

DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

APPROFONDIMENTI

Corporate governance e ruolo degli amministratori in banche ed assicurazioni

Novembre 2026

Giuseppe Guglielmo Santorsola, Professore Ordinario Senior di Asset Management, Corporate Finance e Corporate & Investment Banking; Professore a contratto di Finanza, Università Cattolica del Sacro Cuore – Piacenza





Giuseppe Guglielmo Santorsola, Professore Ordinario Senior di Asset Management, Corporate Finance e Corporate & Investment Banking; Professore a contratto di Finanza, Università Cattolica del Sacro Cuore – Piacenza

Giuseppe Guglielmo Santorsola

Giuseppe G. Santorsola è Professore Ordinario Senior di Asset Management, Corporate Finance e Corporate & Investment Banking e Professore a contratto presso l'Università Cattolica del Sacro Cuore – Sede di Piacenza-Cremona.

Le sue aree di specializzazione sono gli scenari finanziari, la finanza aziendale, l'intermediazione del risparmio individuale e collettivo, la previdenza complementare, la pianificazione successoria individuale e di impresa, la finanza sostenibile ESG, l'applicazione dei principi contabili IAS-IFRS nelle banche, il private equity e il private banking, l'antiriciclaggio e le funzioni di compliance nelle banche.

1. Introduzione e fondamenti della corporate governance

1.1 *Definizione e specificità della governance nel settore finanziario rispetto alle imprese industriali*

La corporate governance viene tradizionalmente definita come l'insieme di regole, relazioni, processi e sistemi aziendali attraverso i quali un'impresa viene diretta e controllata. Nelle imprese industriali e commerciali (*non-financial firms*), l'obiettivo primario dei meccanismi di governance risiede nella mitigazione dei conflitti di agenzia tra azionisti (proprietà) e manager (controllo), al fine di ottimizzare l'allocazione del capitale e massimizzare il valore delle azioni nel lungo periodo.

Nel settore bancario, assicurativo e degli intermediari finanziari, tuttavia, la corporate governance assume una **connotazione marcatamente differente e una complessità sistemica unica**. La specificità degli intermediari finanziari deriva da tre fattori strutturali:

1. **L'elevata leva finanziaria (leverage):** A differenza delle imprese industriali, dove il capitale proprio rappresenta una quota significativa delle fonti di finanziamento, le banche operano con un rapporto tra debito (principalmente depositi) e patrimonio netto estremamente elevato (spesso superiore a 10:1). Ciò significa che i soggetti maggiormente esposti al rischio d'impresa non sono solo gli azionisti, ma i creditori/depositanti (al netto delle protezioni di legge, ma con potenziali effetti critici sulla stabilità).

2. **L'asimmetria informativa opaca:** Gli attivi delle istituzioni finanziarie (prestiti cartolarizzati, derivati complessi, passività assicurative a lungo termine) sono intrinsecamente meno trasparenti rispetto ai beni tangibili o ai brevetti di un'impresa industriale. Valutare la qualità del portafoglio crediti di una banca o le riserve tecniche di un'assicurazione dall'esterno è estremamente difficile per il mercato.

3. **La liquidità delle passività e l'illiquidità degli attivi:** La trasformazione delle scadenze espone gli intermediari al rischio di corse agli sportelli (*bank runs*) o a crisi di liquidità sistemiche che possono propagarsi istantaneamente per effetto contagio.

Di conseguenza, la governance finanziaria cessa di essere una mera questione privata tra soci e am-

vedi l'articolo online

ministratori e diventa un **pilastro della stabilità macroeconomica**, vigilato dalle autorità pubbliche per prevenire il fallimento del mercato.

1.2 ***La teoria dell'agenzia e il paradigma multi-stakeholder: depositanti, assicurati e la stabilità sistemica***

La classica teoria dell'agenzia (Jensen & Meckling, 1976) analizza il rapporto in cui il principale (azionista) delega il potere decisionale all'agente (manager). Nelle istituzioni finanziarie, questa impostazione bidimensionale si rivela da tempo insufficiente e rischiosa (il **moral hazard** del banchiere). La presenza di una pluralità di *stakeholder* con interessi divergenti impone un **paradigma multi-stakeholder**.

- **I Depositanti e gli Assicurati:** Rappresentano i principali fornitori di capitale dell'intermediario, ma sono soggetti a un grave problema di azione collettiva e non possiedono né gli strumenti né gli incentivi per monitorare l'operato del management. La tutela dei loro interessi è delegata *ex ante* alle autorità di vigilanza e ai sistemi di garanzia dei depositi (di categoria per le BCC/CRA, nazionale e comunitario per le altre banche aderenti al FITD).

- **Lo Stato e i Contribuenti:** Poiché il dissesto di un intermediario di rilevanza sistemica (*SIFI - Systemically Important Financial Institution*) comporta costi sociali devastanti, lo Stato funge spesso da garante di ultima istanza. Ciò genera il citato fenomeno di *moral hazard* (azzardo morale): gli azionisti e i manager, sapendo di essere "troppo grandi per fallire" (*Too Big to Fail*) ed operando in prevalenza con mezzi non propri, sono incentivati ad assumere rischi eccessivi, incamerando i profitti in caso di successo e socializzando le perdite in caso di dissesto.

- **Il Regolatore/Vigilante:** Interviene come un "silenzioso ma condizionante driver", inserendo vincoli di capitale e requisiti organizzativi che limitano l'autonomia privata degli organi societari.

La governance finanziaria deve quindi bilanciare la **tutela del capitale di rischio** con la **salvaguardia dei diritti dei clienti** e la **stabilità complessiva** del sistema economico finanziario.

1.3 ***Il trade-off tra massimizzazione del valore per gli azionisti (shareholder value) e tutela dell'interesse pubblico***

La letteratura economico-giuridica ha ampiamente dimostrato che l'allineamento perfetto degli interessi dei manager a quelli degli azionisti – che nelle imprese tradizionali viene perseguito tramite stock option e bonus legati alla performance azionaria – può produrre **effetti distorsivi** in una banca o in un'assicurazione, per la presenza prevalente di crediti protetti e privilegiati .

