LUISS

Dipartimento
di Impresa e Management

Cattedra di Corporate Governance and Internal Auditing

Il Sistema dei Controlli Interni e la funzione di Internal Audit nell'ambito dello SREP

Prof. Simone Scettri
RELATORE

Prof. Giovanni Fiori
CORRELATORE

Margherita Giffi (Matr. 714511)
CANDIDATO

Anno Accademico 2019/2020

INDICE

Introduzione

Il presente lavoro ha inteso esaminare i risvolti che l'affermazione del *Supervisory Review and Evaluation Process* (SREP) ha avuto sulle attività delle banche e, conseguentemente, sul sistema dei controlli interni, sulla funzione di *Internal Audit* e sulla loro evoluzione.

La prospettiva dello studio è stata quella di indagare in concreto le rilevanze più significative che il sistema ha prodotto sugli enti e, nello specifico, si è guardato, comparativamente, ai risultati relativi a quattro istituti di credito.

L'elaborato si articola in tre capitoli, i cui contenuti si richiamano, sia pur brevemente, di seguito.

Nel primo capitolo si introduce il sistema dei controlli interni e la funzione di *Internal Audit*, passando in rassegna la disciplina e gli elementi essenziali sia del sistema dei controlli che dell'*Internal Audit* considerato che rappresentano le premesse essenziali nello sviluppo del tema trattato.

Il secondo capitolo sul *Supervisory Review Process* analizza, in primo luogo, l'evoluzione dell'impianto regolamentare relativo al processo di controllo prudenziale, facendo riferimento alla regolamentazione prevista in Basilea III e recepita in ambito comunitario dalla Direttiva 2013/36/UE e dal Regolamento UE/575/2013, nonché alla normativa nazionale e alle disposizioni emanate da Banca d'Italia. In secondo luogo, si sofferma sul *Supervisory Review Process* e sulle due fasi di tale processo. Si illustra, più in particolare, la prima fase che fa capo alle banche, consistente nei processi interni di valutazione dell'adeguatezza del capitale (*Internal Capital Adequacy Assessment Process*-ICAAP) e della liquidità (*Internal Liquidity Adequacy Assessment Process*-ILAAP).Viene esaminata, inoltre, la seconda fase che è quella del *Supervisory Review and Evaluation Process* in senso stretto, cioè del processo di revisione e valutazione prudenziale di competenza delle Autorità di vigilanza (la Banca Centrale Europea per le banche "significant" e le Autorità di vigilanza nazionale per le banche "less significant").

Il terzo capitolo affronta il sistema dei controlli e la funzione di *Internal Audit* nell'ambito del *Supervisory Review and Evaluation Process* attraverso l'esame degli organi aziendali coinvolti nel processo di controllo prudenziale e la rilevanza dei rispettivi ruoli.
In questa sede vengono riportate le esperienze concrete di talune banche annoverate tra le "significant" e quotate quali Intesa Sanpaolo, Mediobanca, Ubi Banca e Unicredit; la valutazione è stata in relazione al loro sistema di *governance* interna con particolare riferimento alla composizione del Consiglio di Amministrazione, alle caratteristiche di indipendenza, professionalità e competenze richieste ai loro componenti, alla diversificazione in ragione di età e di genere, alle politiche di nomina e di remunerazione, alla presenza di comitati endoconsiliari, al funzionamento dei sistemi di

controllo interno e dei sistemi informativi per addivenire ad una valutazione nell'ottica SREP dell'adeguatezza della loro struttura di *governance* e di controllo interno.

La valutazione di questi ultimi profili, alla luce delle questioni poste e degli elementi trattati nel corso del lavoro, ha condotto ad evidenze riportate nelle considerazioni conclusive unitamente a brevi cenni sulle possibili prospettive future dei meccanismi dei controlli prudenziali.

CAPITOLO 1

Il Sistema dei Controlli Interni e l'Internal Auditing

1. Origine ed evoluzione del Sistema dei Controlli Interni e dell'Internal Auditing

Il concetto di "controlli interni" subisce una significativa evoluzione storica nel corso del tempo. In Italia, prima degli anni novanta, si parla di attività di controllo unicamente con riferimento all'attività di sorveglianza sulla regolarità della gestione aziendale affidata al collegio sindacale e prevista dal diritto commerciale. In quegli anni l'attività di controllo interno non è oggetto di un quadro normativo chiaro ed esaustivo.

Fino agli anni quaranta, infatti, il tema dei controlli interni rappresenta un aspetto marginale, seppure non del tutto irrilevante, della revisione contabile. Un adeguato funzionamento dei controlli interni fornisce ai revisori lo strumento per garantire la veridicità e la completezza dei documenti contabili sottoposti a revisione.

Alla fine degli anni cinquanta viene superata l'accezione meramente contabile di controllo interno per giungere ad una nozione più ampia: per la prima volta si affiancano ai controlli contabili quelli amministrativi, cioè quelli relativi all'efficienza operativa, all'aderenza alle politiche gestionali e alle procedure decisionali.

Intorno alla metà degli anni ottanta il tema dei controlli interni assume progressivamente un ruolo di crescente rilievo, in particolare, nell'ambito di decisioni associate ai processi di *risk assessment* e di *risk management*. Si afferma, dunque, una chiave di lettura del fenomeno più moderna ed incentrata sull'introduzione di protocolli comportamentali finalizzati alla mappatura dei rischi rilevanti e al rafforzamento delle aree più "critiche"[1].

Negli anni novanta il lavoro di ricerca del *Committee of Sponsoring Organizations of the Treadway Commission* (*CoSO*) porta alla nascita dell'"*Internal Control - Integrated Framework*", più noto come *CoSO Report*. Il *CoSO Report* viene pubblicato nel 1992 negli Stati Uniti con l'obiettivo di delineare e promuovere un concetto univoco di controllo interno e un modello di riferimento per società e management nella creazione di un sistema di controllo. In pochi anni, tale report viene adottato in numerosi paesi, tra cui l'Italia, e utilizzato come schema per la predisposizione di codici di autodisciplina, norme e altri documenti sui controlli interni.

Nel 2002 il contesto normativo internazionale si amplia a seguito dell'approvazione negli Stati Uniti del "*Sarbanes Oxley Act*". Questa normativa, risultato degli scandali finanziari che in quegli anni coinvolgono la Enron, la WorldCom e altre grandi società statunitensi e che fanno emergere chiaramente i limiti della *corporate governance*, diventa poi fonte di ispirazione per il legislatore

[1] Cfr. P. TETTAMANZI, *Internal Auditing. Evoluzione storica, stato dell'arte e tendenze di sviluppo,* p. 33.

della Legge 262/2005 sulla tutela del risparmio, avente l'obiettivo di assicurare un'amministrazione aziendale più affidabile e recuperare così la fiducia degli investitori. Per questi motivi, tra gli aspetti principali di tale legge vi sono una maggiore attendibilità delle informazioni finanziarie e dei processi di controllo interno contabile, gli accresciuti poteri di regolamentazione e vigilanza in capo alla *Security and Exchange Commission* e l'indipendenza delle società di revisione contabile.

Data la sempre maggiore importanza assunta dal tema della gestione dei rischi, il *Committee of Sponsoring Organizations of the Treadway Commission* giunge nel 2004 alla pubblicazione di un nuovo report, l'"*Enterprise Risk Management - Integrated Framework*" o *CoSO II*, che amplia la visione del concetto di controllo interno in termini di *risk management*. L'obiettivo è quello di fornire uno schema per l'analisi dei fattori di rischio e la valutazione del loro impatto sulla performance aziendale, consentendo al management di raggiungere il giusto equilibrio tra crescita e redditività da un lato e rischi conseguenti dall'altro.

Il *Coso Report* è stato oggetto di aggiornamenti nel 2013 (aggiornamento dell'*Internal Control - Integrated Framework* del 1992) e nel 2017 (aggiornamento dell'*Enterprise Risk Management - Integrated Framework* del 2004). Le nuove versioni mantengono l'idea di base e gli aspetti principali dei precedenti report apportando le modifiche necessarie dato il nuovo contesto sociale e di *business*. Infatti, il Report del 2013 prima e quello del 2017 poi prevedono, tra l'altro, la necessità di implementare l'efficacia e la trasparenza del Sistema di Controllo Interno così da tener conto di aspetti ulteriori derivanti, per esempio, dalla profonda crisi finanziaria del 2007, dalla globalizzazione e dall'avanzare della tecnologia[2].

Per quanto riguarda l'Internal Auditing (IA), l'evoluzione del suo significato e dell'attività di auditing prende le mosse dall'esperienza degli Stati Uniti e dell'Inghilterra dove tale tematica si è diffusa ed affermata tempo prima rispetto all'Italia. Sebbene le prime testimonianze di funzioni comparabili all'audit in ambito contabile si facciano risalire alla civiltà Sumera, le attività di audit vere e proprie compaiono nella prima metà del '900. Risale, infatti, al 1933 l'emanazione negli Stati Uniti del "*Security Act*" che prevede in capo alle società quotate l'obbligo dell'attività di revisione, anche se già negli anni venti parte del personale di tali società si dedicava esclusivamente all'attività di auditing.

La nascita dell'Internal Audit si fa risalire ufficialmente al 1941, anno in cui viene fondato in Florida l'Institute of Internal Auditors (IIA) con lo scopo di favorire la conoscenza e lo sviluppo della professione dell'internal auditor. Qualche anno dopo nel 1948 viene fondata a Londra l'associazione

[2] Con l'aggiornamento di giugno 2017, il *Committee of Sponsoring Organizations of the Treadway Commission* ha pubblicato un documento denominato "*Enterprise Risk Management – Integrating with strategy and performance"* che evidenzia l'importanza della individuazione e della gestione dei rischi nelle fasi di definizione delle strategie e valutazione delle performance. Il nuovo documento prevede cinque componenti: Governance and Culture, Strategy and Objective – Setting, Performance, Review and Revision, Information, Communication and Reporting.

IIA-UK quale sede distaccata di quella statunitense; successivamente, altri organismi professionali esistenti nel Regno Unito si sono occupati della definizione degli standard di revisione interna[3], mentre in Italia si dovrà attendere la seconda metà del '900.

Nel 1972, infatti, a Milano nasce l'Associazione Italiana Internal Auditors (AIIA) dietro la spinta dell'esperienza inglese e statunitense, ma anche di alcuni interventi normativi. In particolare, di alcuni progetti di legge che hanno condotto all'emanazione della legge 216/1974, cui è stata data attuazione dal D.P.R. 136/1975, concernente il controllo contabile e la certificazione obbligatoria dei bilanci delle società per azioni quotate in Borsa, decreto ormai in parte superato dalla cosiddetta "legge Draghi"[4]. Così anche in Italia l'Internal Auditing intraprende un ampio processo di diffusione assumendo una rilevanza sempre maggiore, come testimonia anche il grande interesse mostrato dal legislatore verso tali tematiche. Nel corso degli anni, infatti, questa funzione subisce una significativa evoluzione: da attività di raccolta di dati e verifica dei controlli avvertita dalla compagine societaria come attività "estranea" e "nemica", ad attività, anche preventiva, di analisi trasversale dei processi di business e di valutazione dei rischi svolta dagli auditors considerati membri del team.

A conclusione di questo breve *excursus* sull'evoluzione storica, risulta evidente come tale argomento abbia assunto nel corso del tempo un ruolo sempre più centrale nelle decisioni di *business*, perdendo quella accezione di mero adempimento che lo caratterizzava all'origine. Riguardo al tema che più direttamente ci interessa ai fini del presente lavoro, sembra utile sottolineare, inoltre, la rilevanza che la questione dei controlli interni ha assunto anche nella comunità finanziaria, divenendo elemento essenziale della gestione bancaria e uno dei principali criteri di valutazione a disposizione della Vigilanza. Tanto è vero che è ormai consolidato l'insegnamento per cui il Sistema dei Controlli Interni è indispensabile per gli obiettivi strategici, per l'attendibilità delle informazioni, per la conformità alle norme e per la gestione dei rischi di perdite e reputazionali, come vedremo più nello specifico nel prosieguo del lavoro.

2. Il contesto normativo

Il tema del controllo interno è oggetto di numerosi interventi normativi e iniziative di autoregolamentazione, quali codici etici e di autodisciplina, nonché di molteplici report prodotti da

[3] Si tratta in particolare dell'*Auditng practices Board* (APB) che nello *Statement of Auditing Standards* (SAS) 500 ha stabilito i compiti dell'IA e le relazioni di questa funzione con la revisione esterna, nonché dell'*Institute of Chartered Accountants in England and Wales* (ICAEW) che utilizza un framework simile a quello dell'Associazione Internal Auditors.

[4] Cfr. G. GASPARRI, *Gli assetti della disciplina italiana e i problemi aperti*.

associazioni di categoria e da società di gestione dei mercati regolamentati[5]. Sebbene ognuno di tali atti meriti una trattazione approfondita, ai fini di questo studio verranno richiamati nel prosieguo del paragrafo gli aspetti e le disposizioni che hanno un considerevole impatto sul Sistema dei Controlli Interni (SCI) e sulla funzione di Internal Auditing (IA).

In Italia bisogna attendere sino al 1997/1998 perché il tema venga affrontato in modo rilevante dal "*Progetto Corporate Governance per l'Italia (PCGI)*" e dalla "*legge Draghi*". Come accennato in precedenza, infatti, sino a quel momento l'unica attività di controllo prevista dalla legge è quella del collegio sindacale, organo societario con fondamentali poteri di supervisione e verifica, ma che rappresenta solo una parte del complesso meccanismo del Sistema di Controllo Interno aziendale.

Prima del 1998, il collegio sindacale ha, ai sensi dell'art. 2403 del Codice Civile, il dovere di "*controllare l'amministrazione della società, vigilare sull'osservanza della legge e dell'atto costitutivo e accertare la regolare tenuta della contabilità sociale, la corrispondenza del bilancio alle risultanze dei libri e delle scritture contabili e l'osservanza delle norme stabilite dall'art. 2426 c.c. per la valutazione del patrimonio sociale. Il collegio sindacale deve altresì accertare almeno ogni trimestre la consistenza di cassa e l'esistenza dei valori e dei titoli di proprietà sociale o ricevuti dalla società in pegno, cauzione o custodia*"[6]. Tali poteri del collegio sindacale, ben presto, vengono considerati inadeguati e, pertanto, divengono oggetto di critica per due ragioni principali: innanzitutto, le lacune normative relative alle indicazioni e ai criteri rigorosi per lo svolgimento dei ruoli del collegio sindacale comportano la necessità di servirsi del Sistema dei Controlli Interni; in secondo luogo, la genericità con cui il legislatore stabilisce i doveri del collegio sindacale rende particolarmente complesso riuscire a delineare una linea di confine tra i poteri di tale organo e quelli affidati a società di certificazione o revisione esterna[7].

