accanto ai più tradizionali rischi di liquidità e riciclaggio, sarà infatti necessario porre attenzione a profili più specifici, quali quelli connessi con la custodia dei *wallet* e con il funzionamento della stessa infrastruttura dei registri elettronici distribuiti (*Distributed Ledger Technologies* – DLT). In particolare, la custodia di *asset* digitali rappresenta una sorta di collegamento tra l'intermediazione tradizionale e la finanza digitale anche per intermediari di piccola dimensione che vogliono 'testare' la nuova operatività limitando – solo apparentemente – i relativi rischi assunti. La sicurezza, la trasparenza e la continuità operativa delle soluzioni tecnologiche adottate dovranno essere pertanto attentamente valutate. In prospettiva, l'operatività dei Crypto Asset Service Providers (CASP), che potranno offrire a intermediari vigilati ovvero alla clientela finale una serie di servizi di diversa natura, potrà porre elementi di attenzione legati alla potenziale concentrazione delle attività ovvero alla connessione con piattaforme localizzate anche in altri paesi.

---

3 Orientamenti della Banca d'Italia sulla composizione e sul funzionamento dei consigli di amministrazione delle LSI (2022); Orientamenti in materia di valutazione dei requisiti e criteri di idoneità allo svolgimento dell'incarico degli esponenti aziendali delle banche LSI, degli intermediari finanziari, dei confidi, degli istituti di moneta elettronica, degli istituti di pagamento, delle società fiduciarie e dei sistemi di garanzia dei depositanti (2023).

Il secondo esempio della rilevanza dei rischi IT riguarda il Regolamento in materia di resilienza operativa (DORA), che fornisce ulteriori indicazioni concrete circa l'esigenza di rafforzamento del governo dei rischi tecnologici. L'ampio ricorso all'outsourcing di servizi IT sposta al di fuori dei soggetti vigilati l'operatività, ma non la relativa responsabilità. Il coinvolgimento di 'terze parti' di fatto amplia il perimetro da presidiare per gestire al meglio i rischi informatici. Questa è la logica che ispira la nuova normativa europea sulla *operational resilience*: si ampliano poteri e prerogative nei confronti delle 'terze parti' critiche, ma si ribadisce l'importanza di adottare un sistema di controlli integrato in materia di rischi informatici, in modo da assicurare l'adeguato governo dei dati e la gestione consapevole dei servizi forniti da soggetti esterni.

La supervisione sta usando un'ampia gamma di strumenti e interventi volti a presidiare il rischio IT, ivi incluse le autovalutazioni degli intermediari e le verifiche ispettive mirate per questa tipologia di rischio. Inoltre, il Meccanismo di Vigilanza Unico (MVU) sta svolgendo l'esercizio di *cyber stress test* per le banche significative europee, che affronta in particolare le fasi relative alla capacità di 'risposta' e 'ripresa' in caso di attacco cibernetico. Sulla gestione dei rischi connessi con l'utilizzo dei servizi *cloud*, sono inoltre state pubblicate per la consultazione le nuove linee guida del MVU[4].

Il terzo esempio che vorrei trattare riguarda la *data governance*. La capacità di gestione del dato è al centro dei processi decisionali, della pianificazione strategica e operativa e del *risk management*; ne determina la qualità e la robustezza, ne garantisce l'affidabilità e la capacità previsiva.

Lo stiamo osservando ad esempio nelle valutazioni dei piani di *funding* e dei *business plans*, dove analisi di scenario non sempre accurate e indisponibilità di dati e metodologie adeguate rischiano di condurre alla formulazione di scelte strategiche e operative poco realistiche o inappropriate. Qualità e disponibilità dei dati svolgono inoltre un ruolo centrale nella progressiva estensione di strumenti di intelligenza artificiale, anche di tipo generativo, sempre più utilizzati a supporto dei processi decisionali e della definizione delle strategie. Algoritmi molto sofisticati alimentati con dati inaccurati, obsoleti, incoerenti, possono produrre risultati inutilizzabili ovvero distorsivi; occorre evitare il rischio di deresponsabilizzazione dei vertici aziendali rispetto a questi modelli, nei quali la componente umana deve mantenere un ruolo pregnante, anche in relazione ai profili etici in gioco. Infine, la semplice carenza di dati, come si sta sperimentando sul fronte della transizione climatica, può spingere gli intermediari a ricorrere a integrazioni provenienti da fonti esterne, sulle quali però non muta la responsabilità degli utilizzatori in termini di garanzie di affidabilità e limiti delle informazioni in uso.

L'attenzione della vigilanza sulla gestione e aggregazione delle informazioni si è rafforzata nel corso degli anni, anche nell'ambito del MVU, in particolare con riferimento al rispetto dei principi emanati dal Comitato di Basilea nel 2013 che ribadiscono l'esigenza di dotarsi di adeguati meccanismi di raccolta, gestione e aggregazione dei dati di rischio[5].