Se il consiglio di amministrazione risponde esclusivamente alla logica dello *shareholder value*, spingerà l'intermediario verso una maggiore assunzione di rischio (*risk-taking*), poiché gli azionisti godono di una responsabilità limitata (asimmetria del profilo di payoff: **guadagni illimitati, perdite limitate** al capitale versato). Durante la crisi finanziaria globale del 2007-2008, le banche con modelli di governance focalizzati in modo aggressivo sugli interessi degli azionisti di breve termine hanno registrato le perdite più severe (*Laeven & Levine, 2009*).

I moderni sistemi di governance negli intermediari finanziari devono pertanto risolvere questo trade-off internalizzando l'interesse pubblico all'interno dei processi decisionali del Board. Ciò si traduce nella definizione di sistemi di remunerazione differiti, legati a metriche corrette per il rischio (*risk-adjusted performance measures* come il RAROC o il RORAC, differenti fra loro al denominatore – patrimonio o capitale economico nei due casi) e nell'attribuzione di responsabilità legali specifiche agli amministratori nei confronti delle autorità di vigilanza.

2. Il quadro regolamentare europeo e nazionale: banche

2.1 ***Il Single Supervisory Mechanism (SSM) e le linee guida dell'European Banking Authority (EBA) sulla internal governance***

A seguito della crisi del debito sovrano europeo, la creazione dell'Unione Bancaria ha ridisegnato l'architettura della vigilanza, accentrando il controllo sulle istituzioni significative (*Significant Institutions - SIs*) in capo alla **Banca Centrale Europea** attraverso il Meccanismo di Vigilanza Unico (SSM).

La BCE esercita la vigilanza sulla governance bancaria non solo attraverso verifiche documentali, ma

vedi l'articolo online

mediante il processo di revisione e valutazione prudenziale (**SREP - Supervisory Review and Evaluation Process**), all'interno del quale la governance e il risk management costituiscono uno dei quattro pilastri fondamentali di valutazione. Una governance carente comporta l'irrogazione di requisiti patrimoniali aggiuntivi (*Pillar 2 Requirements - P2R*) o misure restrittive sulla distribuzione dei dividendi.

A livello di normazione tecnica, l'**European Banking Authority (EBA)** emana periodicamente le *Guidelines on Internal Governance* (da ultimo aggiornate in coordinamento con l'ESMA). Queste linee guida (certamente condizionanti ma non cogenti) stabiliscono ugualmente standard stringenti in materia di:

- chiarezza della struttura organizzativa (*sound and holistic internal governance arrangements*);
- definizione delle linee di responsabilità e flussi informativi bidirezionali tra comitati e Board;
- politiche di remunerazione e incentivazione volte a non incorrere in rischi contrari al profilo di rischio della banca.

2.2 *La Direttiva CRD V e il Regolamento CRR II (con i successivi affinamenti del pacchetto CRD VI/CRR III)*

L'ossatura normativa europea della governance bancaria poggia sul pacchetto normativo composto dalla **Direttiva 2013/36/UE (CRD IV)** e dal **Regolamento (UE) n. 575/2013 (CRR)**, successivamente emendati dalla **CRD V** e dal **CRR II** nel 2019, e giunti al definitivo consolidamento con il recepimento del pacchetto **CRD VI / CRR III** (in attuazione degli ultimi accordi di Basilea 3/4).

Il testo normativo europeo impone obblighi precisi in ordine a:

1. **separazione delle funzioni:** Netta distinzione tra la funzione di gestione (esecutiva) e la funzione di supervisione strategica (non esecutiva). L'accumulo delle cariche di Presidente del Consiglio di Amministrazione e di Amministratore Delegato (*CEO duality*) è fortemente limitato e subordinato all'autorizzazione della vigilanza.
2. **tempo da dedicare alla carica (*Time Commitment*):** La direttiva fissa un tetto massimo al numero di incarichi di amministratore che un singolo soggetto può ricoprire contemporaneamente in diverse società, per garantire che la dedizione al monitoraggio della singola banca sia effettiva.
3. **capacità di sfida (*Clarity and Challenge*):** Il Board deve essere strutturato in modo da consentire un dibattito costruttivo. I membri non esecutivi devono possedere l'autonomia intellettuale e le competenze tecniche per sfidare apertamente le decisioni del management esecutivo.

2.3 *Il recepimento italiano: la Circolare 285 di Banca d'Italia e il ruolo della vigilanza prudenziale*

In Italia, le disposizioni in materia di corporate governance bancaria trovano la loro declinazione di dettaglio nella **Circolare n. 285 del 17 dicembre 2013 di Banca d'Italia** (Parte Prima, Titolo IV, Capitolo 1 "Il sistema di governo societario").

La regolamentazione italiana recepisce il modello europeo declinandolo secondo il principio di proporzionalità e classificando le banche in tre categorie (banche di maggiori dimensioni o complessità operativa, banche intermedie, banche di minori dimensioni). I punti cardine della Circolare 285 includono:

- **l'allocazione e la assegnazione dei poteri:** lo statuto deve chiaramente individuare i compiti degli organi sociali. L'organo con funzione di supervisione strategica definisce e riesamina periodicamente il modello di business, il RAF (*Risk Appetite Framework*) e la struttura organizzativa.
- **la composizione qualitativa e quantitativa:** Le banche devono effettuare un'analisi preventiva sulla composizione ottimale del Board, individuando i profili professionali necessari prima del rinnovo delle cariche in ottica di adeguata diversificazione delle competenze.
- **l'autovalutazione del Consiglio (*Board Evaluation*):** È obbligatorio condurre con cadenza annuale un processo di autovalutazione sull'efficac ia del funzionamento dell'organo, che per le banche sistemiche deve avvalersi, almeno ogni tre anni, del supporto di un consulente esterno indipendente.