Nell'intento di superare questi aspetti critici relativi al funzionamento delle attività di controllo, gli organismi professionali elaborano una serie di documenti riguardanti il Sistema di Controllo Interno e le modalità della sua implementazione. In particolare, nel 1996 il Consiglio Nazionale dei Dottori Commercialisti e dei Ragionieri (attuale Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili – CNDCEC) emana i "*Principi di comportamento del Collegio Sindacale*" contenenti una norma specifica sulla valutazione del sistema di controllo interno e dell'organizzazione contabile della società[8].

---

[5]La trattazione della regolamentazione del settore finanziario verrà approfondita nel secondo capitolo nell'ambito dello studio del contesto normativo che circonda il Supervisory Review Process.

[6] Testo dell'art. 2403 c.c., primo e secondo comma, prima delle modifiche apportate prima dal D.lgs 58/1998 e successivamente dalla c.d. Riforma del diritto societario.

[7] cfr. P.JAEGER, F. DENOZZA, *Appunti di diritto commerciale. Impresa e società*, Milano, Giuffrè, 1997, pp. 429 e ss.

[8] La norma citata è la n. 2.5 che prevede una definizione di SCI e i passaggi e i documenti necessari ai fini della valutazione del grado di affidabilità dello stesso da parte dei sindaci. Per un esame più approfondito, cfr. CNDCR, *Principi di comportamento del collegio sindacale*, Milano; Giuffrè, 1996.

Sul finire dello stesso anno i temi del controllo interno e della *corporate governance* sono discussi nel "*Libro Verde*" della Commissione europea[9]. Sulla stessa scia il "*Progetto Corporate Governance per l'Italia*" che porta, nel 1997, alla pubblicazione del risultato delle ricerche su come ridefinire e rendere applicabili in Italia i principi per un buon SCI e un buon governo dell'impresa previsti nel già citato *CoSO Report*.

Gli interventi e i provvedimenti sino ad ora citati non hanno però natura né validità legale bensì solo di raccomandazioni per le imprese.

Sotto tale aspetto, la prima svolta si ha nel 1998 con l'entrata in vigore del "*Testo Unico della Finanza - TUF*" (D.lgs. n. 58 del 24 febbraio 1998, noto anche come "legge Draghi") che formalizza l'importanza del Sistema di Controllo Interno, introducendo per la prima volta nella legislazione italiana tale espressione e, seppure implicitamente, anche quella dell'Internal Auditing[10]. Si tratta del primo intervento legislativo che pone l'accento sugli aspetti di controllo aziendale, prevedendo innanzitutto che controllo contabile e controllo sull'amministrazione debbano essere separati: il primo affidato ad una società di revisione o ad un revisore esterno e il secondo ai sindaci. Inoltre, riqualifica e ridefinisce il ruolo, il funzionamento e le responsabilità del collegio sindacale delle società con azioni quotate attribuendo allo stesso nuovi poteri di vigilanza sull'operato degli amministratori e di supervisione dell'adeguatezza del Sistema di Controllo Interno. L'articolo 149, primo comma, lettera *c* della "*legge Draghi*" dispone infatti: "*il collegio sindacale vigila sull'adeguatezza della struttura organizzativa della società per gli aspetti di competenza, del sistema di controllo interno e del sistema amministrativo-contabile nonché sull'affidabilità di quest'ultimo nel rappresentare correttamente i fatti di gestione*". L'articolo 150, quarto comma, stabilisce inoltre che "*coloro che sono preposti al controllo interno riferiscono anche al collegio sindacale di propria iniziativa o su richiesta anche di uno solo dei sindaci*". La norma delinea un sistema incentrato sullo scambio costante di informazioni tra tutti gli organi preposti al controllo per l'espletamento delle relative funzioni.

Il TUF rappresenta il punto di partenza da cui la regolamentazione di settore e l'autoregolamentazione dei singoli emittenti quotati prendono le mosse per l'individuazione di un quadro d'insieme delle regole concernenti il buon governo d'impresa.

---

[9] Il documento originale "*Libro verde. Il ruolo, la posizione e la responsabilità del revisore legale dei conti nell'Unione europea*" è stato pubblicato sulla Gazzetta ufficiale delle Comunità europea n.c. 321/1 del 28.10.96 ed è contenuto nella rivista Auditing n. 28, gennaio-aprile 1997.

[10] Il D.lgs 58 del 1998 è stato aggiornato aggiornato, da ultimo, con le modifiche introdotte dal D.lgs. 21 maggio 2018, n. 68.

Il primo intervento in tal senso è la nota di indirizzo emanata nel febbraio 1999 dall'Associazione Italiana Internal Auditors (AIIA) per assistere le imprese nella gestione dei cambiamenti in atto[11].

Nel corso del 1998 e 1999 al fine di disciplinare i punti cruciali della governance degli emittenti quotati e del loro Sistema di Controllo Interno, contribuiscono, tra gli altri, anche Banca d'Italia, ISVAP e CONSOB attraverso la pubblicazione di documenti e circolari aventi ad oggetto, in particolare, gli aspetti di natura organizzativa e procedurale[12].

Un commento e una guida al D.lgs. 58/1998 giungono anche dal Consiglio Nazionale dei Dottori Commercialisti che, nel mese di maggio 1999, pubblica un documento dal nome "Principi di comportamento del Collegio sindacale nelle società di capitali con azioni quotate nei mercati regolamentati"[13].

Proseguendo in ordine cronologico, nel 1999 Borsa Italiana costituisce un comitato (Comitato per la corporate governance) con il compito di raccogliere in un documento le linee guida per l'applicazione dei principi di *corporate governance*. Così nasce, nell'ottobre 1999, il Codice di Autodisciplina, conosciuto anche come "*codice Preda*", dal nome dell'allora presidente di Borsa Italiana SpA e coordinatore del Comitato per la *corporate governance*[14]. Gli obiettivi del codice sono implementare il controllo dei rischi d'impresa, creare un adeguato sistema di deleghe, garantire la trasparenza nei flussi informativi e massimizzare la creazione di valore per gli azionisti. Il codice Preda accoglie un'idea ampia di SCI, ricomprendendo tra i suoi compiti quello di verificare che vengano effettivamente rispettate le procedure interne - sia operative sia amministrative - al fine di garantire una corretta ed efficiente gestione, e di identificare, prevenire e gestire rischi di natura finanziaria e operativa e frodi a danno della società. Si tratta dell'intervento più significativo in relazione all'Internal Auditing, la cui rilevanza viene evidenziata prevedendo, tra l'altro, che la figura del soggetto incaricato di verificare l'adeguatezza del controllo interno venga individuata nel responsabile della funzione di Internal Auditing[15].

In risposta a questo intervento, tra il 2000 e il 2001 vengono pubblicati il primo *position paper* predisposto dall'AIIA, "*Il Reporting sul sistema di controllo interno. Un aspetto qualificante dei più avanzati codici di autodisciplina espressi dal movimento internazionale di riforma della corporate*

---

[11] cfr. AIIA, *Iniziativa di comunicazione da parte dell'internal auditing verso il collegio sindacale e il vertice esecutivo*, Nota di indirizzo professionale n. 1/99, Milano, AIIA, febbraio 1999.

[12] V. Banca d'Italia, *Istruzioni di vigilanza per le banche, Sistemi dei controlli interni, compiti del collegio sindacale*, 1998; cfr. tra le altre Delibera CONSOB n. 11522, Regolamento di attuazione del d.lgs 58/1998 – disciplina degli intermediari – del luglio 1998 e Circolare n. 366D ISVAP del 3 marzo 1999.

[13] CNDCR, *Principi di comportamento del collegio sindacale nelle società di capitali con azioni quotate nei mercati regolamentati (osservanza del D.lgs. 24 febbraio 1998, n. 58)*, Milano, Giuffrè, 1999, supplemento al fascicolo II/99 della rivista Il controllo legale dei conti.

[14] Il Codice di Autodisciplina è stato emanato nel 1999 e rivisitato nel 2002, 2006, 2010, 2011, 2014, 2015 e 2018; l'ultima versione, sotto il nome di Codice di Corporate Governance, è stata approvata nel gennaio 2020 e sarà applicata dalle società a partire dal 31 dicembre 2020.

[15] V. Codice di Autodisciplina, art. 7. P. 3 – lett. b

governance" e la "*Guida operativa sulla vigilanza del sistema di controllo interno*" come aggiornamento dei "*Principi di comportamento del Collegio sindacale nelle società di capitali con azioni quotate nei mercati regolamentati*" a cura del Consiglio Nazionale dei Dottori Commercialisti e dei Ragionieri[16].

Le tematiche del controllo interno hanno un ruolo centrale anche nel D.lgs n. 231 del 19 giugno 2001 in materia di responsabilità amministrativa degli Enti, con o senza personalità giuridica, per i reati commessi nel loro interesse dai soggetti impiegati nell'ente[17]. La norma attribuisce importanza fondamentale al Sistema di Controllo Interno e all'Internal Auditing in quanto lo svolgimento di tali attività diviene strumento di valutazione della responsabilità degli amministratori. Infatti, per tutelare l'ente da tale responsabilità, la normativa esclude l'applicazione delle sanzioni a quelle società che dimostrano di aver attuato ed implementato un modello di gestione e controllo e un organo di controllo (Organismo di Vigilanza) in grado di individuare e prevenire ipotesi di reato e, ancora, provano che gli autori del reato hanno fraudolentemente violato tale modello nonostante la diligenza dell'Organismo di Vigilanza e degli auditors. La predisposizione di modelli di organizzazione, gestione e controllo viene facilitata dal cospicuo numero di linee guida emanate immediatamente dopo la pubblicazione del D.lgs 231/2001 e negli anni successivi. Tra i lavori più noti si ricordano il *position paper* dell'Associazione Italiana Internal Auditors e le Linee Guida elaborate da Confindustria. Nell'ambito di tale normativa è opportuno richiamare anche il D.lgs n. 61 dell'11 aprile 2002 che estende la disciplina del D.lgs 231/2001 ai reati societari.

Un ulteriore intervento normativo di fondamentale importanza per la delineazione dell'attuale Sistema di Controllo Interno è rappresentato dal D.lgs n. 6 del 17 gennaio 2003 contenente la riforma organica della disciplina delle società di capitali. Tale riforma introduce importanti novità per le società per azioni e per le società a responsabilità limitata, quotate e non, con l'obiettivo di lasciare ampio margine all'autonomia statutaria, di semplificare la disciplina delle società e di agevolare l'accesso ai mercati finanziari.

Il cambiamento più significativo può individuarsi nella previsione, accanto al modello tradizionale, di due nuovi modelli di amministrazione e controllo: il sistema dualistico e il sistema monistico.

Per quanto riguarda il modello tradizionale, in cui l'assemblea nomina l'organo amministrativo e il collegio sindacale, la principale novità introdotta dalla riforma verte sul tema del controllo contabile,

---

[16] Cfr. CNDCR, *Guida operativa sulla vigilanza del sistema di controllo interno*, Milano, Giuffrè., supplemento al fascicolo 1/2001 della rivista Il controllo legale dei conti.

[17] Senza prolungarsi sulla natura della responsabilità dell'Ente, in questa sede si ritiene necessario specificare che in caso di commissione dei reati previsti dal D.lgs 231/2001 si configura una vera e propria responsabilità penale esclusivamente in capo al soggetto (persona fisica) che ha commesso il reato nell'esercizio delle funzioni e dei poteri all'interno dell'impresa, mentre per le persone giuridiche si parlerà di responsabilità "amministrativa" dipendente da reato.

che deve essere affidato, anche nelle società non quotate, ad un revisore esterno o ad una società di revisione; solo le società che non fanno ricorso al capitale di rischio e che non sono tenute a redigere il bilancio consolidato, possono affidare il controllo contabile al collegio sindacale, composto da revisori contabili.

Il modello dualistico prevede la presenza di un consiglio di sorveglianza, nominato dall'assemblea, e di un consiglio di gestione, nominato dal consiglio di sorveglianza. In tale sistema, rispetto al modello tradizionale, i poteri dell'assemblea sono diminuiti e quelli del consiglio di sorveglianza sono maggiori rispetto a quelli riconosciuti ai sindaci. Il controllo contabile deve essere gestito da un revisore esterno o da una società di revisione.

L'ultimo sistema previsto dalla riforma è quello monistico in cui l'amministrazione e il controllo sono affidati, rispettivamente, al consiglio di amministrazione e al comitato per il controllo sulla gestione costituito al suo interno. Per le società che aderiscono a tale modello, l'obbligo di affidare il controllo contabile ad un organo esterno è previsto solo se fanno ricorso al mercato di capitali di rischio e redigono il bilancio consolidato.

Il legislatore della riforma sottolinea l'importanza dei controlli sia interni che esterni e la necessità di una efficace struttura di tali controlli e di una adeguata distribuzione dei poteri tra i diversi organi societari[18].

Nel 2005 il panorama legislativo vede l'entrata in vigore della Legge sulla tutela del risparmio (Legge 28 dicembre 2005, n. 262) che introduce importanti novità su diversi temi nonché alcune modifiche al Testo Unico della Finanza, al Testo Unico Bancario e al Codice civile. Tra i vari elementi innovativi, questa legge prevede nuove responsabilità, in particolare la figura del "dirigente preposto alla redazione dei documenti contabili societari" con il compito di predisporre adeguate procedure amministrative e contabili per la redazione del bilancio e di ogni altra comunicazione di carattere finanziario, e il riordino delle autorità di controllo e di vigilanza. Riguardo a questo ultimo aspetto, i nuovi obblighi in capo agli organi di controllo sono quello di vigilare sulle modalità di attuazione delle regole di governo societario previste dai codici di comportamento, la cui osservanza diviene, dunque, oggetto di specifico controllo, e quello di collaborare con gli altri organi della stessa società e di società controllate. Tali disposizioni hanno il fine di garantire una migliore qualità dell'informazione, una maggiore efficacia della *governance* e più spazio al ruolo delle minoranze.

