RISK MANAGEMENT E BANCHE

Paola Ferretti
A.A.2023-2024

paola.ferretti@unipi.it

Interazione tra rischi operativi e altre forme di rischio

- La digital transformation che sta sempre più coinvolgendo le economie moderne non manca di produrre cambiamenti anche sugli intermediari bancari, in termini di business model, di condizioni di efficienza operativa, di assetto organizzativo e distributivo, di politiche commerciali nei confronti della clientela, con intuitive ripercussioni (positive) sul business e sulla redditività, così come sul loro posizionamento competitivo nei mercati di riferimento.
- Si tratta in buona sostanza dell'opportunità di trarre vantaggio dalla trasformazione digitale: ciò pare possibile solo in presenza di una solida governance interna, in grado di indirizzare efficacemente le scelte aziendali verso lo sviluppo e l'implementazione di strategie per l'innovazione (e non solo).
- È questa la via per raggiungere ambiziosi obiettivi di redditività e di creazione di valore, da considerare congiuntamente all'esigenza di presidiare i correlati rischi. Le banche sono chiamate infatti a prestare grande attenzione alle sfide poste dalla trasformazione digitale, compresa la rischiosità che ne deriva, allo scopo di assicurare la tenuta dei propri modelli di business.

Segue

- Il rischio e la sua gestione rappresentano ancora una volta i fattori determinanti, insieme ad altri, sui cui poggiare le prospettive di consolidamento e di crescita della banca dei giorni nostri, sempre più dipendente dai sistemi informativi, dai servizi forniti da terzi e dalle tecnologie innovative.
- La questione, ribadita anche in termini di priorità della vigilanza europea per il periodo 2023-2025, sottolinea l'importanza, tra l'altro, della declinazione dei rischi a cui gli intermediari si espongono con la trasformazione digitale in atto, anche allo scopo di predisporre opportuni meccanismi di gestione proattiva, tali da garantire la sostenibilità delle scelte operate e del modello imprenditoriale adottato nel medio-lungo termine.
- Si aggiunga l'opportunità di considerare la digitalizzazione, tenuto conto anche dei correlati rischi, quale driver per la generazione di valore attraverso anche la gestione e il miglioramento della reputazione

Segue

- Uno dei temi centrali del cambiamento strutturale legato alla digitalizzazione è quello dell'adeguatezza dei sistemi di governo e controllo dei rischi relativi alle tecnologie dell'informazione (Information and Communication Technology – ICT) e di sicurezza.
- Nello specifico, il rischio ICT viene riferito alla possibilità di subire perdite a causa di fattori, quali la violazione della riservatezza; la carenza nell'integrità dei sistemi e dei dati; l'inadeguatezza o l'indisponibilità dei sistemi e dei dati; nel caso di cambiamento dei requisiti di contesto esterno o dell'attività, l'incapacità di sostituire l'IT in tempi e a costi ragionevoli.
- D'altra lato, il rischio di sicurezza è ricollegabile a processi interni inadeguati o errati; a eventi esterni (compresi gli attacchi informatici); a livelli di sicurezza fisica inappropriata.

Segue

- Si noti che ai fini ICAAP i rischi ICT e di sicurezza sono inquadrati, in base agli aspetti specifici via via considerati, tra i rischi operativi, reputazionali e strategici. Le disposizioni di vigilanza richiedono che il processo di gestione dei rischi in parola risulti pienamente integrato con il complessivo processo di risk management della banca. A tal fine gli intermediari sono tenuti a individuare, analizzare, misurare, monitorare e gestire i rischi ICT e di sicurezza assunti o assumibili, il cui livello deve essere mantenuto nei limiti della propensione stabiliti dalla singola banca. Deve essere altresì garantita la conformità dei sistemi e progetti ICT alla regolamentazione esterna ed interna (statuti, codici etici, etc.).

Segue

- Nell'ottica di bilanciare l'esigenza di sostenere la trasformazione digitale con quella di assicurare la cyber security, anche per conservare la fiducia del mercato nei confronti dell'operato del settore bancario e garantire la stabilità finanziaria, la vigilanza prudenziale svolge un ruolo cruciale.
- Questo risulta ulteriormente rafforzato da interventi legislativi UE sui temi della sicurezza dei servizi finanziari e della resilienza operativa digitale, tesi a fornire un quadro armonizzato a livello europeo.
- Il riferimento, per citare i provvedimenti più rilevanti, è alla Payment Services Directive - PSD2 (Direttiva UE 2015/2366 del Parlamento europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno), alla network Information Security Directive - NIS2 (Direttiva UE 2022/2555 del Parlamento europeo e del Consiglio del 14 Dicembre 2022 sulle misure per un livello comune elevato di cyber sicurezza) e al Digital Operational Resilience Act – DORA.

Segue

- DORA, in particolare, introduce requisiti per la resilienza operativa dei player, compresi anche quelli più innovativi come le piattaforme di crowdfunding. Definisce altresì i principi tesi a limitare i rischi collegati all'interconnessione del sistema finanziario con provider tecnologici e alla concentrazione in capo a uno stesso fornitore di tanti rapporti di esternalizzazione.
- Ne emerge un contesto sovranazionale che intende muoversi in modo sinergico, nella convinzione che la cooperazione tra le diverse autorità e operatori del settore finanziario risulti l'elemento cardine dello sviluppo di un approccio condiviso, in grado di favorire la gestione dei rischi ICT e di sicurezza per la più efficace risposta alle minacce e agli attacchi che possono causare severe interruzioni di operatività. Il tutto accompagnato dal potenziamento del capitale umano, delle competenze professionali e della cultura al rischio, ai fini di una piena assunzione di consapevolezza circa i rischi (oltre che le opportunità) posti dalla digitalizzazione (incluso il ricorso all'intelligenza artificiale).

Segue

- La digital transformation pone dunque al centro dell'attenzione, sia della vigilanza, sia degli operatori, anche il tema, prima richiamato, relativo all'esternalizzazione, e ai rischi connessi, quale modalità di accesso alle nuove tecnologie cui gli intermediari ricorrono per lo svolgimento delle attività e la prestazione di servizi. Ciò evidentemente accresce il grado di complessità e di interconnessione tra le istituzioni attive sul mercato finanziario, aggiungendo elementi di possibile vulnerabilità, anche su scala globale.
- In generale dunque alle banche si chiede di dotarsi di appropriati sistemi di governo dei rischi in materia di esternalizzazione e di adeguati presidi di sicurezza informatica e cibernetica. Il tutto per riuscire a garantire la continuità operativa in un contesto di stabilità complessiva.

Segue

- Il focus sui rischi operativi e le sue componenti è ribadito anche dall'EBA nel periodico documento di rilevazione dei rischi e vulnerabilità per le banche europee. In quella sede infatti viene sottolineata la persistente rilevanza del rischio operativo, evidenziandone tra i key-factors i rischi ICT e cyber, come sopra definiti, oltre che i rischi di riciclaggio e di finanziamento al terrorismo e il rischio di condotta.
- Quanto al **rischio di riciclaggio e finanziamento al terrorismo**, questo rappresenta, nell'ambito del rischio operativo, il rischio attuale o prospettico di subire perdite collegate agli impatti, anche di carattere reputazionale, che possono discendere dalle attività di riciclaggio e finanziamento al terrorismo.
- Sempre nella sfera del rischio operativo, il **rischio di condotta** viene definito come il rischio attuale o prospettico di perdite riconducibili sia a un'offerta inappropriata di servizi finanziari, in aggiunta ai relativi costi processuali, sia a casi di condotta intenzionalmente inadeguata o negligente.