vedi l'articolo online

3. La governance nel settore assicurativo

3.1 *Il framework Solvency II e i pilastri della governance assicurativa (Pilastro II)*

La corporate governance delle imprese di assicurazione e riassicurazione trova la sua matrice comunitaria nella **Direttiva 2009/138/CE (Solvency II)**, e successive modifiche, la quale ha introdotto un sistema di vigilanza economico-patrimoniale basato su tre pilastri. Mentre il Pilastro I disciplina i requisiti patrimoniali quantitativi (SCR e MCR – *Solvency e Minimum*) e il Pilastro III gli obblighi di trasparenza e informativa al mercato, è il **Pilastro II** a sancire la centralità del sistema di governo societario, considerandolo un presidio fondamentale per la solvibilità aziendale nel lungo termine.

Ai sensi di Solvency II, la governance deve garantire una gestione *sana* e prudente dell'attività attraverso una struttura organizzativa trasparente, una netta separazione delle funzioni e un sistema di trasmissione delle informazioni efficiente. Il fulcro del Pilastro II è rappresentato dal processo di autovalutazione del rischio e della solvibilità, denominato **ORSA (Own Risk and Solvency Assessment)**. L'ORSA non è un mero adempimento tecnico delegato alle funzioni attuariali, bensì uno strumento strategico sotto la diretta responsabilità dell'organo amministrativo. Con le debite differenze il processo ORSA ricopre lo stesso ruolo assegnato per le banche all'ICAAP e all'ILAAP. Il Board deve utilizzare i risultati dell'ORSA per:

- valutare il fabbisogno di solvibilità globale in relazione al profilo di rischio specifico, tenendo conto delle interdipendenze tra rischi di sottoscrizione, di mercato, di credito e operativi.
- verificare la resilienza della compagnia attraverso stress test e analisi di scenario multi-anno.
- allineare le scelte strategiche, la pianificazione del capitale e le politiche di tariffazione alla propensione al rischio deliberata.

3.2 *Ruolo e responsabilità dell'IVASS e le specificità del sistema dei controlli interni nelle assicurazioni*

A livello nazionale, l'autorità deputata alla vigilanza sul settore assicurativo è l'**IVASS** (Istituto per la Vigilanza sulle Assicurazioni), che opera in stretta coordinazione con l'EIOPA (*European Insurance and Occupational Pensions Authority*). Le disposizioni nazionali di dettaglio sulla governance sono organicamente racchiuse nel **Codice delle Assicurazioni Private (CAP - D.Lgs. 209/2005)** e, in particolare, nel **Regolamento IVASS n. 38 del 3 luglio 2018** in materia di sistema di governo societario.

La regolamentazione italiana attribuisce una responsabilità apicale e non delegabile all'organo amministrativo, delineando un sistema dei controlli interni che prevede l'istituzione obbligatoria di **quattro funzioni fondamentali di controllo**, le quali devono essere tra loro indipendenti dal punto di vista organizzativo e operativo:

1. **Funzione di Gestione dei Rischi (Risk Management):** Preposta alla strutturazione delle politiche di rischio e all'implementazione del framework ORSA.
2. **Funzione di Verifica della Conformità (Compliance):** Incaricata di prevenire il rischio di sanzioni legali, perdite finanziarie o danni reputazionali derivanti dalla non conformità a norme primarie e secondarie, con focus specifico sulla trasparenza dei prodotti e sulla tutela del consumatore (*Product Oversight and Governance - POG*).
3. **Funzione di Revisione Interna (Internal Audit):** Svolge un'attività indipendente di *assurance* e consulenza sull'adeguatezza e l'efficacia dell'intero sistema di controllo interno.
4. **Funzione Attuariale:** Una specificità esclusiva del settore assicurativo, responsabile di coordinare e monitorare il calcolo delle riserve tecniche, esprimere un parere sulla politica di sottoscrizione globale e sugli accordi di riassicurazione, contribuendo direttamente all'efficacia del risk management.

I titolari di tali funzioni dispongono di un canale di comunicazione diretto con l'organo con funzione di supervisione strategica e con l'organo di controllo (Collegio Sindacale), **bypassando se necessario il management esecutivo**.

3.3 *La gestione dei rischi biometrici, finanziari e di sottoscrizione nelle strutture di governo societario*

La natura del passivo di bilancio di un'impresa di assicurazione impone alla governance dinamiche simmetricamente opposte rispetto a quelle bancarie: mentre la banca raccoglie a breve e impiega a medio-lungo termine, l'assicurazione incassa premi certi *ex ante* a fronte di impegni di liquidazione futuri

vedi l'articolo online

e incerti *ex post*. Questa inversione del ciclo produttivo richiede che il Board possieda competenze tecniche specifiche per governare un portafoglio rischi altamente eterogeneo:

- **Rischi Biometrici e di Sottoscrizione (Ramo Vita e Danni):** Il Board deve approvare le politiche di riservazione e tariffe adeguate a fronteggiare i rischi di mortalità, longevità, morbilità e catastrofali. Il monitoraggio richiede flussi informativi costanti sull'andamento del *loss ratio* e sulla deviazione delle ipotesi demografiche/statistiche rispetto all'andamento reale del portafoglio.

- **Rischi Finanziari e di Mercato (Asset-Liability Management - ALM):** L'organo amministrativo deve governare il rischio di sfasamento temporale e quantitativo tra le attività e le passività (*mismatching*). La governance deve definire limiti stringenti alle politiche di investimento in applicazione del **principio dell'operatore prudente (*Prudent Person Principle*)**, abbandonando i vecchi vincoli quantitativi rigidi a favore di una valutazione qualitativa dei rischi di tasso, azionari, immobiliari e di spread, con particolare attenzione alla sostenibilità finanziaria delle garanzie di rendimento minimo offerte nei contratti rivalutabili.