Di primaria importanza è anche il D.lgs 39 del 22 gennaio 2010 che attua parzialmente la direttiva 2006/43/CE sulla revisione legale dei conti e riordina e armonizza le norme del nostro ordinamento

[18]Cfr. P. BALZARINI, *La riforma del diritto societario*, Strumenti 30 del settembre/ottobre 2003 in mondadorieducation.it.

con la normativa europea[19]. In relazione al tema del controllo, si ritiene rilevante l'articolo 19 che, per gli enti di interesse pubblico, definisce i compiti assegnati al Comitato per il controllo interno e la revisione contabile. La norma attribuisce al Comitato, tra gli altri, il compito di vigilare sul processo di informativa finanziaria, sull'efficacia dei Sistemi di Controllo Interno, di revisione interna e di gestione del rischio, sulla revisione legale del bilancio d'esercizio e di quello consolidato e sull'indipendenza dei revisori legali o della società di revisione legale, in particolare per quanto concerne la prestazione di servizi non di revisione all'ente sottoposto alla revisione legale dei conti. Il decreto prevede anche che tale organo coincida con il collegio sindacale nel sistema tradizionale, con il consiglio di sorveglianza nel sistema dualistico e con il Comitato per il controllo sulla gestione nel sistema monistico. Tali organi, dunque, dovranno valutare in maniera indipendente il sistema dei controlli e, in particolare, l'attendibilità delle informazioni finanziarie.

3. Il Sistema di Controllo Interno

Nell'affrontare il tema relativo alla definizione di sistema di controllo interno, si deve fare i conti con l'inesistenza di una definizione univoca, soprattutto a livello normativo. Questo lavoro si propone di richiamare le due definizioni di controllo interno più diffuse e più rilevanti ai fini della delineazione della natura, delle componenti e del funzionamento del Sistema di Controllo Interno: si tratta delle definizioni fornite dal Codice di Autodisciplina e dal *CoSO Report I*.

Secondo il Codice di Autodisciplina, il Sistema di Controllo Interno e di Gestione dei Rischi è l'insieme delle regole, delle procedure e delle strutture organizzative volte a consentire l'identificazione, la misurazione, la gestione e il monitoraggio dei principali rischi, così da contribuire a una conduzione dell'impresa coerente con gli obiettivi aziendali e che favorisca l'assunzione di decisioni consapevoli[20]. Un efficace Sistema di Controllo Interno (SCI) deve perseguire e garantire la salvaguardia del patrimonio sociale, l'efficienza e l'efficacia dei processi aziendali, l'affidabilità delle informazioni tra organi sociali e verso il mercato e il rispetto di leggi, regolamenti, statuto sociale e procedure interne[21].

La concezione di controllo interno che emerge dal Codice di Autodisciplina ruota attorno alla nozione di rischi aziendali: l'individuazione e il monitoraggio dei rischi rappresentano il filo conduttore del Sistema di Controllo Interno e Gestione dei Rischi.

Il Sistema di Controllo Interno deve essere integrato nel più ampio assetto della *governance* della società e coinvolge tutti gli organi sociali che devono operare, ognuno in relazione alle proprie

[19] Il testo del decreto è stato oggetto di diversi interventi successivi, l'ultimo dei quali con il D. lgs del 17 luglio 2016, n. 135.
[20] Codice di Autodisciplina, art. 7.P.1
[21] Codice di Autodisciplina, art. 7.P 2

competenze, coordinandosi al fine di massimizzare l'efficienza del sistema stesso e ridurre le duplicazioni di attività[22].

Il consiglio di amministrazione, che in quanto organo di supervisione strategica rappresenta la figura apicale nel SCI, deve indirizzare e valutare l'adeguatezza del sistema. Attraverso le linee di indirizzo definite, il consiglio deve far in modo che i rischi, correttamente individuati e gestiti, convivano con gli obiettivi strategici dell'impresa. Con cadenza almeno annuale, deve approvare il piano di lavoro disposto dal responsabile della funzione di Internal Audit e valutare l'adeguatezza del sistema di controllo. Quest'ultima valutazione deve essere espressa nella relazione sul governo societario insieme alla descrizione delle principali caratteristiche del SCI e alle modalità di coordinamento tra gli organi sociali coinvolti. Inoltre, se in sede di revisione legale emergono questioni di particolare rilevanza, il revisore deve esporle nella lettera di suggerimenti o nella relazione e il consiglio deve dare una propria valutazione.

Nello svolgimento di questi compiti, l'organo di gestione è coadiuvato da uno o più amministratori incaricati dell'istituzione e del mantenimento del sistema di controllo e gestione dei rischi e da un comitato controllo e rischi.

L'amministratore (o gli amministratori) incaricato del Sistema di Controllo Interno e di Gestione dei Rischi si occupa dell'identificazione dei rischi aziendali e dell'esecuzione delle linee di indirizzo definite dal consiglio di amministrazione, progettando e realizzando il sistema di controllo; deve garantire che il sistema si adatti alle caratteristiche delle attività svolte dall'impresa, alle condizioni operative e al contesto normativo e regolamentare; in caso di problematiche e criticità, riferisce tempestivamente al comitato controllo e rischi o al consiglio di amministrazione.

Il comitato controllo e rischi deve supportare decisioni e valutazioni del consiglio, svolgendo un'adeguata attività istruttoria e, almeno semestralmente, riferendo allo stesso sull'attività svolta e sull'adeguatezza del sistema di controllo; deve anche valutare il corretto utilizzo dei principi contabili ed esprimere pareri riguardo l'identificazione dei principali rischi aziendali. Inoltre, monitora l'efficacia della funzione di Internal Auditing a cui può chiedere di effettuare verifiche su specifiche aree operative.

Ruolo fondamentale è svolto dal responsabile della funzione Internal Audit (RIA) che dipende gerarchicamente dal consiglio di amministrazione e non è responsabile di aree operative. Il RIA, sulla base di un processo strutturato di analisi e identificazione dei principali rischi, prepara un piano di audit volto a valutare l'operatività e l'idoneità del sistema di controllo. Ha accesso a tutte le informazioni necessarie per l'incarico e, sempre nell'ambito del piano di audit, verifica l'affidabilità dei sistemi informativi. Inoltre, predispone delle relazioni periodiche contenenti, oltre alla valutazione

[22] Cfr. C.A. DITTMEIER, *Internal Auditing. Chiave per la corporate governance,* p. 101.

sull'idoneità del sistema di controllo, informazioni relative alle attività svolte e alle modalità di gestione e contenimento dei rischi; tali relazioni devono essere trasmesse ai presidenti del collegio sindacale, del comitato controllo e rischi e del consiglio di amministrazione e all'amministratore incaricato del Sistema di Controllo Interno e di Gestione dei Rischi. Inoltre, è previsto che la funzione di Internal Auditing possa essere affidata esternamente ad un soggetto in possesso dei requisiti di professionalità, indipendenza e organizzazione.

Il collegio sindacale, nonostante venga definito dal Codice di Autodisciplina come "*il vertice del sistema di vigilanza di un emittente*", trova in realtà poco spazio nell'articolo 7, il quale si limita a stabilire che tale organo vigila sull'adeguatezza del Sistema di Controllo Interno e Gestione dei Rischi. Tralasciando le disposizioni relative alla composizione – e, quindi, a tutti i profili riguardanti le cause di ineleggibilità e decadenza, i requisiti di onorabilità e professionalità, i limiti relativi al numero degli incarichi e alla minoranza – le funzioni del collegio sindacale devono essere esaminate prendendo in considerazione il combinato disposto costituito dal TUF e dal Codice Civile[23]. Dall'analisi di queste disposizioni emerge che i ruoli principali del collegio sindacale sono: vigilare sul rispetto della legge, dello statuto e dei principi di corretta amministrazione; valutare l'idoneità della struttura organizzativa della società e del suo sistema amministrativo e contabile e, come visto sopra, monitorare l'adeguatezza del Sistema di Controllo Interno.

Lo scenario degli attori coinvolti nel Sistema di Controllo Interno è completato dall'organismo di vigilanza (OdV) introdotto dal D.lgs 231/2001, che prevede, come già richiamato in precedenza, che la responsabilità dell'ente per reati commessi dai vertici aziendali e dai soggetti a loro sottoposti viene meno nell'ipotesi in cui l'azienda si doti di un modello di organizzazione, gestione e controllo idoneo, sia presente un organismo di vigilanza che vigili sul funzionamento del modello e si dimostri che l'autore del reato ha agito fraudolentemente. L'organismo di vigilanza deve controllare che il modello di organizzazione, gestione e controllo sia adeguato e correttamente applicato e proporre le modifiche e gli aggiornamenti necessari. Esso non ha poteri diretti di intervento nel caso in cui riscontri delle anomalie durante la sua attività di monitoraggio, ma in tali ipotesi deve riferire immediatamente al vertice societario le anomalie individuate e, più in generale, i risultati delle verifiche periodicamente effettuate.

Infine - in relazione alle dimensioni, alla complessità e al profilo di rischio dell'impresa - specifici compiti, nell'ambito del SCI, possono essere assegnati ad altri ruoli e funzioni[24].

L'intera architettura del Sistema di Controllo Interno si articola su tre livelli. I controlli "di primo livello" o "di linea" sono quelli effettuati dai responsabili di aree operative e sono di carattere

[23] V. art. 2403 del Codice Civile e artt. 149,150, 151 del TUF.

[24] V. Codice di Autodisciplina, art 7.P.3 e criteri applicativi.

procedurale, informatico, amministrativo-contabile, ecc. Sono indispensabili per tutte le aziende di qualsiasi dimensione in quanto garantiscono il corretto svolgimento delle operazioni sul piano operativo, del rischio e normativo e assicurano così la tenuta dell'intero sistema. I controlli "di secondo livello" sono quelli di gestione consistenti nella pianificazione e nel controllo sul *business* aziendale. Sono affidati alle funzioni aziendali e sono volti a presidiare il processo di monitoraggio e gestione dei rischi aziendali, compresi il rischio legale e di *compliance*. Dei controlli "di terzo livello" è investita la funzione di Internal Audit che svolge un'attività di verifica generale sulla struttura e fornisce una garanzia (*assurance*) indipendente sul funzionamento dei controlli interni, come verrà approfondito nel prossimo paragrafo.

La seconda definizione di controllo interno, una delle più autorevoli, è quella fornita dal *CoSO Report*. Nell'ottica del *CoSO*, il controllo interno è un processo che coinvolge consiglio di amministrazione, dirigenti e tutto il personale aziendale ed è volto a fornire una ragionevole sicurezza sul perseguimento di obiettivi aziendali in relazione ai seguenti aspetti:

- efficacia ed efficienza delle attività operative (*Operations*);
- attendibilità del bilancio e delle informazioni finanziarie (*Financial reporting*);
- conformità a leggi e regolamenti (*Compliance*).

Questa definizione risulta particolarmente utile in quanto contiene al suo interno tutti gli elementi principali caratterizzanti il Sistema di Controllo Interno.

Primo aspetto fondamentale è la concezione di controllo interno come "processo": non si tratta, infatti, di un'attività isolata da svolgere in specifiche circostanze né di un fine da raggiungere, bensì del processo, del mezzo attraverso il quale perseguire determinati obiettivi.

Questo processo è attuato da soggetti ad ogni livello dell'organizzazione ed è la stessa definizione ad individuare gli attori del sistema: "il consiglio di amministrazione, i dirigenti ed altri soggetti della struttura aziendale". Si evince chiaramente che il controllo interno è considerato un elemento rilevante del sistema direzionale e una delle principali responsabilità del management, non coinvolgendo esclusivamente organi di controllo quali collegio sindacale, revisore o altre funzioni di controllo interne all'azienda[25].

Dalla definizione emerge anche che il fine del controllo interno è quello di fornire una "ragionevole sicurezza" sul conseguimento di determinati obiettivi: il controllo interno, dunque, è in grado di fornire non la certezza assoluta bensì solo un ragionevole livello di sicurezza sul raggiungimento degli obiettivi, da intendersi come probabilità di realizzazione degli stessi date le risorse a disposizione e la struttura organizzativa adottata. Questo limite intrinseco al Sistema di Controllo Interno è dovuto principalmente al fatto che questo processo, come già ricordato, non è un insieme di

[25] V. ODCEC, *Caratteristiche e definizioni del Sistema di Controllo Interno*.

procedure e manuali ma è messo in atto da persone e, perciò, è esposto al rischio di valutazioni sbagliate, errori, sviste nonché alla possibilità di violazioni ed elusioni delle regole.

Il *CoSo Report*, nel definire il controllo interno, prevede anche i principali obiettivi, comuni a tutte le imprese, che devono essere perseguiti: l'efficacia e l'efficienza della gestione operativa (*operations*), l'attendibilità delle informazioni finanziarie (*financial reporting*) e il rispetto delle regole (*compliance*).

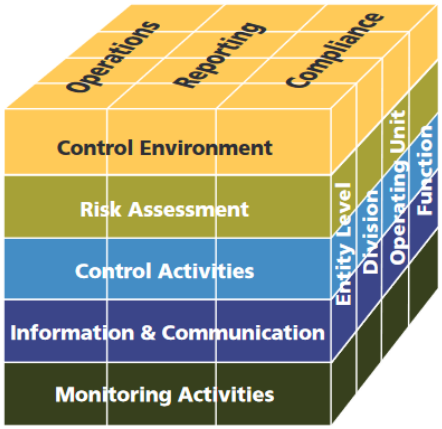
Per la realizzazione del primo obiettivo, riconducibile alla categoria delle attività operative, il SCI deve garantire un'adeguata struttura interna in grado di consentire il perseguimento degli obiettivi strategici attraverso un impiego efficace ed efficiente delle risorse. Il raggiungimento di questo obiettivo permette, nel medio lungo termine, di salvaguardare il patrimonio aziendale.

Il secondo obiettivo riguarda le informazioni di bilancio e, in particolare, l'affidabilità dei bilanci e delle informazioni finanziarie pubblicate dall'impresa. Per poter essere considerata attendibile, l'informazione generata dall'impresa deve rispecchiare la realtà alla quale si riferisce e possedere i requisiti dell'esistenza, della completezza, dell'accuratezza e della tempestività. Con specifico riferimento ai bilanci, l'attendibilità è garantita se questi sono redatti in maniera corretta e nel rispetto dei principi contabili e della legge.