---

4 ECB consults on outsourcing cloud services.

5 Cfr. BCBS 'Progress in adopting the Principles for effective risk data aggregation and risk reporting'; BCE 'Guide on effective risk data aggregation and risk reporting'.

Nostre analisi sul grado di effettiva attuazione di questi principi a livello nazionale evidenziano che, indipendentemente dalla dimensione, le aree più critiche sono rappresentate dalla *governance*, dall'architettura dei dati e dall'infrastruttura IT (sistemi IT obsoleti o inefficienti per effetto di stratificazioni successive non accompagnate da una fase di razionalizzazione delle infrastrutture; scarsa interoperabilità tra le procedure, ecc.). Di conseguenza, la Vigilanza si aspetta che gli intermediari includano questi profili tra le priorità strategiche e valutino l'entità e la sostenibilità degli investimenti necessari.

L'esperienza operativa ci insegna dunque che il rischio organizzativo, nelle sue diverse manifestazioni, va adeguatamente e tempestivamente gestito, per non incorrere in situazioni di difficoltà. Per questo continueremo a rafforzare la nostra azione sulla *risk culture,* agendo con gli strumenti ed entro i margini previsti dal quadro regolamentare.

Il principio di proporzionalità, che già trova diverse applicazioni (ad esempio negli obblighi di reporting ridotti per le '*small and non-complex institutions*', ovvero nelle semplificazioni del processo di valutazione annuale di vigilanza, ove ne ricorrano i presupposti), deve essere declinato sulla base del rischio specifico dell'intermediario e tenendo conto del possibile contagio al resto del sistema, con l'obiettivo ultimo di preservare stabilità e fiducia della clientela.

Chiudo queste riflessioni toccando un elemento trasversale rispetto ai profili trattati: la disponibilità di risorse adeguate per affrontare l'evoluzione in atto. Competenze specialistiche, ora rare e difficili da trattenere, devono essere sviluppate in linea con le tendenze di mercato, al fine di cogliere le opportunità emergenti comprendendo tuttavia i relativi rischi. È questo un tema sensibile anche per i supervisori: i rischi dell'innovazione richiedono anche competenze ed esperienze specifiche, che spesso presuppongono il rafforzamento delle forme di collaborazione all'interno delle istituzioni e con altre autorità nazionali e internazionali.

Considerazioni conclusive

L'evoluzione delle condizioni di mercato e del modello operativo degli intermediari è sempre più complessa e difficile da valutare per gli operatori e per le autorità di controllo. Gli elementi di incertezza sono numerosi, ma il sistema ha dimostrato una elevata resilienza nell'affrontare situazioni di crisi.

Lo sviluppo di partnership e collaborazioni sempre più intense con operatori non tradizionali promuove la segmentazione della "catena del valore" e dei processi produttivi aumentando l'interconnessione tra i soggetti presenti sul mercato, finanziari e non. L'innovazione tecnologica offre opportunità di rilievo, i cui benefici possono tuttavia essere massimizzati solo avendo la capacità di mantenere modelli operativi sostenibili e credibili nel tempo, anche per preservare la fiducia della clientela, un bene prezioso, ma fragile.

L'esperienza concreta di vigilanza, italiana e internazionale, dimostra che situazioni di difficoltà hanno in ultima analisi origine in debolezze degli assetti di governo e controllo: una buona *governance* non è pertanto soltanto il primo presidio nei confronti

dei rischi, ma è essa stessa un fattore competitivo su cui investire risorse economiche e professionali. È necessario aggiornare le competenze umane, fattore di successo in contesti incerti e mutevoli.

L'azione della vigilanza prudenziale resta focalizzata sull'identificazione e sul monitoraggio dei rischi, prescindendo dalla forma tecnica delle operazioni e dalla forma giuridica degli intermediari coinvolti, al fine di mantenere una valutazione integrata della sostenibilità dei modelli operativi, nel rispetto dei principi di sana e prudente gestione. Sulla base dell'esperienza operativa, aggiorniamo nel continuo le nostre metodologie, contribuiamo alla revisione degli standard prudenziali e definiamo le modalità implementative degli interventi di vigilanza, adattandole all'evoluzione del contesto operativo, tecnologico e regolamentare.

Il nostro sistema finanziario è da molto tempo in una fase di transizione e non è nuovo a dover gestire gli effetti dell'innovazione. Permettetemi qui di richiamare integralmente i messaggi lungimiranti che Vincenzo Desario diede al sistema in un convegno sull'E-banking parlando della 'frammentazione della catena del valore' in atto: '*Il sistema creditizio è di fronte a una sfida: è chiamato a verificare l'adeguatezza degli assetti organizzativi e del sistema dei controlli interni; a monitorare e prevenire i possibili rischi; a ripensare i sistemi di formazione e gestione delle risorse umane*.' Si tratta di messaggi ancora validi, a quasi 25 anni di distanza.

Il sistema finanziario ha nel tempo dimostrato la capacità di realizzare progressi rilevanti; questi risultati ci consentono di mantenere una prospettiva positiva, necessaria per accogliere nuove sfide senza trascurare i relativi rischi.

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