4. Gli intermediari finanziari non bancari (ex art. 106 TUB) e le SGR

4.1 *Il principio di proporzionalità nell'applicazione delle regole di governance*

L'universo degli intermediari finanziari non bancari comprende una platea eterogenea di soggetti: intermediari finanziari vigilati iscritti all'albo unico di cui all'**art. 106 del Testo Unico Bancario (TUB)** (società di leasing, factoring, credito al consumo, confidi maggiori), i soggetti operanti nel comparto dei servizi di pagamento (IP ed IMEL) e le società di gestione del risparmio (**SGR**), regolate dal **Testo Unico della Finanza (TUF)**.

Per questi operatori, il legislatore europeo e le Autorità di Vigilanza nazionali (Banca d'Italia e Consob) applicano rigidamente il **principio di proporzionalità**. Tale principio stabilisce che l'architettura organizzativa, i presidi di controllo, i requisiti dimensionali degli organi e i relativi flussi informativi debbano essere strettamente calibrati in base a:

- natura, portata e complessità delle attività effettivamente esercitate.
- dimensioni patrimoniali e volume delle transazioni intermediate.
- profilo di rischio intrinseco del modello di business operativo.

Sulla scorta di questo impianto, Banca d'Italia classifica gli intermediari ex art. 106 TUB in differenti fasce dimensionali e di complessità (intermediari "maggiori" o a rilevanza sistemica vs intermediari "minori"). Se per i primi i requisiti organizzativi tendono ad assimilarsi a quelli previsti per le banche commerciali minori (**obbligo di comitati endoconsiliari tecnici, funzioni di controllo interne separate e strutturate**), per i secondi è **consentito l'accentramento delle funzioni di controllo o l'*outsourcing* societario**, purché siano costantemente preservate l'efficacia del monitoraggio e la responsabilizzazione del Board.

4.2 Struttura organizzativa e presidi di controllo per gli intermediari finanziari ed i soggetti del risparmio gestito (TUF)

Nelle Società di Gestione del Risparmio (SGR), la corporate governance assume una configurazione peculiare derivante dalla netta separazione giuridica ed economica tra il **patrimonio proprio della società** e i **patrimoni dei fondi comuni d'investimento** (o dei portafogli individuali) da essa gestiti.

Il quadro regolamentare congiunto Banca d'Italia-Consob (attuativo della Direttiva UCITS V e della Direttiva AIFMD II) impone presidi specifici volti a mitigare il rischio di condotta e a prevenire i conflitti di interesse sistemici tra la SGR, gli azionisti di controllo e i partecipanti ai fondi. I pilastri della governance nel risparmio gestito includono:

- **la Governance del Rischio di Investimento:** Accanto alla funzione di risk management aziendale, la SGR deve strutturare un presidio gerarchicamente indipendente deputato al controllo del rischio dei prodotti finanziari gestiti, verificando quotidianamente il rispetto dei limiti di leva finanziaria, la concentrazione degli attivi, il rischio di controparte e il profilo di liquidità dei fondi (*liquidity stress testing*), a tutela esclusiva degli investitori.

- **la separazione fisica e funzionale della custodia:** Il Board deve assicurare la corretta interazione con il **Depositario** (soggetto terzo indipendente), incaricato della custodia degli attivi del

vedi l'articolo online

fondo e del controllo di legittimità sulle operazioni di emissione e rimborso delle quote.

- **la gestione dei conflitti di interesse nelle operazioni intergruppo:** Nel caso di SGR appartenenti a gruppi bancari o assicurativi, la governance deve dotarsi di procedure stringenti per garantire che le transazioni (es. acquisto di titoli collocati da consociate) avvengano a condizioni di mercato e nell'esclusivo interesse dei sottoscrittori dei fondi, azzerando le asimmetrie e le rendite di posizione.

5. La composizione e il funzionamento degli organi sociali

5.1 *I requisiti di Fit & Proper (onorabilità, professionalità, indipendenza e competenza) alla luce dei decreti ministeriali più recenti*

La qualità della corporate governance degli intermediari finanziari dipende in via prioritaria dall'idoneità dei soggetti chiamati a guidarli. A livello nazionale, il recepimento delle direttive europee (CRD V,,in prospettiva CRD VI e Solvency II, in prospettiva Solvency III) ha trovato la sua massima espressione nell'impianto normativo del **Decreto del Ministero dell'Economia e delle Finanze (MEF) n. 169/2020** per il settore bancario e creditizio, e nelle corrispondenti disposizioni IVASS per le assicurazioni.

La valutazione *Fit & Proper* non si limita più a una mera verifica formale dei requisiti di onorabilità (assenza di condanne penali o procedimenti concorsuali), ma si estende a un'analisi sostanziale e dinamica articolata su quattro pilastri fondamentali:

1. **professionalità:** Gli esponenti devono possedere un'esperienza pregressa (teorica e pratica) in posizioni di responsabilità e in settori coerenti con la complessità dell'intermediario.
2. **indipendenza di giudizio (*Independence of Mind*):** Tutti i membri del Board, a prescindere dal possesso dei requisiti formali di indipendenza qualificata, devono agire con autonomia intellettuale, integrità e coraggio morale, ponendosi in una condizione che consenta loro di porre quesiti stringenti (*challenge*) e di esprimere un dissenso costruttivo rispetto alle proposte del management esecutivo.
3. **competenza collettiva (*Collective Suitability*):** Il Consiglio di Amministrazione, valutato nel suo complesso, deve presentare una diversificazione di competenze tale da coprire tutte le aree strategiche della banca o dell'assicurazione (dalla finanza quantitativa alle tecnologie digitali, dalla regolamentazione legale ai fattori ESG).
4. **disponibilità di tempo (*Time Commitment*):** Gli esponenti devono garantire il tempo necessario per una partecipazione attiva e preparata alle riunioni degli organi e dei comitati. La normativa fissa limiti quantitativi precisi al cumulo degli incarichi, ponderati in base alla dimensione e alla natura sistemica delle istituzioni in cui le cariche sono ricoperte.