L'obiettivo di conformità richiede lo svolgimento dell'attività di impresa nel rispetto delle leggi e dei regolamenti in vigore, sia esterni che interni. L'impresa deve operare nel rispetto della normativa proveniente dall'esterno come Codice Civile, Testo unico della Finanza, normativa tributaria, ma anche dei regolamenti interni, tra cui codici di condotta, procedure di autorizzazione e di delega e politiche aziendali in genere. L'obiettivo di conformità, insieme a quello di attendibilità delle informazioni, essendo basato su norme provenienti dall'esterno, è particolarmente importante per l'immagine dell'impresa in quanto, se rispettato, consente di migliorarne la reputazione agli occhi di tutti gli *stakeholder*.

Il *CoSO Report* non si limita a fornire una definizione di Sistema di Controllo Interno, ma prevede anche le componenti di quest'ultimo che possono essere rappresentate da una matrice tridimensionale come quella della figura 1. Quest'ultima mostra le connessioni e i rapporti diretti tra le componenti, gli obiettivi e le attività riferibili al sistema: ogni componente copre a pieno le aree relative ai tre obiettivi e si applica sia all'azienda nel suo complesso sia ad una singola unità di business/processo.

Figure 1: The COSO Cube



Fonte: J.S. McNally, "The 2013 COSO Framework & SOX Compliance", The Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Le cinque componenti, che operano congiuntamente in maniera integrata, sono:

- ambiente di controllo (*control environment*)
- valutazione dei rischi (*risk assessment*)
- attività di controllo (*control activities*)
- informazione e comunicazione (*information and communication*)
- monitoraggio (*monitoring activities*)

L'ambiente di controllo rappresenta il fondamento su cui poggia l'intero sistema e consiste nella cultura del controllo diffusa in un'organizzazione. In particolare, si identifica nell'integrità e nei valori etici dei soggetti che operano nell'impresa, da valutarsi anche sulla base della presenza o meno di codici di condotta o codici etici e del livello di diffusione e condivisione di questi da parte del personale. Compito del top management, dunque, non è solo definire i valori etici di riferimento per l'impresa, ma soprattutto comunicare tali valori all'intera organizzazione aziendale facendo in modo che vengano compresi e assimilati a tutti i livelli. A tal fine, può risultare particolarmente utile l'adozione di un codice etico in cui il management individua i principi etici e morali da rispettare nello svolgimento dell'attività aziendale. Si tratta di un insieme di norme di comportamento che indirizzano il funzionamento dell'impresa e le procedure decisionali verso il rispetto di corretti principi giuridici, etici e morali. L'adozione di un codice etico non garantisce, tuttavia, che questo venga in concreto condiviso e applicato da tutti. Per questo motivo, è necessario che i valori etici e morali di un'impresa vengano affermati ad un livello ancora più profondo della cultura aziendale rappresentato sia da un esempio quotidiano da parte del top management sia dall'adozione di procedure formali ispirate ai principi da rispettare. Testimonianza di tale cultura aziendale si può

trovare nelle relazioni sulla *corporate governance* che sempre più spesso contengono specifici riferimenti alla correttezza dei comportamenti[26].

Per quanto riguarda la valutazione dei rischi, è necessario che l'impresa disponga di un sistema capace di individuare e limitare tutti i rischi che possono pregiudicare la sopravvivenza della stessa. Sembra opportuno sottolineare, infatti, che non tutti i rischi sono oggetto di *risk assessment*, ma solo quelli che incidono sul raggiungimento degli obiettivi dell'impresa. Questo è il principale motivo per cui la prima attività che deve essere svolta dal management aziendale è quella di individuare un livello di rischio accettabile e, quindi, di mantenere l'attività dell'impresa entro tale limite.

I rischi sono funzione degli obiettivi tanto che è proprio in sede di pianificazione degli obiettivi strategici che assumono rilevanza i rischi che possono ostacolarne il raggiungimento e le relative misure di contenimento. In tale ottica, è facile comprendere perché il processo di pianificazione strategica rappresenti un presupposto ed una fase indispensabile del Sistema di Controllo Interno, pur non rientrando tra le sue componenti.

Dopo aver definito gli obiettivi e individuato i rischi ad essi associati, si deve attuare un processo di analisi dei rischi che consenta di classificarli sulla base dell'importanza e della probabilità che il rischio si verifichi. Sulla base di questa classificazione, l'analisi dei rischi deve proseguire con una stima dei costi dovuti ad eventuali perdite connesse ai rischi e con l'identificazione delle misure più opportune per contenerli. Uno degli strumenti più utilizzati per svolgere l'analisi dei rischi e per classificarli in relazione all'importanza e alla probabilità è la matrice impatto/probabilità[27]. In particolare, questa individua quattro possibili combinazioni di importanza e probabilità:

1. Bassa probabilità – Basso impatto: questa ipotesi riguarda rischi che non richiedono particolari interventi ma che devono essere monitorati in modo tale da poter intervenire se le condizioni dovessero cambiare;
2. Bassa probabilità – Alto rischio: un rischio con un'elevata rilevanza ma con una limitata probabilità di manifestarsi, come ad esempio una catastrofe naturale, può essere gestito prevedendo misure che ne attutiscano l'impatto in caso di verificazione;
3. Alta probabilità – Basso impatto: in questo caso bisogna valutare se sia necessario modificare dei processi per ridurre la probabilità o se, al contrario, la bassa rilevanza del rischio non sia in grado di pregiudicare l'operatività dell'azienda;
4. Alta probabilità – Alto impatto: i rischi con impatto e probabilità di accadimento elevati possono essere gestiti esclusivamente attraverso un efficace ed efficiente Sistema di Controllo Interno in grado di prevenirli o di contenerli in caso di verificazione.

[26] Cfr. C.A. DITTMEIER, op. cit.

[27] Cfr. M. ANACLERIO, A. MIGLIETTA, S. SQUAIELLA, *Internal auditing. Dalla teoria alla pratica*, p. 113 e ss.

La valutazione dei rischi necessita, infine, di una fase di gestione sia dei costi derivanti dall'individuazione e dal contenimento del rischio sia dei cambiamenti che possono rappresentare fonti di rischio per il Sistema di Controllo Interno.

La terza componente del SCI è costituita dalle attività di controllo. Queste sono parte integrante delle attività operative e sono finalizzate a contenere il rischio ad un livello ragionevole. Si tratta delle politiche e delle procedure messe in atto dal management per garantire l'attuazione tempestiva ed efficace delle misure di contenimento dei rischi. In particolare, le politiche prevedono in linea teorica le attività che devono essere effettuate, mentre le procedure consistono nell'applicazione e nell'attuazione delle politiche. Se dall'applicazione delle procedure emergono rilievi o debolezze, questi devono essere analizzati e, eventualmente, sottoposti ad adeguate azioni correttive. Le attività di controllo, dunque, si concentrato sulla prevenzione, sull'individuazione e sulla correzione dei rischi. È possibile distinguere, sulla base delle tempistiche, tra controlli preventivi e controlli successivi e, sulla base delle modalità, tra controlli manuali e controlli automatizzati.

A titolo esemplificativo possono citarsi alcuni tipi di controlli:

- Analisi svolte dal top management: tali attività consistono, tra l'atro, nell'analizzare le performance realizzate - comparandole con risultati di periodi precedenti, risultati di concorrenti, budget - e l'andamento delle iniziative intraprese per valutare il livello di conseguimento degli obiettivi prefissati;
- Controlli specifici sulla gestione delle attività e delle funzioni: sono i controlli che analizzano l'andamento e i dati relativi a specifiche filiali, regioni e attività;
- Attività di controllo sui sistemi informatici: i sistemi informatici devono essere sottoposti a controlli per verificarne il funzionamento in termini di precisione e compiutezza delle elaborazioni delle operazioni. In particolare, si distingue tra controlli specifici e controlli generali: i primi hanno ad oggetto singoli sistemi applicativi (ad esempio l'elaborazione di uno specifico report), mentre i secondi si riferiscono in generale a più applicazioni e supportano le attività dei controlli specifici (ad esempio verifica dei software di sistema, delle utenze, degli accessi);
- Controlli fisici: tali attività comprendono, innanzitutto, la protezione fisica di beni, attrezzatture, scorte, liquidità, etc. Questi devono poi essere soggetti a inventario e a comparazione con le risultanze contabili;
- Indicatori di performance: si tratta di controlli che mettono a confronto dati operativi o finanziari per poi analizzare i risultati derivanti da tale confronto e individuare le relative azioni correttive. Queste indagini possono avere ad oggetto tendenze e risultati anomali e imprevisti;

- Separazione delle funzioni: i compiti e le responsabilità vengono assegnati a più persone (o uffici) per limitare il rischio di commissione e occultamento di errori e irregolarità causati sia da comportamenti non intenzionali sia da frodi. Un esempio di separazione dei compiti è quello relativo al soggetto che autorizza le operazioni che deve essere diverso dal soggetto che si occupa di contabilizzarle e, ancora, da quello che custodisce i beni.

La componente dell'informazione e della comunicazione svolge un ruolo cruciale per il funzionamento del Sistema di Controllo Interno. Quest'ultimo opera adeguatamente solo se le informazioni più rilevanti vengono prontamente identificate, elaborate e diffuse in tutta l'organizzazione. Tutto ciò può avvenire anche attraverso i sistemi informativi che ricoprono, quindi, un'importanza fondamentale. Infatti, il sistema informativo consente la produzione di dati rilevanti che supportano l'assunzione di decisioni interne e che, allo stesso tempo, vengono comunicati all'esterno. All'interno dell'organizzazione è fondamentale la diffusione di informazioni relative all'importanza del controllo interno, alle responsabilità e ai ruoli di ciascun individuo. Le informazioni più rilevanti devono essere condivise a tutti i livelli dell'impresa, ma soprattutto devono essere comunicate verso l'alto attraverso meccanismi accessibili da parte di tutto il personale. In particolare, le informazioni riguardanti performance, sviluppi, rischi, progetti e altri dati significativi devono essere comunicati dalla direzione al consiglio di amministrazione; la qualità di tali informazioni influenza direttamente lo svolgimento delle funzioni del Cda. Il flusso informativo deve operare anche nella direzione opposta cioè dal Consiglio al management.

Di fondamentale importanza sono anche le comunicazioni verso l'esterno e dall'esterno. Le informazioni provenienti dall'esterno, infatti, possono essere elemento di valutazione del funzionamento del Sistema di Controllo Interno. Ad esempio, i dati provenienti dai revisori esterni, dai clienti e dai fornitori rappresentano uno strumento significativo per ricevere informazioni e anche per conoscere come viene percepita l'impresa dall'esterno[28].

La medesima rilevanza ricoprono le informazioni che l'impresa comunica verso l'esterno, ad esempio ai soci e agli stakeholders in generale, che rappresentano ulteriori strumenti di comunicazione indiretti anche per l'interno.

Proseguendo con l'ultima componente, per monitoraggio del Sistema di Controllo Interno si intende il processo volto a valutare l'idoneità dei controlli interni nonché la loro capacità di adeguarsi ai cambiamenti in modo tale da mantenere costante nel tempo la loro efficacia. Per questo motivo, l'attività di monitoraggio dovrebbe essere un processo continuo e automatico, integrato nelle attività operative, che valuta l'efficacia del SCI periodicamente. Nella pratica, la frequenza con cui queste attività devono essere svolte è stabilita sulla base della rilevanza dei rischi da contenere e della misura

[28] Cfr. P. TETTAMANZI, op. cit. p. 12 e ss.

in cui i controlli influenzano tale contenimento. La connessione con le attività operative consente di individuare tempestivamente eventuali anomalie e criticità del Sistema di Controllo Interno in modo da poter reagire con le dovute misure correttive.

Per completezza di esposizione, si ritiene utile richiamare la struttura del Sistema di Controllo Interno prevista dall' "*Enterprise Risk Management - Integrated Framework - ERM*" o *CoSO Report II* pubblicato nel 2004[29]. L'*Enterprise Risk Management* non è una modifica né una revisione del *Coso Report I*, ma, come visto in precedenza, ne rappresenta un'evoluzione che amplia il concetto di controllo e lo riconduce nell'ambito della gestione dei rischi, alla quale viene data una maggiore rilevanza, come è mostrato sotto nella figura 2.

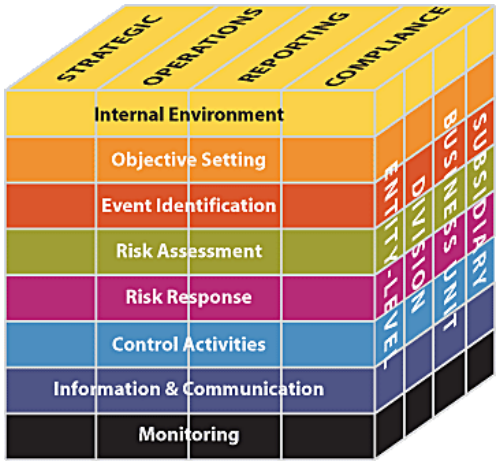


Figura 2: "*Enterprise Risk Management – Integrated Framework*" in coso.org

Ai fini di questo studio, sembra opportuno richiamare quegli elementi che hanno innovato rispetto al precedente *Framework* del 1992. In particolare rispetto al *CoSo I*, accanto agli obiettivi operativi, informativi e di *compliance*, sono stati aggiunti quelli strategici. Si tratta di obiettivi che rispecchiano la *mission* dell'impresa e consentono di perseguire i fini aziendali. Inoltre l'ERM prevede non più cinque componenti ma otto, rappresentate dalle componenti del *CoSO Report I* (l'ambiente interno, la valutazione dei rischi, le attività di controllo, informazione e comunicazione e il monitoraggio) più tre nuove componenti:

- Definizione degli obiettivi: consiste nell'individuazione da parte del management degli obiettivi aziendali in armonia con le strategie, in quanto gli obiettivi le influenzano direttamente. Poiché il perseguimento degli obiettivi richiede l'assunzione di rischi e, quindi,

[29] Come visto nel primo paragrafo, a seguito della versione del 2004 ci sono stati gli aggiornamenti del 2013 e del 2017, che non vengono richiamati in questa sede in quanto non hanno previsto novità relative alla struttura del SCI.

la previsione di misure di contenimento, la definizione degli obiettivi deve essere svolta tenendo conto del livello di rischio considerato accettabile;

- Identificazione degli eventi: permette di individuare gli eventi, interni ed esterni, che possono influenzare il raggiungimento degli obiettivi e di classificarli in base al loro impatto. Gli eventi con impatto positivo - opportunità - devono essere presi in considerazione nell'ambito della pianificazione strategica, mentre quelli con impatto negativo - rischi – sono necessari per l'individuazione delle opportune azioni di mitigazione;
- Risposta al rischio: consente al management di predisporre gli strumenti più idonei per gestire il rischio. Le risposte al rischio possono consistere nell'evitarlo, accettarlo, ridurlo e condividerlo. La scelta tra una di queste strategie, che viene effettuata sulla base di un'analisi dei costi e dei benefici, deve poi ricadere su quella che consente di contenere il rischio al di sotto del livello di accettabilità[30].

4. L'internal Auditing

Nello studio della funzione di Internal Auditing (IA) si riscontra lo stesso problema richiamato in precedenza in relazione alla definizione di Sistema di Controllo Interno. La mancanza di fonti normative contenenti definizioni univoche, infatti, è ancora più significativa in materia di Internal Auditing.

Queste lacune normative vengono, in parte, colmate dall'attività di autoregolamentazione[31] delle associazioni professionali di settore come "*The Institute of Internal Auditors - IIA*", "*The European Confederation of Institutes of Internal Auditing – ECIIA*" e "*Associazione Italiana Internal Auditors – AIIA*". Una delle più significative fonti di informazioni circa la natura e le attività di Internal Auditing è rappresentata dall' "*International Professional Practices Framework – IPPF*" pubblicato dall'IIA[32]. Il primo contenuto rilevante previsto dall'IPPF è la *mission* dell'Internal Auditing che si pone come fondamento dell'intero *Framework* per far emergere con chiarezza le finalità che tale funzione deve conseguire all'interno delle organizzazioni. La *mission* è "*proteggere ed accrescere il valore dell'organizzazione, fornendo assurance obiettiva e risk based, consulenza e competenza*".

Questo *Framework* ha poi l'obiettivo di organizzare e rendere facilmente accessibili le *Authoritative Guidance* dell'IIA. Le *Authoritative Guidance* sono i principi e le linee guida essenziali per la pratica professionale di Internal Auditing e possono suddividersi in vincolanti e raccomandate.

---

[30] Cfr. M. ANACLERIO, A. MIGLIETTA, S. SQUAIELLA, op. cit. p. 88 e ss.

[31] A tal proposito, si è già richiamato nel precedente paragrafo il Codice di Autodisciplina e le relative disposizioni riguardanti, tra l'altro, l'Internal Auditing, motivo per il quale si tralasceranno in tale sede.

[32] V. *International Professional Practices Framework – IPPF* in aiiaweb.it

Le *guidance* raccomandate sono solo consigliate alle imprese per favorire un'adeguata attuazione del codice etico e degli Standard Internazionali per la pratica professionale dell'Internal Auditing (Standard) e comprendono le guide attuative e le guide supplementari:

- le guide attuative indirizzano l'approccio e le modalità dell'attività, senza prevedere dettagli su procedure e processi, per spingere i professionisti a conformarsi agli Standard;
- le guide supplementari prevedono processi, procedure, tecniche, approcci metodologici in maniera dettagliata per consentire lo svolgimento nella pratica dell'Internal Auditing.

Le *guidance* vincolanti, invece, sono linee guida e principi ai quali le organizzazioni devono pienamente conformarsi; nascono dalle procedure stabilite e richiedono particolari modalità di *public exposure*. Esse includono: i Principi Fondamentali per la pratica professionale di Internal Auditing, la definizione di Internal Auditing, il Codice Etico e gli Standard Internazionali per la pratica professionale dell'Internal Auditing (Standard).

Di seguito, si proseguirà con brevi cenni sui Principi Fondamentali e sul Codice Etico, lasciando per ultima un'analisi più approfondita della definizione di IA e degli Standard ritenuti più significativi e rilevanti per il nostro tema di studio.

I Principi Fondamentali, se rispettati ed applicati adeguatamente, garantiscono l'efficacia della funzione di Internal Audit. Il mancato rispetto dei principi comporta il mettere in discussione che l'operato di tale funzione sia efficiente e coerente con la *mission*. Si riportano di seguito i dieci Principi Fondamentali[33]:

1. Agire con manifesta integrità
2. Dimostrare competenza e diligenza professionale
3. Mantenere obiettività ed indipendenza di giudizio (libera da indebiti condizionamenti)
4. Operare in coerenza con le strategie, gli obiettivi e i rischi dell'organizzazione
5. Avere un appropriato posizionamento organizzativo e risorse adeguate al ruolo
6. Dimostrare elevati standard qualitativi ed essere orientati al miglioramento continuo
7. Comunicare con efficacia
8. Fornire una *risk based assurance*
9. Operare con un approccio propositivo, proattivo e lungimirante
10. Favorire il miglioramento dell'organizzazione

Il Codice Etico è uno strumento finalizzato ad ispirare l'attività professionale di Internal Auditing promuovendo il rispetto della cultura etica. Esso definisce i principi e le regole di condotta che devono guidare i comportamenti sia individuali sia dell'intera organizzazione. I principi previsti dal Codice

[33] V. *International Professional Practices Framework* - Principi Fondamentali in aiiaweb.it

Etico sono l'integrità, l'obiettività, la riservatezza e la competenza e, per ciascuno di questi, le regole di condotta contengono una guida per la loro applicazione. Il principio dell'integrità dell'internal auditor "*permette lo stabilirsi di un rapporto fiduciario e quindi costituisce il fondamento dell'affidabilità del suo giudizio professionale*". Le relative regole di condotta stabiliscono che l'internal auditor deve: "*operare con onestà, diligenza e senso di responsabilità; rispettare la legge e divulgare all'esterno solo se richiesto dalle leggi e dai principi della professione; non essere consapevolmente coinvolto in attività illegali; rispettare e favorire il conseguimento degli obiettivi dell'organizzazione, se etici e legittimi*".

Il Codice Etico prevede poi l'obiettività in base alla quale "*nel raccogliere, valutare e comunicare le informazioni attinenti l'attività o il processo in esame, l'internal auditor deve manifestare il massimo livello di obiettività professionale. L'internal auditor deve valutare in modo equilibrato tutti i fatti rilevanti, senza venire indebitamente influenzato da altre persone o da interessi personali nella formulazione dei propri giudizi*". Per garantire l'obiettività l'internal auditor "*non deve partecipare ad alcuna attività o avere relazioni che pregiudichino o appaiano pregiudicare l'imparzialità della sua valutazione; non deve accettare nulla che pregiudichi o appaia pregiudicare l'imparzialità della sua valutazione; deve riferire tutti i fatti significativi a lui noti, la cui omissione possa fornire un quadro alterato delle attività analizzate*".

Il terzo principio è quello della riservatezza secondo cui "*l'internal auditor deve rispettare il valore e la proprietà delle informazioni che riceve ed è tenuto a non divulgarle senza autorizzazione, salvo che lo impongano motivi di ordine legale o deontologico*". Le regole di condotta prevedono che, per l'applicazione di questo principio, l'internal auditor "*deve acquisire la dovuta cautela nell'uso e nella protezione delle informazioni acquisite nel corso dell'incarico e non deve usare le informazioni ottenute né per vantaggio personale, né secondo modalità che siano contrarie alla legge o di nocumento agli obiettivi etici e legittimi dell'organizzazione*".

Il principio della competenza richiede che, nello svolgimento dei propri servizi professionali, l'internal auditor utilizzi "*il bagaglio più appropriato di conoscenze, competenze ed esperienze*". Ne consegue che l'internal auditor deve "*effettuare solo prestazioni per le quali abbia la necessaria conoscenza, competenza ed esperienza; prestare i propri servizi in pieno accordo con gli Standard internazionali per la Pratica Professionale dell'Internal Auditing e continuamente migliorare la propria preparazione professionale nonché l'efficacia e la qualità dei propri servizi*"[34].

Come visto sopra, tra le *guidance* vincolanti è inclusa la definizione di Internal Auditing, secondo la quale "*l'Internal Auditing è un'attività indipendente e obiettiva di assurance e consulenza, finalizzata al miglioramento dell'efficacia e dell'efficienza dell'organizzazione. Assiste l'organizzazione nel*

[34] V. *International Professional Practices Framework* – Codice Etico in aiiaweb.it

perseguimento dei propri obiettivi tramite un approccio professionale sistematico, che genera valore aggiunto in quanto finalizzato a valutare e migliorare i processi di controllo, di gestione dei rischi e di Corporate Governance"[35]. Se studiata in ogni sua componente, questa definizione consente di comprendere gli obiettivi, la natura e l'ambito di riferimento dell'attività di Internal Audit. Innanzitutto, bisogna sottolineare che si parla di attività e non di funzione. L'attenzione, dunque, si pone sulla natura dell'attività di auditing e non sull'unità organizzativa come nel passato, prescindendo dal fatto che chi la svolge sia un soggetto interno o esterno. Si ammette così la possibilità dell'*outsourcing* cioè la possibilità che il soggetto incaricato dell'attività di Internal Auditing sia esterno all'organizzazione[36].

Questa attività deve essere svolta coerentemente con gli obiettivi di indipendenza e obiettività. Per indipendenza, sul piano sostanziale, si intende neutralità *super partes* dell'attività di IA, ma allo stesso tempo non si intende esclusione di qualsiasi forma di coinvolgimento con la gestione, né mera attività di contrapposizione o correzione. Al contrario, l'Internal Auditor dovrebbe avere un atteggiamento partecipativo e propositivo, seppure con una collocazione organizzativa che gli consenta di operare senza condizionamenti. Sull'indipendenza, lo Standard 1100 - "Indipendenza e obiettività" prevede che l'internal auditor deve poter adempiere i propri compiti senza pregiudizi e vincoli così da poter giungere ad una valutazione imparziale e obiettiva. Da un punto di vista formale, l'indipendenza deve essere garantita attraverso un'adeguata collocazione organizzativa che consenta all'IA il pieno adempimento delle proprie responsabilità. Il responsabile di internal audit (RIA) deve avere accesso libero e diretto al consiglio di amministrazione e al vertice manageriale. A tal fine, l'Internal Auditing deve essere, idealmente, in posizione di dipendenza funzionale dal consiglio di amministrazione o dal comitato per il controllo interno e in posizione di dipendenza gerarchica dal vertice manageriale. A garanzia dell'indipendenza, il Codice di Autodisciplina prevede, quindi, un duplice riporto organizzativo. Il riporto funzionale al *board* e al comitato per il controllo interno rappresenta la fonte principale di indipendenza e comporta, tra l'altro: l'approvazione da parte del *board* del mandato, del piano e del budget dell'attività di IA nonché delle decisioni relative alla nomina, alla revoca e al compenso del RIA; la comunicazione da parte del RIA al *board* dei risultati delle attività di IA e la verifica ad opera del *board* dell'adeguatezza dell'ambito di copertura e delle risorse. Nella pratica, il referente diretto del RIA è il comitato per il controllo interno che fa da intermediario tra il RIA e il consiglio di amministrazione assicurando maggiore trasparenza e chiarezza delle informazioni.

Il riporto gerarchico al vertice manageriale consente di facilitare l'operatività quotidiana delle funzioni attraverso la collaborazione delle funzioni soggette ad audit, l'ampio ambito di gestione delle

---

[35] V. *International Professional Practices Framework* – Definizione di IA in aiiaweb.it

[36] Sulla questione della convenienza o meno dell'outsourcing vedi G. Palmieri, "*L'auditing si divide sull'outsourcing. Ma l'attività deve essere in linea con gli standard professionali",* Italia Oggi, p. 37.

attività di IA e l'autonomia nello svolgimento delle attività e nella comunicazione dei risultati[37]. L'internal auditor, in ogni caso, deve comunicare prontamente eventuali interferenze nelle attività svolte e nei flussi informativi al comitato per il controllo interno.

L'obiettività fa riferimento ad un atteggiamento mentale e poggia sui concetti di competenza professionale, indipendenza e imparzialità. Tale atteggiamento deve condurre l'internal auditor ad agire senza cadere in possibili conflitti di interesse o compromessi e senza sottostare al giudizio di altri. Alcuni strumenti per conseguire l'obiettività dell'IA sono: confidare nei risultati della propria attività, ricoprire gli incarichi a rotazione e non accettare compensi per l'attività[38].

Sia per l'indipendenza che per l'obiettività, oltre agli aspetti sopra richiamati, è necessario che non vi sia alcun coinvolgimento nei processi di business e nei controlli di linea. Inoltre, anche se l'indipendenza si riferisce all'intera attività di IA mentre l'obiettività è un requisito individuale richiesto all'internal auditor, le due sono strettamente connesse: infatti, l'assenza di indipendenza rende impossibile garantire l'obiettività[39].

La definizione di IA fa poi riferimento all'*assurance* e alla consulenza. L'*assurance* consente di effettuare una valutazione indipendente dei processi di gestione del rischio, di controllo o di *governance* attraverso analisi oggettive delle evidenze e dei dati risultanti dall'esecuzione di tali processi. Ricomprende quei servizi finalizzati al miglioramento dell'efficienza dei processi decisionali, in particolar modo, incrementando la qualità delle informazioni sia in termini di affidabilità e attendibilità sia in termini di modalità di produzione ed utilizzo delle stesse[40].

L'attività di consulenza prevede che l'internal auditor non si limiti a svolgere attività di ispezione e analisi, ma esegua anche attività di supporto e sostegno al fine di potenziare i controlli, il *risk management* e la *governance*. Si tratta di servizi volti a fornire valore aggiunto ma senza assumere responsabilità manageriale.

La definizione di Internal Auditing prevede poi che l'attività di IA deve essere "*finalizzata al miglioramento dell'efficacia e dell'efficienza dell'organizzazione*". Efficacia ed efficienza si pongono, quindi, come i risultati da raggiungere e mostrano il motivo principale per cui viene condotta un'attività di Internal Auditing. Il miglioramento dei due obiettivi consente di ottimizzare il conseguimento degli obiettivi (efficacia) minimizzando l'uso delle risorse scarse (efficienza). L'attività di IA comporta, dunque, lo svolgimento di una vera e propria consulenza di natura organizzativa.