La responsabilità della valutazione grava primariamente sull'intermediario stesso tramite il processo di *Fit & Proper Assessment* condotto dal comitato nomine, ed è soggetta alla successiva validazione e controllo formale da parte delle Autorità di Vigilanza (BCE tramite i processi unici di *Fit and Proper Assessment* o Banca d'Italia/IVASS).

5.2 *I comitati consiliari endoconsiliari obbligatori: Rischi, Nomine, Remunerazioni*

Negli intermediari finanziari di maggiori dimensioni o complessità operativa, il Consiglio di Amministrazione deve costituire al proprio interno specifici comitati con funzioni istruttorie, consultive e propositive. La presenza di tali comitati mira a garantire l'efficacia del processo decisionale su materie ad alto tasso di tecnicismo:

- **Comitato Rischi:** È l'organo endoconsiliare cardine per il monitoraggio della stabilità finanziaria dell'intermediario. Supporta il Board nella definizione del Risk Appetite Framework (RAF), valuta l'adeguatezza del sistema dei controlli interni, verifica il recepimento delle indicazioni delle Autorità di Vigilanza e analizza l'allineamento dei prodotti e dei servizi offerti al profilo di rischio aziendale.
- **Comitato Nomine:** Presiede ai processi di selezione, rinnovo e valutazione degli esponenti aziendali. Identifica i profili ottimali per la composizione del Board, gestisce i piani di successione delle posizioni chiave (*Succession Planning*) e conduce i processi periodici di autovalutazione (*Board Evaluation*).

vedi l'articolo online

- **Comitato Remunerazioni:** Ha il delicato compito di strutturare i sistemi di incentivazione del personale più rilevante (*Material Risk Takers*). Deve garantire che la componente variabile della remunerazione sia strutturata in modo da non incentivare l'assunzione di rischi eccessivi a breve termine, prevedendo quote significative di pagamento differito in strumenti finanziari (azioni o opzioni) e clausole di riduzione o restituzione (*malus* e *clawback*) ancorate a indicatori di solidità patrimoniale e di liquidità a lungo termine.

I comitati devono essere composti prevalentemente da **amministratori non esecutivi**, con una presenza maggioritaria di **membri indipendenti**, e presieduti da soggetti con comprovata **esperienza specifica nella materia** di competenza del comitato.

5.3 ***Il bilanciamento di genere, la cognitive diversity e la successione dei vertici***

La composizione degli organi sociali deve attivamente perseguire obiettivi di diversità per evitare i fenomeni di omologazione decisionale (il cosiddetto *groupthink*). Il bilanciamento di genere, inizialmente introdotto da vincoli normativi nazionali e europei, è ormai integrato nei codici di corporate governance come un fattore di mitigazione del rischio e di miglioramento della performance finanziaria.

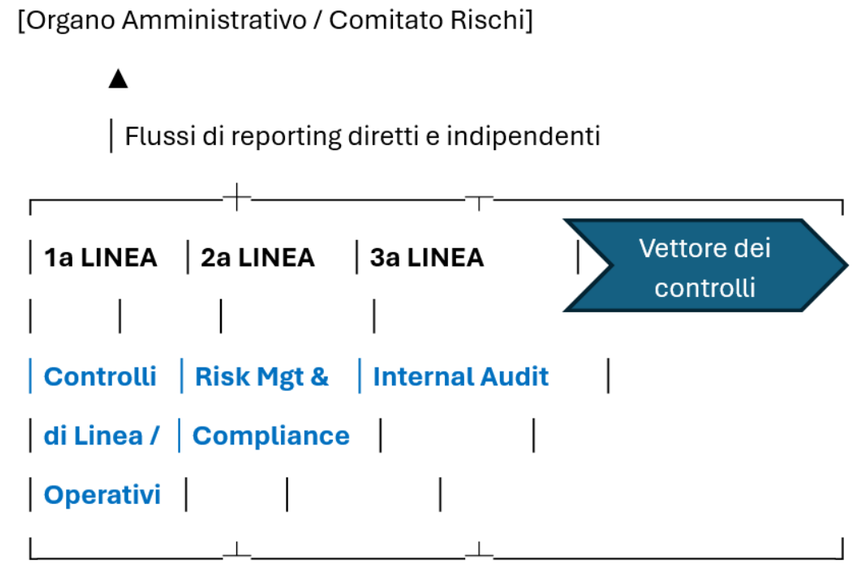
Tuttavia, la frontiera più avanzata della governance richiede la valorizzazione della **diversità cognitiva (*cognitive diversity*)**, intesa come pluralità di background culturali, percorsi di carriera, provenienze geografiche ed età anagrafiche. Un Board cognitivamente diversificato possiede una maggiore capacità di intercettare i rischi emergenti e di comprendere le evoluzioni dei mercati globali e delle tecnologie.

In questo contesto, la pianificazione della successione dei vertici (*CEO and Key Positions Succession Planning*) assume un ruolo strategico fondamentale. La governance deve dotarsi di procedure formali ed emergenziali volte ad assicurare la continuità operativa aziendale anche in caso di cessazione improvvisa del mandato dei vertici esecutivi, evitando vuoti di potere che potrebbero compromettere la fiducia del mercato e la stabilità dell'intermediario.