---

[37] V. Standard sull'indipendenza organizzativa (S – 1110) in aiiaweb.it.

[38] V. Standard sull'indipendenza e sull'obiettività (S – 1100) in aiiaweb.it

[39] Cfr. C.A. DITTMEIER, op. cit. p. 217 e ss.

[40] Nella definizione di Internal Auditing tradotta dall'AIIA il termine *assurance* è rimasto in lingua originale perché non esiste nella lingua italiana una parola con la stessa efficacia.

Dalla definizione emerge, inoltre, che l'IA "*assiste l'organizzazione nel perseguimento dei propri obiettivi*". Tale espressione sta a significare che le decisioni relative al livello di rischio ritenuto accettabile e alle modalità per gestirli restano competenza esclusiva del management. Quest'ultimo può essere assistito dall'Internal Auditing che, comunque, ricopre un ruolo di staff, sussidiario. L'assistenza all'organizzazione avviene "*tramite un approccio professionale sistematico*". L'approccio sistematico si riscontra nel metodo di indagine e nella capacità di sistematizzare tipici della professione dell'IA che consentono di trovare soluzione ai problemi oggetto di analisi. Questo approccio ricomprende, tra l'altro, tecniche di intervista, attuazione di procedure analitiche di auditing, raccolta di dati, campionamento statistico.

Proseguendo con l'esame della definizione, va evidenziato che l'approccio sistematico implementato dall'IA "*genera valore aggiunto in quanto finalizzato a valutare e migliorare i processi di controllo, gestione dei rischi e corporate governance*". La creazione di valore aggiunto dipende dalla competenza e dalla professionalità degli internal auditors e dalla coerenza tra obiettivi della funzione e necessità concrete dell'organizzazione. In particolare, si parla di valore aggiunto in relazione alle finalità che il metodo sistematico consente di perseguire, cioè la valutazione e il miglioramento dei processi di controllo, gestione dei rischi e *corporate governance*.

I tre processi appena richiamati rappresentano la natura dell'attività di Internal Auditing, così come descritta dallo Standard 2100[41].

Per quanto riguarda il processo di *risk management* (gestione del rischio), lo Standard 2120 prevede che l'IA si assicuri che l'organizzazione abbia implementato adeguati sistemi per l'individuazione, la valutazione e la gestione dei rischi[42]. La valutazione sull'adeguatezza di questi elementi consente all'auditor di determinare se il processo di *risk management* nel suo insieme sia o meno efficace. Oggetto di valutazione devono essere i rischi relativi alla *governance,* ai sistemi informativi, alla presenza di casi di frode, agli obiettivi dell'incarico e qualsiasi altro rischio significativo. In ogni caso, gli auditors non devono assumere responsabilità manageriali attraverso una gestione diretta dei rischi.

I processi di controllo costituiscono l'oggetto primario dell'attività di monitoraggio compiuta dall'IA. Come indicato nello Standard 2130, essi consistono nel valutare l'efficacia e l'efficienza dei controlli al fine di mantenerne la validità e promuoverne il continuo miglioramento[43]. L'adeguatezza dei controlli va stabilita in relazione al raggiungimento degli obiettivi strategici, all'adeguatezza delle

---

[41] Standard 2100 –Natura dell'attività: "*L'attività di internal audit deve valutare e contribuire al miglioramento dei processi di governance, gestione del rischio e controllo dell'organizzazione, tramite un approccio sistematico, rigoroso e risk based. La credibilità e il valore dell'internal auditing sono rafforzati quando gli auditor agiscono in maniera proattiva e le loro valutazioni offrono nuove riflessionie tengono in considerazione gli impatti futuri*".

[42] V. Standard sulla gestione del rischio (S – 2120) in aiiaweb.it.

[43] V. Standard sul controllo (S – 2130) in aiiaweb.it.

informazioni, all'efficacia delle operazioni, alla salvaguardia del patrimonio e al rispetto delle normative.

Lo Standard 2110 prevede tra le finalità dell'Internal Auditing anche quella di assistere l'organizzazione nel miglioramento del processo di *governance*[44]. L'IA deve valutare la *governance* nel suo complesso per verificare se l'architettura presente nell'organizzazione sia idonea a garantire la correttezza gestionale e la trasparenza informativa, oltre che lo sviluppo di valori etici adeguati e la creazione di valore per tutti gli *stakeholder*[45].

Infine, si ritiene utile richiamare brevemente le interrelazioni che si instaurano tra l'IA e gli altri organi di controllo. Il consiglio di amministrazione e il comitato per il controllo possono svolgere compiutamente le attività di verifica sull'idoneità del SCI soprattutto grazie ai flussi informativi garantiti dal responsabile dell'internal auditing in esito alle verifiche svolte.

L'Internal Auditing svolge un fondamentale ruolo di supporto anche al collegio sindacale, in particolare nelle attività di controllo dei rischi e del sistema informativo contabile. In relazione a tali attività, diviene ancora più importante l'esigenza di informazioni complete e obiettive provenienti dall'IA che consentono, se necessario, di attuare eventuali misure di urgenza.

L'Internal Auditing è poi il principale riferimento per le funzioni dell'Organismo di Vigilanza (OdV) ex D.ls 231 del 2001. Se l'organismo è composto da soggetti interni tra questi vi è il responsabile dell'internal auditing; ma anche quando l'organismo è costituito solo da soggetti esterni, l'IA è indispensabile in quanto l'OdV può affidarsi a tale funzione per buona parte degli obiettivi di vigilanza e, più in generale, per ricevere assistenza, anche operativa, quando necessario.

Anche le funzioni di controllo di secondo livello fanno affidamento sull'Internal Auditing per ricevere supporto e consulenza. In particolare, l'IA verifica che queste funzioni vengano svolte coerentemente con l'efficacia e l'efficienza del SCI e fornisce le informazioni più opportune per i processi di gestione dei rischi. Per contrastare il rischio di sovrapposizioni e duplicazioni di attività, il ruolo dell'IA deve limitarsi ad offrire le informazioni richieste e i chiarimenti sulle metodologie utilizzate per le valutazioni dei rischi e dei controlli e sull'andamento del Sistema di Controllo Interno.

Allo stesso modo, l'Internal Auditing fornisce consulenza ai controlli di linea, con riferimento alle sole attività che possono impattare sul SCI e verifica la corretta attuazione di tali controlli[46].

Date tutte le interrelazioni instaurate, l'IA è in grado di avere e di comunicare una rappresentazione complessiva dello stato di salute del Sistema di Controllo Interno, perseguendo in tal modo uno degli obiettivi principali della funzione.

---

[44] V. Standard sulla governance (S – 2110) in aiiaweb.it.

[45] La pianificazione e lo svolgimento dell'attività di Internal Auditing con i relativi Standard saranno oggetto dell'ultimo capitolo, con focus specifico sul settore bancario.

[46] Cfr. C. A. DITTMEIER, op. cit. p. 101 e ss.

In conclusione, l'IA grazie alle sue attività e ai flussi informativi costantemente diretti agli altri organi societari rappresenta il filo conduttore che guida le varie funzioni e fa sì che operino all'interno del sistema in modo integrato, coordinandosi e collaborando per il raggiungimento di obiettivi comuni e nell'interesse della società e di tutti gli stakeholder.

CAPITOLO 2

Il Supervisory Review Process

1. Il contesto normativo e regolamentare

Il *Supervisory Review Process* (SRP) si afferma in un contesto normativo e di regolamentazione risalente nel tempo. Nel 1974 a Basilea i Governatori delle Banche Centrali appartenenti al G10 fondano all'interno della Banca dei Regolamenti Internazionali (BRI) un comitato, conosciuto come Comitato di Basilea[47]. Questa organizzazione ha l'intento di perseguire la stabilità economica e finanziaria attraverso la cooperazione tra le Banche Centrali e l'armonizzazione dei processi nazionali di vigilanza. L'attività del Comitato si esplica attraverso l'emanazione di linee guida, standard e raccomandazioni che, tuttavia, non hanno efficacia legale nei diversi paesi membri. L'operatività di queste disposizioni è, dunque, rimessa alle singole autorità nazionali che, nella fase di recepimento delle stesse, dovrebbero prediligere approcci condivisi con gli altri ordinamenti. Ad oggi, le proposte del Comitato vengono accolte alla stregua di normativa vincolante in molti paesi, tra cui l'Italia dove vengono recepite nelle Disposizioni di Vigilanza per le Banche emesse da Banca d'Italia[48]. Di seguito, si richiamano, seppure brevemente, i principali accordi di Basilea che hanno aperto la strada all'attuale contesto di regolamentazione.

Un primo contributo in tema di vigilanza prudenziale da parte del Comitato di Basilea si ha nel 1988 con il cosiddetto "Accordo di Basilea I". Nell'ottica dell'armonizzazione delle regole prudenziali rivolte alle banche dei diversi paesi, tale accordo si pone come obiettivi quello di migliorare la stabilità e la solvibilità delle banche a livello internazionale e quello di ridurre eventuali elementi di disparità sia sul piano concorrenziale sia sul piano regolamentare. Viene affrontato, a tal proposito, il tema dell'adeguatezza patrimoniale della banca rispetto al rischio di credito assunto. In base a quest'ultimo principio, ad ogni apertura di credito deve corrispondere, in via precauzionale, una copertura di capitale tanto maggiore quanto più è elevato il rischio correlato a quella attività. L'adeguatezza patrimoniale viene misurata attraverso il c.d. coefficiente patrimoniale di solvibilità che individua l'entità del patrimonio di vigilanza in relazione alle attività ponderate per il rischio e che non può essere inferiore all'8%[49]. In estrema sintesi, l'ammontare minimo di patrimonio di vigilanza che le banche devono mantenere deve essere uguale all'8% delle attività ponderate in relazione ai rischi di perdita.

---

[47] Si tratta dei governatori delle banche centrale di Belgio, Canada, Francia, Germania, Giappone, Italia, Olanda, Regno Unito, Svezia, Svizzera (dal 1984), USA.

[48] Banca d'Italia, circolare n. 285 del 17 dicembre 2013 – ultimo aggiornamento del 2 novembre 2016.

[49] La formula può essere riassunta come segue: coefficiente patrimoniale = PV/APR ≥ 8%, dove PV = patrimonio di vigilanza e APR = attività ponderate per il rischio.

L'attenzione verso le problematiche riguardanti la vigilanza bancaria e la supervisione prudenziale spinge il Comitato di Basilea a pubblicare nel 1998 lo "*Schema per i sistemi di controllo interno nelle organizzazioni bancarie*"[50]. Questo schema individua i principali elementi del sistema dei controlli, che coinvolge tutte le operazioni bancarie, e i principi in relazione ai quali le autorità di vigilanza devono valutare l'adeguatezza del sistema[51]. Il documento si basa, dunque, sul principio in base al quale buone regole di vigilanza prudenziale debbano riferirsi non solo a requisiti quantitativi, come il coefficiente patrimoniale di solvibilità, ma anche a requisiti qualitativi, come un efficiente ed adeguato sistema dei controlli interni. Come si vedrà più nel dettaglio nel terzo capitolo, si diffonde l'idea secondo cui un rigoroso sistema dei controlli interni è, da un lato, un elemento essenziale per la corretta amministrazione delle banche e per la stabilità del sistema finanziario in generale e, dall'altro, un criterio indispensabile di valutazione a disposizione della Vigilanza.

Negli anni seguenti i parametri stabiliti da Basilea I si rivelano troppo rigidi e statici rispetto a vari profili, tra cui le diverse tipologie di rischio, i diversi livelli di solvibilità e le diverse scadenze. I limiti dell'accordo del 1988 fanno nascere l'esigenza di un nuovo schema di adeguatezza patrimoniale e di valutazione dei rischi che nel 2004 viene trasfuso nel "*Nuovo accordo sul capitale o Convergenza internazionale della misurazione del capitale e dei coefficienti patrimoniali*", conosciuto anche come Basilea II. Il Nuovo accordo sul capitale (NAC) si fonda su tre punti focali, i cosiddetti pilastri, riguardanti i requisiti patrimoniali minimi, il processo di controllo prudenziale e la disciplina di mercato. Con riguardo al primo pilastro, la principale novità consiste nell'ampliare le tipologie di rischio in relazione alle quali va determinato il requisito patrimoniale minimo ricomprendendo, oltre al rischio di credito, anche il rischio di mercato e il rischio operativo. In particolare, viene prevista una modifica non del coefficiente di solvibilità, bensì delle procedure di quantificazione delle "attività ponderate per il rischio", che possono consistere in metodologie standard stabilite dalla normativa di vigilanza oppure in metodologie sviluppate dall'intermediario (in questo secondo caso, è necessaria un'autorizzazione dell'Autorità di Vigilanza). L'idea di fondo del NAC è, dunque, che il patrimonio di vigilanza debba essere individuato attraverso la ponderazione di tutte le attività per i diversi fattori di rischio, sempre nel rispetto del limite dell'8%[52].

Il secondo pilastro introduce il processo di controllo prudenziale o *Supervisory Review Process* (SRP) con l'intento di incentivare l'instaurazione di dialoghi e interrelazioni tra banche e Autorità di

---

[50]: Cfr. Comitato di Basilea (1998), "*Schema per i sistemi di controllo interno nelle organizzazioni bancarie",* traduzione italiana in www.bis.org.

[51] Tutti i principi e gli aspetti della vigilanza bancaria che interessano più nel dettaglio il sistema dei controlli interni saranno affrontati nel corso del terzo capitolo.

[52] Cfr. C.A. DITTMEIER, "*Internal Auditing. Chiave per la corporate governance",* dove il concetto viene sintetizzato nella formula: Patrimonio di Vigilanza ≥ 8%* [(RWA Rischio Credito) + (RWA Rischio mercato) + (RWA Rischio Operativo)] dove RWA (Risk-Weighted Assets) rappresenta l'attivo ponderato in funzione dei rischi.

Vigilanza, affidando alle prime il compito di implementare processi interni di valutazione dell'adeguatezza del capitale rispetto ai rischi assunti e alle seconde di vigilare su tali attività ed intervenire ove necessario. Rimandando al secondo paragrafo una disamina più dettagliata del SRP e delle sue fasi, in questa sede si ritiene opportuno evidenziare il grande cambiamento introdotto da Basilea II e rappresentato da una nuova concezione di vigilanza prudenziale. Questa concezione prevede in capo ai vertici delle banche il dovere di individuare la natura e il livello di rischio assunto e, in relazione a questo, di valutare l'adeguatezza dei mezzi propri in un'ottica attuale e prospettica. Ciò deve avvenire sotto il controllo delle Autorità di Vigilanza con le quali le banche devono intrattenere dialoghi frequenti e diretti, così da consentire alle stesse di intervenire celermente, ma anche di concentrare la loro attenzione su intermediari con profili di rischio o operativi maggiormente critici.

Il terzo pilastro riguarda la disciplina di mercato e la trasparenza delle informazioni. Questi due aspetti sono strettamente connessi tra loro in quanto è indispensabile un elevato grado di trasparenza delle informazioni rivolte al pubblico se si vuole che il mercato e la conseguente selezione operino come spinta all'adozione di un patrimonio di vigilanza adeguato da parte delle banche. A tal fine il NAC individua l'informativa minima che le banche devono comunicare all'esterno, in particolare, sulla situazione patrimoniale e finanziaria, sui profili di rischio e sulla gestione. Lo schema di adeguatezza patrimoniale previsto da Basilea II viene recepito dalla regolamentazione europea attraverso le direttive 2006/48/CE e 2006/49/CE e da quella nazionale attraverso alcune modifiche al Testo unico bancario e la circolare n. 263 del 27/12/2006 di Banca d'Italia[53].

Così come per Basilea I, anche per il Nuovo accordo emergono alcuni limiti tra cui l'impossibilità di plasmare lo schema di vigilanza previsto alle varie realtà delle banche, a discapito, in particolare, di quelle di minori dimensioni; il fenomeno della prociclicità finanziaria, causa dell'aumento del costo di approvvigionamento al credito; l'ignorare il rischio di liquidità correlato alla creazione di un "cuscinetto" di capitale come salvagente nei casi di insolvenza.

I punti critici di Basilea II, resi ancor più evidenti dalla crisi finanziaria del 2007/2008, portano il Comitato di Basilea a considerare l'eventualità di una riforma di tale accordo. Dopo alcune variazioni apportate a Basilea II, nel 2010 viene approvato un nuovo accordo, conosciuto come Basilea III[54]. Basilea III mantiene lo schema della regolamentazione precedente richiamando dunque i tre pilastri, ma, allo stesso tempo, introduce alcuni aspetti innovativi. In particolare, il nuovo accordo amplia il requisito minimo del patrimonio di vigilanza e migliora la copertura dei rischi. Introduce, inoltre, il

[53] Banca d'Italia (2006), *Nuove disposizioni di vigilanza prudenziale per le banche*, Circ. n. 263 del 27/12/2006 e successivi aggiornamenti in www.bancaditalia.it.

[54] Nel 2010 viene annunciato l'inizio dei lavori, mentre l'entrata in vigore è prevista in più fasi, a partire dal 2013 fino ad arrivare all'applicazione dell'accordo nella sua totalità nel 2019.

c.d. *leverage ratio* per il controllo dell'indebitamento del sistema bancario e altri indici per il controllo della liquidità.

Per completezza di esposizione, si ritiene necessario richiamare all'attenzione i numerosi tentativi di modifica anche di quest'ultimo accordo; tentativi di entità tale da rappresentare un vero e proprio progetto di riforma al quale si fa riferimento con il nome di Basilea IV. L'entrata in vigore di tali modifiche dovrebbe cominciare a partire dal 2021 per poi arrivare ad una completa attuazione nel 2027. Le novità principali riguardano, tra l'altro, gli approcci, sia standard sia avanzati, per i rischi di credito, di mercato e operativi, nonché il regime delle cartolarizzazioni e hanno come obiettivo quello di imporre limiti più restrittivi sui rischi, in particolare quelli di credito e quelli operativi, intervenendo sugli accantonamenti prudenziali.

Le regole sino ad ora richiamate, in particolare quelle previste da Basilea III, sono recepite dalla normativa europea attraverso il c.d. "pacchetto CRR-CRD IV" contenente la direttiva 36/2013/UE – *Capital Requirements Directive* (CRD IV) – e il regolamento UE/575/2013 – *Capital Requirements Regulation* (CRR). L'obiettivo principale di queste disposizioni è ridurre la discrezionalità degli Stati nell'applicazione delle regole di vigilanza prudenziale, che è causa di distorsioni della concorrenza e di arbitraggi regolamentari. In breve, la nuova normativa prevede nuove regole riguardanti diversi aspetti della vigilanza prudenziale, tra cui[55]:

a) l'obbligo di aumentare il livello sia qualitativo sia quantitativo del patrimonio di vigilanza da accantonare;
b) l'obbligo di classificare il capitale in base alla qualità e al rischio;
c) la previsione di requisiti specifici per ridurre il rischio di controparte;
d) l'obbligo di comunicare il coefficiente di leva finanziario, impedendo una leva finanziaria troppo elevata che possa mettere a rischio la solvibilità della banca;
e) l'obbligo di disporre di attività liquide sufficienti.

Con specifico riferimento alla qualità del capitale, vengono introdotte sia la nozione di *common equity tier 1* corrispondente, nella sostanza, alle azioni ordinarie e alle riserve provenienti da utili sia riserve addizionali in funzione di conservazione del capitale, in funzione anticiclica e per le istituzioni a rilevanza sistemica. In particolare:

- la riserva di conservazione del capitale è volta a preservare il livello minimo di capitale regolamentare nei momenti di tensione del mercato;
- la riserva di capitale anticiclica ha lo scopo di proteggere il settore bancario nelle fasi di eccessiva crescita del credito;

[55] Per maggiori dettagli si rimanda al sito internet del Consiglio europeo e del Consiglio dell'Unione europea e al comunicato stampa della Commissione europea, CRD IV/CRR, *Frequently asked questions.*

- le riserve di capitale per gli enti a rilevanza sistemica globale (G-SII buffer) e quelle per gli altri enti a rilevanza sistemica (O-SII buffer), richiedono risorse patrimoniali aggiuntive a quei soggetti che proprio per la loro rilevanza sistemica, globale o domestica, pongono rischi maggiori per il sistema finanziario.

L'obbligo di riserve di capitale aggiuntive comporta la dotazione, da parte delle banche, di mezzi patrimoniali di elevata qualità cui ricorrere in occasione di tensione del mercato per prevenire disfunzioni del sistema bancario ed evitare interruzioni nel processo di erogazione del credito oltre che per fronteggiare rischi derivanti dalla rilevanza sistemica a livello globale o domestico di talune banche. Infine, la normativa europea prevede obblighi di *disclosure*, con frequenza annuale, con riferimento alle informazioni relative all'utile/perdita prima delle imposte, all'ammontare delle imposte stesse sull'utile/perdita e ai contributi pubblici ricevuti e l'ulteriore obbligo di *disclosure* del coefficiente di leva finanziaria.

Il ricorso allo strumento normativo del regolamento, accanto a quello della direttiva, per consentire di salvaguardare le diverse specificità delle giurisdizioni destinatarie del regolamento, prevede alcune discrezionalità nazionali che possono essere esercitate dagli Stati membri e dalla Autorità di vigilanza. In ogni caso, va comunque evidenziato che tali discrezionalità sono di gran lunga inferiori rispetto a quelle previste dalla normativa precedente. La Banca d'Italia le ha esercitate tenendo conto sia dell'attuale impianto normativo e degli orientamenti e delle best practices di vigilanza maturati negli ultimi anni a livello internazionale sia delle peculiarità del mercato italiano nel contesto europeo.

In Italia, il D.lgs. n. 72 del 12 maggio 2015, sulla base della delega contenuta nell'articolo 3 della L. n. 154 del 7 ottobre 2014 (Legge di delegazione europea 2013 - secondo semestre), apporta alcune modifiche al Testo Unico Bancario e al Testo Unico della Finanza dirette proprio al recepimento della Direttiva CRD IV. Il Regolamento CRR, direttamente applicabile nel nostro ordinamento, viene attuato con la circolare n. 285 del 17 dicembre 2013 (e successivi aggiornamenti) della Banca d'Italia.

Nonostante le regole del "pacchetto CRR-CRD IV" vengano recepite anche dagli altri Stati dell'Unione europea piuttosto celermente, l'attuazione completa del nuovo sistema di regolazione non è stata altrettanto rapida, in particolare, a causa della situazione di stallo relativa all'applicazione di alcuni standards di Basilea III (tra cui, quelli relativi a *Leverage Ratio, Fundamental Review of Trading Book, Net Stable Funding Ratio*). Si deve attendere il febbraio 2019 per un nuovo pacchetto di regole attuativo degli standards sopra citati e che modifica in parte la Direttiva CRD IV, il Regolamento CRR, nonché la Direttiva 2014/59/UE ed il Regolamento n. 806/2014 in materia di risanamento e risoluzione delle banche in dissesto.

A livello nazionale, gli interventi più rilevanti in materia di vigilanza prudenziale sono la circolare n. 263 del 27 dicembre 2006 (Nuove disposizioni di vigilanza prudenziale per le banche), la circolare

n. 269 del 7 maggio 2008 (Guida per l'attività di vigilanza) e la circolare n. 285 del 17 dicembre 2013 (Disposizioni di vigilanza per le banche).

Con la circolare n. 263 del 27 dicembre 2006, Banca d'Italia dà applicazione alla disciplina di Basilea II[56]. Tale circolare, benché abrogata in gran parte dal framework di Basilea III e, in particolare, dalla relativa circolare n. 285, resta ancora in vigore per alcuni aspetti, quali la disciplina dei conflitti di interesse verso i soggetti collegati e la disciplina del Sistema dei Controlli Interni, introdotta con il 15° Aggiornamento. L'obiettivo, di profonda portata innovativa, è quello di diffondere all'intera vita aziendale la cultura dei rischi, attraverso l'identificazione degli stessi, la fissazione dei limiti, il ruolo delle funzioni di controllo, i flussi informativi ed altri ulteriori aspetti[57].

Brevemente si può osservare che la circolare 263 ha ancora un ruolo portante quantomeno in relazione al Titolo V, in particolare, ai capitoli sui soggetti collegati e ai capitoli 7, 8 e 9, introdotti appunto con il richiamato 15° Aggiornamento[58].

Questi capitoli riguardano:

- Il Sistema dei Controlli Interni (Capitolo7).
- Il Sistema Informativo (Capitolo 8).
- La Continuità Operativa (Capitolo 9).

In quanto di maggiore interesse ai fini del presente lavoro, si richiamano gli interventi relativi al Sistema dei Controlli Interni (SCI).

La normativa, entrata in vigore a partire dal mese di luglio 2014, impone alle istituzioni finanziarie una serie di nuovi obblighi e vincoli. Si è registrato un notevole sforzo delle banche per adeguarsi e tradurre la nuova disciplina in regole, assetti organizzativi, metodologie e strumenti applicativi concreti.

La circolare affronta due diversi ambiti di particolare rilievo:

- Dimensione organizzativa: le disposizioni enfatizzano la necessità di una definizione precisa degli organi e delle funzioni aziendali, in particolare dell'organo di gestione e con funzione strategica e dell'organo con funzione di controllo. Viene dato rilievo alle procedure di nomina dei responsabili delle funzioni di controllo e ai relativi requisiti professionali e all'esigenza di idonee linee di riporto tra gli organi di controllo e quelli di amministrazione. In particolare, si evidenzia l'importanza di una netta separazione dei controlli di terzo livello, quelli in capo all'Internal Audit, dai controlli di secondo livello.

[56] Banca d'Italia, *Nuove disposizioni di vigilanza prudenziale per le banche,* Circ. n. 263 del 27 dicembre 2006.
[57] C. BRESCIA MORRA e G. MELE (2014), "*Le nuove fonti della vigilanza prudenziale*".
[58] Banca d'Italia (2014), Nota di chiarimento del 6 giugno 2014, "*Sistema dei controlli interni, sistema informativo e continuità operativa*".

- Dimensione degli ambiti di responsabilità delle funzioni di controllo: la circolare 263 elenca in modo molto ampio il perimetro delle attività e delle competenze connesse, concentrandosi sulla funzione di *risk management* e su quella di *compliance.* Prevede, inoltre, la necessità del documento di Coordinamento e Politiche in materia di SCI, che deve fungere da policy di riferimento sia a livello metodologico che di processo. Introduce il *Risk Appetite Framework*, più noto come RAF. Su tutti i rischi identificati e mappati, meglio se quantificabili, la banca deve definire, tra gli altri, gli obiettivi di rischio (*target o risk appetite*), la deviazione consentita da tale risk appetite (*risk tolerance*), il massimo rischio sopportabile (*risk capacity*) per vincoli di patrimonio o normativi. La banca deve sapere misurare effettivamente il livello di rischio (*risk profile*). È necessario individuare profili di coerenza e contestualizzazione con il processo ICAAP di auto-valutazione dell'adeguatezza patrimoniale.

Un altro richiamo che si ritiene particolarmente utile è quello alla circolare 269 del 7 maggio 2008, recante una "Guida per l'attività di vigilanza", date le numerose disposizioni riguardanti il *Supervisory Review and Evaluation Process*, oggetto del presente studio[59]. Infatti, in questa guida sono contenuti i criteri generali e le metodologie utilizzate dalla Banca d'Italia, in coerenza con la disciplina europea, nel processo di revisione e di valutazione prudenziale (SREP) e i requisiti minimi del processo aziendale di valutazione dell'adeguatezza patrimoniale (*Internal Capital Adequacy Assessment Process* - ICAAP) condotto dagli intermediari vigilati. In particolare, la Guida ha l'obiettivo di predisporre uno schema operativo unitario per il processo SREP, al quale i responsabili della vigilanza possono fare riferimento, garantendo in tal modo la coerenza dei comportamenti e delle valutazioni. Inoltre, nella Guida si trova anche una disciplina delle attività di controllo sugli intermediari, fatta eccezione per le sole fasi costitutive e procedure di risoluzione. La circolare fornisce gli strumenti affinché sia garantita l'efficacia e l'efficienza della vigilanza sulle condizioni di sana e prudente gestione e sul rispetto della normativa, sempre secondo i principi di trasparenza e proporzionalità.