6. Il sistema dei controlli interni e la gestione dei rischi

6.1 ***Le tre linee di difesa: controlli di linea, Risk Management e Compliance, Internal Audit***

L'architettura dei controlli interni negli intermediari finanziari è strutturata secondo il modello internazionale delle **tre Linee di Difesa**, recepito in Italia dalla Circolare 285 di Banca d'Italia e dal Regolamento IVASS n. 38/2018:



1. **Prima Linea (Controlli di Linea od Operativi):** È costituita dalle strutture operative e di business (es. gestori della clientela, sale mercati, filiali). Sono i soggetti che originano il rischio e hanno la responsabilità primaria di identificarlo, valutarlo e monitorarlo quotidianamente, applicando le procedure operative e i limiti stabiliti dalle policy aziendali.

vedi l'articolo online

2. **Seconda Linea (Controlli sui Rischi e sulla Conformità):** È esercitata da funzioni distinte da quelle produttive. La funzione di **Risk Management** è responsabile della definizione dei metodi di misurazione del rischio e della verifica del rispetto dei limiti operativi. La funzione di **Compliance** ha il compito di verificare la conformità dei processi aziendali all'evoluzione del quadro normativo, prevenendo il rischio legale e reputazionale. Nel **settore assicurativo**, a queste si affianca la **Funzione Attuariale**.

3. **Terza Linea (Revisione Interna - Internal Audit):** È una funzione indipendente che effettua un controllo di terzo livello sull'intero sistema. Valuta l'adeguatezza e l'efficacia complessiva dell'architettura dei controlli di prima e seconda linea, l'affidabilità dei sistemi informativi e la tenuta delle procedure operative attraverso un piano di audit annuale approvato dal Board.

6.2 *Il Chief Risk Officer (CRO) e il canale di riporto diretto al Board*

All'interno del sistema di governo societario, la figura del **Chief Risk Officer (CRO)** — o Responsabile della Funzione di Gestione dei Rischi — riveste una posizione di assoluta centralità gerarchica e funzionale. Per garantire l'effettiva indipendenza del CRO dalle pressioni commerciali delle funzioni esecutive d'impresa, la normativa prevede specifici presidi di tutela:

- **nomina e revoca:** La decisione in ordine alla nomina, alla revoca e alla definizione della remunerazione deal CRO è di competenza esclusiva dell'organo con funzione di supervisione strategica (CdA), sentito il parere dell'organo di controllo (Collegio Sindacale) e del Comitato Rischi, **sottraendo tale potere all'Amministratore Delegato**.

- **autonomia informativa:** Il CRO dispone di un **canale di riporto diretto e formale** verso il Consiglio di Amministrazione e i comitati endoconsiliari, con la facoltà di **accedere a qualsiasi informazione o dato aziendale** senza alcuna mediazione da parte dei vertici esecutivi.

- **diritto di veto o escalation:** Nei sistemi di governance più robusti, al CRO è attribuito un potere di *escalation* o di parere vincolante sulle operazioni di maggiore rilievo dal punto di vista del profilo di rischio (*Material Transactions*), consentendogli di sottoporre direttamente all'attenzione del Board le decisioni aziendali che reputi non coerenti con i limiti di rischio deliberati.

6.3 *La cultura del rischio (Risk Culture) e il Risk Appetite Framework (RAF)*

Il **Risk Appetite Framework (RAF)** costituisce lo strumento quadro di governance attraverso il quale il Board determina la tipologia e il livello di rischio che l'intermediario è disposto ad assumere nel perseguimento dei propri obiettivi strategici. Il RAF si articola in diverse metriche quantitative e qualitative:

- **Risk Appetite (Propensione al rischio):** Il livello di rischio obiettivo che l'intermediario intende assumere in condizioni normali di operatività.

- **Risk Tolerance (Tolleranza al rischio):** Il margine di deviazione massimo consentito rispetto alla propensione al rischio, volto a fronteggiare situazioni di stress moderato senza compromettere la stabilità.

- **Risk Capacity (Capacità di rischio):** Il livello massimo di rischio tecnicamente assumibile dall'intermediario prima di violare i requisiti patrimoniali e di liquidità minimi di carattere regolamentare.

- **Risk Limits (Limiti operativi):** La declinazione granulare delle metriche del RAF per singole linee di business, portafogli o unità operative (es. limiti di concentrazione verso un singolo settore o controparte).

Affinché il RAF non rimanga un mero modello matematico astratto, è indispensabile che l'intermediario sviluppi e diffonda una solida **cultura del rischio (*Risk Culture*)** a tutti i livelli dell'organizzazione. La *Risk Culture* rappresenta l'insieme di valori, credenze, attitudini e comportamenti condivisi dal personale in relazione alla percezione, all'assunzione e alla gestione dei rischi d'impresa. Una cultura del rischio efficace promuove la trasparenza, incentiva la segnalazione tempestiva degli errori (*speaking-up culture*) e allinea i comportamenti individuali agli obiettivi di stabilità di lungo periodo fissati dalla governance.

vedi l'articolo online

7. Le nuove frontiere della governance: ESG, digitalizzazione e cybersecurity

7.1 L'integrazione dei fattori di sostenibilità (SFDR, Tassonomia UE, CSRD) nelle strategie del Consiglio

Negli ultimi anni, l'evoluzione della regolamentazione europea ha trasformato i fattori ambientali, sociali e di governance (**ESG**) da meri elementi di rendicontazione etica in componenti strutturali della gestione dei rischi finanziari. Per banche, assicurazioni e SGR, l'integrazione della sostenibilità è governata da tre pilastri normativi interconnessi:

- **Regolamento SFDR (oggi nella seconda versione) (Sustainable Finance Disclosure Regulation):** Impone obblighi di trasparenza sull'integrazione dei rischi di sostenibilità nei processi decisionali di investimento e nella consulenza, classificando i prodotti finanziari in base al loro grado di sostenibilità (Articoli 6, 8 e 9).

- **Regolamento Tassonomia UE:** Definisce i criteri scientifici ed "eco-logici" per stabilire se un'attività economica possa considerarsi ecosostenibile, vincolando i flussi di capitale verso la transizione green.

- **Direttiva CSRD (Corporate Sustainability Reporting Directive):** Estende l'obbligo di rendicontazione di sostenibilità a una vasta platea di imprese, introducendo il principio della **doppia materialità** (*double materiality*). La governance deve valutare non solo come i fattori ESG impattino sulle performance economiche dell'intermediario (*outside-in*), ma anche come l'attività creditizia e di investimento influenzi l'ambiente e la società (*inside-out*).

- Per completezza, esiste anche una quarta normativa la **Corporate Sustainability Due Diligence Directive** (CSDDD) ed estende gli obblighi di responsabilità e trasparenza ESG a tutta la filiera; la direttiva, nota anche con il nome di Supply Chain Act, mira a fare in modo che le aziende prendano consapevolezza e intervengano sugli impatti sociali e ambientali della propria catena di approvvigionamento, dai fornitori ai partner.

Il Consiglio di Amministrazione non può più limitarsi a delegare la materia a funzioni terze. Il Board deve definire la strategia di transizione climatica dell'intermediario, approvando piani di transizione allineati agli obiettivi dell'Accordo di Parigi e integrando i rischi climatici (sia fisici che di transizione) all'interno del Risk Appetite Framework (RAF). La vigilanza bancaria (BCE) e assicurativa (IVASS) sanziona attivamente le carenze di governance che espongono gli intermediari al rischio di contenzioso o di perdita reputazionale da ecologismo di facciata (**greenwashing**).

7.2 L'impatto dell'Intelligenza Artificiale e la governance dei dati finanziari

L'adozione pervasiva di modelli di **Intelligenza Artificiale (IA)** e di ***Machine Learning*** per il credit scoring, la profilazione della clientela, il monitoraggio delle frodi e la gestione algoritmica dei portafogli ha introdotto rischi tecnologici, etici e operativi di nuova generazione. La governance dei dati (***Data Governance***) è divenuta una prerogativa essenziale del Consiglio di Amministrazione.

Con l'entrata in vigore e il consolidamento dell'**AI Act** a livello europeo, gli organi di supervisione strategica degli intermediari finanziari devono implementare un quadro rigoroso di governance dell'IA, fondato sui seguenti principi:

- **trasparenza e spiegabilità (*Explainability*):** I modelli di IA utilizzati per assumere decisioni che impattano sulla clientela (es. concessione di un mutuo) non possono operare come scatole nere (*black boxes*). La governance deve assicurare che la logica algoritmica sia tracciabile, comprensibile e verificabile dalle funzioni di controllo interne e dalle Autorità di Vigilanza.

- **mitigazione dei bias e dei Rischi di Discriminazione:** Il Board deve approvare presidi organizzativi volti a monitorare la qualità dei dati storici utilizzati per l'addestramento degli algoritmi, evitando che l'IA perpetui o amplifichi discriminazioni sistemiche o pregiudizi statistici.

- **responsabilizzazione umana (*Human-in-the-Loop*):** Qualsiasi processo decisionale automatizzato ad alto rischio deve prevedere la supervisione e la possibilità di intervento o revoca da parte di operatori umani qualificati.

vedi l'articolo online

7.3 *La resilienza operativa digitale (DORA - Digital Operational Resilience Act) e la Cybersecurity Governance*

La dipendenza strutturale degli intermediari finanziari dalle tecnologie dell'informazione e della comunicazione (TIC) e la frequenza crescente degli attacchi informatici su scala globale hanno spinto il legislatore europeo a emanare il Regolamento **DORA (Digital Operational Resilience Act)**, pienamente applicabile dal **17 gennaio 2025** ed entrato stabilmente a regime.

Il DORA ridefinisce radicalmente la responsabilità del Consiglio di Amministrazione in materia di sicurezza informatica e resilienza operativa. Sotto il framework DORA, l'organo di gestione assume la **responsabilità ultima e personale** per la gestione dei rischi legati alle TIC (l'acronimo italiano di **Tecnologie dell'Informazione e della Comunicazione**, in inglese ICT - **Information and Communication Technology** . La governance cyber non può essere considerata una mera questione tecnica delegata al Chief Information Officer (CIO) o al Chief Information Security Officer (CISO). Il Board deve attivamente:

- approvare e verificare periodicamente la strategia di resilienza operativa digitale e le policy di gestione dei rischi TIC.
- determinare la tolleranza al rischio per le interruzioni delle funzioni aziendali critiche o importanti.
- supervisionare il monitoraggio e la classificazione dei gravi incidenti informatici e l'efficacia dei piani di continuità operativa (*Business Continuity*) e di ripristino (*Disaster Recovery*).
- monitorare e governare il rischio derivante da terze parti fornitrici di servizi TIC (es. fornitori di servizi cloud), definendo clausole contrattuali standardizzate e piani di uscita (*exit strategies*) per evitare blocchi sistemici.

Gli esponenti aziendali sono tenuti a seguire programmi di formazione continua e specialistica per mantenere un livello di conoscenze e competenze adeguato a comprendere e valutare i rischi legati alle TIC e il loro impatto sull'attività dell'intermediario.

8. Conclusioni

In conclusione, una **tabella comparativa** analitica (con riferimento ai capitoli e ai paragrafi ove vengono trattati) che sintetizza e mette a confronto diretto i requisiti e le specificità della corporate governance tra il settore bancario e quello assicurativo, evidenziando le asimmetrie regolamentari e operative trattate nel testo:

Tabella Comparativa: Governance Bancaria vs Governance Assicurativa

Dimensione di Governance	Settore Bancario	Settore Assicurativo
Framework Normativo Apicale	**CRD V / CRD VI** e Regolamento CRR II/III (recepimento in Italia tramite **Circolare 285 Banca d'Italia**) [2.2, 2.3].	**Solvency II** (recepimento in Italia tramite **Codice delle Assicurazioni Private** e **Regolamento IVASS 38/2018**) [3.1, 3.2].
Autorità di Vigilanza Apicale	**Banca Centrale Europea (BCE)** per le istituzioni significative (SSM) e **Banca d'Italia** (per LSI) [2.1, 2.3].	**EIOPA** a livello europeo e **IVASS** a livello nazionale [3.2].
Modello di Rischio Principale	**Attivo Opaco e Illiquido** (Rischio di credito, mercato, liquidità e trasformazione delle scadenze) [1.1, 6.1].	**Passivo Invertito e di Lungo Termine** (Rischi biometrici, di sottoscrizione, catastrofali e di mercato/ALM) [3.3].
Strumento di Autovalutazione Strategica	**SREP** (Supervisory Review and Evaluation Process) e processi interni di ICAAP/ILAAP [2.1].	**ORSA** (Own Risk and Solvency Assessment) sotto la diretta responsabilità del Board [3.1].
Funzioni di Controllo Fondamentali (Pilastri)	**Tre linee di difesa**: 1. Controlli di linea; 2. Risk Management & Compliance; 3. Internal Audit [6.1].	**Quattro funzioni chiave**: Risk Management, Compliance, Internal Audit e l'esclusiva **Funzione Attuariale** [3.2].
Principio Guida per gli Investimenti	Vincoli quantitativi prudenziali e limiti di concentrazione del portafoglio crediti/titoli [2.2, 6.3].	**Principio dell'Operatore Prudente** (*Prudent Person Principle*) basato su criteri qualitativi di ALM [3.3].
Focus della Tutela degli Stakeholder	Tutela dei **depositanti** e salvaguardia della stabilità macroeconomica sistemica (*Too Big to Fail*) [1.1, 1.2].	Tutela degli **assicurati/beneficiari** e della solvibilità di lungo periodo degli impegni futuri [1.2, 3.1].
Remunerazioni e Incentivi (Material Risk Takers)	Vincoli stringenti sul rapporto fisso/variabile (Bonus Cap) e quote differite in strumenti finanziari [2.1, 5.2].	Politiche tariffarie e provvisionali ancorate alla sostenibilità tecnica e a indicatori corretti per il rischio pluriennale [3.1, 5.2].
Impatto della Resilienza Digitale	Piena applicazione del **DORA** con focus sulla continuità dei sistemi di pagamento e transazionali [7.3].	Piena applicazione del **DORA** con focus sulla protezione dei dati sensibili e continuità della liquidazione dei sinistri [7.3].

Prospettive dell'Integrazione Metodologica

vedi l'articolo online

Dalla comparazione emerge chiaramente come, pur condividendo la medesima impostazione rigorosa sulle tre linee di difesa e sui presidi *Fit & Proper* [5.1, 6.1], la governance assicurativa sia storicamente e strutturalmente orientata al **governo del passivo e delle riserve tecniche** (tramite la funzione attuariale e l'ORSA) [3.1, 3.2], mentre la governance bancaria si concentri sulla **stabilità immediata dell'attivo e della liquidità** (tramite lo SREP e i limiti del RAF) [2.1, 6.3].

Entrambi i modelli convergono oggi in modo simmetrico sulle sfide tecnologiche e di sostenibilità imposte dai framework ESG e dal Regolamento DORA [7.1, 7.3].

Il tutto in attesa della **Direttiva** e dei **Regolamenti** legati alla ***Retail Investment Strategy (RIS)*** che impatterà su **MiFID II, IDD, Solvency II, UCITS, AIFMD** e Regolamento **PRIIPs. (i sette cardini normativi in via di armonizzazione).**

9. Bibliografia essenziale e riferimenti normativi

- **Regolamento (UE) 2022/2554** del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario (**DORA**).
- **Direttiva (UE) 2019/878** del Parlamento europeo e del Consiglio, del 20 maggio 2019, che modifica la direttiva 2013/36/UE per quanto riguarda gli esponenti esenti, i requisiti di fondi propri e di passività ammissibili, la vigilanza macroprudenziale, la governance aziendale e la remunerazione (**CRD V**).
- **Direttiva 2009/138/CE** del Parlamento europeo e del Consiglio, del 25 novembre 2009, in materia di accesso ed esercizio delle attività di assicurazione e di riassicurazione (**Solvency II**).
- **Decreto del Ministero dell'Economia e delle Finanze 23 novembre 2020, n. 169**, Regolamento concernente i requisiti e i criteri di idoneità allo svolgimento dell'incarico degli esponenti aziendali delle banche e degli intermediari finanziari.
- **Banca d'Italia**, Circolare 17 dicembre 2013, n. 285, "Disposizioni di vigilanza per le banche" (e successivi aggiornamenti, con focus sulla Parte Prima, Titolo IV, Capitolo 1 "Il sistema di governo societario").
- **IVASS**, Regolamento 3 luglio 2018, n. 38, recante disposizioni in materia di sistema di governo societario delle imprese di assicurazione e riassicurazione.

Bibliografia Scientifica ed Economica

- **Bebchuk, L. A., & Spamann, H. (2010).** *Regulating bankers' pay.* Georgetown Law Journal, 98(2), 247-287.
- **EBA-ESMA (2021).** *Joint Guidelines on the assessment of the suitability of members of the management body and key function holders.* European Banking Authority & European Securities and Markets Authority.
- **ECB (Banca Centrale Europea) (2024).** *Guide on governance and risk culture.* Single Supervisory Mechanism.
- **Jensen, M. C., & Meckling, W. H. (1976).** *Theory of the firm: Managerial behavior, agency costs and ownership structure.* Journal of Financial Economics, 3(4), 305-360.
- **Laeven, L., & Levine, R. (2009).** *Bank governance, regulation and risk taking.* Journal of Financial Economics, 93(2), 259-275.
- **Mülbert, P. O. (2009).** *Corporate governance of banks after the financial crisis - A theory-of-the-firm approach.* European Company and Financial Law Review, 6(4), 440-475.
- **Sironi, A. (2020).** *Evoluzione del sistema dei controlli interni e della cultura del rischio nel settore finanziario.* Rivista Bancaria - Minerva Bancaria, 4, 12-35.

vedi l'articolo online



DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it