Infine, si richiama la circolare n. 285 del 17 dicembre 2013, entrata in vigore il 1 gennaio 2014, con cui la Banca d'Italia illustra le nuove disposizioni di vigilanza per le banche e le imprese di investimento, recependo il "pacchetto CRR-CRD IV", costituito, come già detto, dalla direttiva 2013/36/UE e dal regolamento UE 575/2013[60]. Con la circolare n. 285/2013 vengono rivisitate ed aggiornate le diposizioni in tema di vigilanza prudenziale, sicché dalla data di entrata in vigore della circolare, alle banche e ai gruppi bancari restano applicabili solo alcuni capitoli della precedente circolare n. 263/2006. In particolare, i capitoli relativi al Governo e alla gestione del rischio di

[59] Banca d'Italia, *Guida per l'attività di vigilanza,* Circ. n. 269 del 7 maggio 2008.
[60] Banca d'Italia, *Disposizioni di vigilanza per le banche*, Circ. n. 285 del 17 dicembre 2013.

liquidità (Tiolo V, Capitolo 2), alle Obbligazioni bancarie garantite (Titolo V, Capitolo 3), alle Attività di rischio e conflitti di interesse nei confronti di soggetti collegati (Titolo V, Capitolo 5), alla Banca depositaria di OICR e fondi pensione (Titolo V, Capitolo 6), al Sistema dei controlli interni (Titolo V, Capitolo 7), al Sistema informativo (Titolo V, Capitolo 8) e alla Continuità operativa (Titolo V, Capitolo 9).

Fatti salvi tali capitoli, la circolare n. 285/2013 abroga, per le banche e i gruppi bancari, la circolare n. 263/2006 che continua ad essere applicata completamente solo alle SGR, agli IMEL, agli istituti di pagamento e agli intermediari finanziari ex art. 107 del Testo Unico Bancario (TUB), relativamente ai riferimenti a essa contenuti nelle rispettive disposizioni di vigilanza.

Le nuove "Disposizioni di vigilanza per le banche" mirano a potenziare le prerogative delle banche in relazione alle proprie capacità di assorbire shock derivanti da tensioni finanziarie ed economiche, a migliorare la gestione del rischio e la *governance* e a rafforzare la trasparenza e l'informativa delle banche, in considerazione degli spunti e degli insegnamenti della crisi finanziaria. La circolare 285 fa suo il sistema imperniato sui tre pilastri con il fine di accrescere quantità e qualità della dotazione di capitale degli intermediari, focalizzando l'attenzione anche su strumenti di vigilanza anticiclici e, nel contempo, introducendo norme sulla gestione del rischio di liquidità. In definitiva, si introduce un duplice ordine di riforma, uno afferente a profili microprudenziali relativi alla regolamentazione a livello delle singole banche; l'altro avente ad oggetto profili macroprudenziali, riguardanti i rischi a livello di sistema che possono stratificarsi nel settore bancario, tutto ciò senza trascurare l'amplificazione prociclica di questi rischi nel tempo.

Come evidenziato sopra, nel recepimento del pacchetto CRR-CRD IV vi sono ambiti lasciati alla discrezionalità delle autorità di vigilanza nazionali. Dal confronto con il documento di consultazione pubblicato nell'agosto 2013 e dall'applicazione in Italia del reg. UE n. 575/2013 e della dir. 2013/36/UE emerge che la Banca d'Italia ha esercitato discrezionalità in materia di partecipazioni assicurative, di esposizioni infragruppo, di disposizioni transitorie per le banche che utilizzano i sistemi IRB o i metodi AMA (floor), di concentrazione dei rischi, di disciplina della liquidità applicabile a livello individuale (waiver), di ponderazione del rischio e proibizione delle partecipazioni qualificate al di fuori del settore finanziario.

Sul piano delle fonti della vigilanza prudenziale a livello nazionale, emergono, dalla breve disamina svolta, aree di sovrapposizione delle nuove regole rispetto alle precedenti circolari, che hanno alimentato non poche incertezze applicative. Mentre in ambito comunitario la vecchia normativa, contenuta nelle direttive 2006/48/CE e 2006/49/CE, viene interamente abrogata con l'emanazione del pacchetto CRR-CRD IV, in Italia l'entrata in vigore della nuova circolare 285/13 non coincide con

l'abrogazione dei precedenti riferimenti normativi. Rimangono tuttora in vigore, ad eccezione di alcune parti, la circolare n. 263/2006 e n. 229/1999[61].

Tra le fonti normative che disciplinano la materia del processo di controllo prudenziale, di fondamentale importanza è il Testo unico delle leggi in materia bancaria e creditizia – TUB (Decreto legislativo 1° settembre 1993 n. 385)[62]. In questa sede, si ritiene opportuno limitarsi a richiamare, seppure brevemente, quelle disposizioni più direttamente riferibili alla materia della vigilanza bancaria. Il legislatore del TUB, all'art. 53, comma 1 prevede che: "*La Banca d'Italia emana disposizioni di carattere generale aventi a oggetto:*

a) l'adeguatezza patrimoniale;

b) il contenimento del rischio nelle sue diverse configurazioni;

c) le partecipazioni detenibili;

d) il governo societario, l'organizzazione amministrativa e contabile, nonché i controlli interni e i sistemi di remunerazione e di incentivazione;

d-bis) l'informativa da rendere al pubblico sulle materie di cui alle lettere da a) a d)".

In sintesi, in questa disposizione il legislatore attribuisce alla Banca d'Italia, in conformità delle deliberazioni del CICR, il potere di emanare disposizioni di carattere generale aventi a oggetto l'adeguatezza patrimoniale, il contenimento del rischio nelle sue diverse configurazioni e l'organizzazione amministrativa e contabile e i controlli interni. Il comma 2- bis, in relazione alle disposizioni riguardanti l'adeguatezza patrimoniale di cui alla lett. a del primo comma, prevede che: "*Le disposizioni emanate ai sensi del comma 1, lettera a), prevedono che le banche possano utilizzare:*

a) le valutazioni del rischio di credito rilasciate da società o enti esterni; le disposizioni disciplinano i requisiti, anche di competenza tecnica e di indipendenza, che tali soggetti devono possedere e le relative modalità di accertamento;

b) sistemi interni di misurazione dei rischi per la determinazione dei requisiti patrimoniali, previa autorizzazione della Banca d'Italia. Per le banche sottoposte alla vigilanza consolidata di un'autorità di un altro Stato comunitario, la decisione è di competenza della medesima autorità, qualora, entro sei mesi dalla presentazione della domanda di autorizzazione, non venga adottata una decisione congiunta con la Banca d'Italia e sempre che, entro il medesimo termine, il caso non sia

[61] Le disposizioni in materia di autorizzazione all'attività bancaria erano inizialmente contenute nel Titolo I, Capitolo 1 della circolare 229/1999; nel 2013, a seguito di un aggiornamento della disciplina, è stato abrogato il Titolo 1, Cap. 1, della Circolare 229 e le nuove norme in materia di autorizzazione all'attività bancaria sono state inserite nella Circolare 263/2006 (Titolo 1, Capitolo3).Infine, l'entrata in vigore della circolare 285/2013 ha abrogato, anche se solo in parte, le norme contenute nella circolare 263/2006.

[62] Testo Unico delle leggi in materia bancaria e creditizia, d.lgs n. 385 del 1° settembre 1993, aggiornato da ultimo dal D.l n. 22 del 25 marzo 2019 convertito, con modificazioni, dalla legge n. 41 del 20 maggio 2019.

stato rinviato all'ABE ai fini della procedura per la risoluzione delle controversie con le autorità di vigilanza degli altri Stati membri in situazioni transfrontaliere".

L'art. 65 definisce i soggetti inclusi nell'ambito della vigilanza consolidata, identificandoli nelle:

"*a) società appartenenti a un gruppo bancario;*

b) società bancarie, finanziarie e strumentali partecipate almeno per il 20% dalle società appartenenti a un gruppo bancario o da una singola banca;

c) società bancarie, finanziarie e strumentali non comprese in un gruppo bancario, ma controllate dalla persona fisica o giuridica che controlla un gruppo bancario ovvero una singola banca;

d) (soppressa)

e) (soppressa)

f) (soppressa)

g) (soppressa)

h) società che controllano almeno una banca;

i) società diverse da quelle bancarie, finanziarie e strumentali quando siano controllate da una singola banca ovvero quando società appartenenti a un gruppo bancario ovvero soggetti indicati nella lettera h) detengano, anche congiuntamente, una partecipazione di controllo"[63].

Di fondamentale importanza sono poi le disposizioni dell'art. 67, il quale, al primo comma, lett. a), b) e d), al fine di realizzare la vigilanza consolidata, prevede che la Banca d'Italia, in conformità alle deliberazioni del CICR, impartisca alla capogruppo o a componenti del gruppo bancario, con provvedimenti di carattere generale o particolare, disposizioni aventi a oggetto l'adeguatezza patrimoniale, il contenimento del rischio nelle sue diverse configurazioni e l'organizzazione amministrativa e contabile e i controlli interni. Il terzo comma prevede che: "*Le disposizioni emanate dalla Banca d'Italia per esercitare la vigilanza su base consolidata possono tenere conto, anche con riferimento alla singola banca, della situazione e delle attività dei soggetti indicati nelle lettere b) e c) del comma 1 dell'articolo 65*". In altre parole, questo comma stabilisce che le disposizioni emanate dalla Banca d'Italia per realizzare la vigilanza consolidata possono tenere conto, anche con riferimento alla singola banca, della situazione e delle attività delle società bancarie, finanziarie e strumentali partecipate almeno per il 20% dalle società appartenenti a un gruppo bancario o da una singola banca, nonché delle società bancarie, finanziarie e strumentali non comprese in un gruppo bancario ma controllate dalla persona fisica o giuridica che controlla un gruppo bancario ovvero una singola banca.

[63] Le lettere *d, e, f, g* sono state soppresse dall'art. 1, comma 1, lett. f), n. 1, D.L. 27 dicembre 2006, n. 297, convertito, con modificazioni, dalla L. 23 febbraio 2007, n. 15.

Di particolare rilevanza è anche l'art. 69, commi 1 e 1- bis, secondo cui: "*Al fine di agevolare l'esercizio della vigilanza su base consolidata nei confronti di gruppi operanti in più Stati comunitari la Banca d'Italia, sulla base di accordi con le autorità competenti, definisce forme di collaborazione e coordinamento, istituisce collegi di supervisori e partecipa ai collegi istituiti da altre autorità. In tale ambito, la Banca d'Italia può concordare specifiche ripartizioni di compiti e deleghe di funzioni.*
1-bis. Per effetto degli accordi di cui al comma 1, la Banca d'Italia può esercitare la vigilanza consolidata anche:
a) sulle società finanziarie e sulle società di partecipazione finanziaria mista, aventi sede legale in un altro Stato comunitario, che controllano una capogruppo o una singola banca italiana;
b) sulle società bancarie, finanziarie e strumentali controllate dai soggetti di cui alla lettera a);
c) sulle società bancarie, finanziarie e strumentali partecipate almeno per il venti per cento, anche congiuntamente, dai soggetti indicati nelle lettere a) e b)".
In queste disposizioni si mette in luce l'importanza di forme di collaborazione e di coordinamento nonché della ripartizione dei compiti specifici di ciascuna autorità in ordine all'esercizio della vigilanza consolidata nei confronti di gruppi operanti in più Paesi e si individuano i soggetti sui quali viene esercitata la vigilanza consolidata.

2. Il Supervisory Review Process

L'obiettivo dell'implementazione di un sistema di vigilanza prudenziale uniforme per tutte le banche europee rientra nel più ampio progetto riguardante la creazione dell'Unione Bancaria avviata a partire dal 2012. Il tema della vigilanza, infatti, costituisce proprio uno dei pilastri su cui si fonda l'Unione Bancaria, quello del Single Supervisory Mechanism (SSM) o Meccanismo di Vigilanza Unico (MVU)[64]. Il SSM entra in vigore nel 2014 al fine di assicurare l'uniformità e la coerenza delle regole di vigilanza applicate dalle banche europee e di garantire l'efficacia e la qualità della vigilanza stessa, come si evince nel report prodotto in esito ai lavori del gruppo "*de Larosière*" del Febbraio 2009[65]. Il sistema opera attraverso la cooperazione tra la Banca Centrale Europea (BCE) e le Autorità Nazionali Competenti (ANC) degli stati membri, sfruttando la visione di più ampio raggio della BCE in materia di stabilità macroeconomica e finanziaria e le conoscenze più specifiche delle ANC riguardo alle giurisdizioni degli stati di appartenenza[66].

---

[64]L' Unione bancaria viene fondata su tre pilastri: il meccanismo di vigilanza unico, il meccanismo di risoluzione unico e lo schema di garanzia dei depositi.
[65]Il gruppo "de Larosière" nasce nell'ottobre 2008 su indicazione dell'allora Presidente della Commissione Europea Barroso, il quale conferì a Jacques de Larosière, ex governatore della Banca Centrale Francese e capo del Fondo Monetario Internazionale, il mandato di costituire un gruppo di studiosi con il compito di formulare un parere in merito al futuro della regolamentazione e della vigilanza prudenziale del sistema finanziario europeo.
[66] Cfr. Banca Centrale Europea, "Manuale di vigilanza dell'MVU. Vigilanza bancaria europea: funzionamento dell'MVU e approccio di vigilanza" in www.bankingsupervision.europa.eu.

La divisione dei compiti si basa sulla significatività degli enti vigilati. Come si vedrà più nel dettaglio in seguito, gli enti ritenuti significativi sono sottoposti alla vigilanza diretta della BCE, mentre quelli meno significativi sono soggetti alle attività di vigilanza delle ANC, sempre sotto la supervisione della BCE[67].

L'attività di vigilanza deve essere svolta nel rispetto dei principi previsti nella "Guida alla vigilanza bancaria" pubblicata nel 2014 sul sito internet della BCE[68]. Tali principi, che rappresentano il fondamento dell'intero Meccanismo di Vigilanza Unico, sono:

- Principio 1- Impiego delle migliori prassi

  Il Meccanismo di Vigilanza Unico deve basarsi su prassi e processi sottoposti a continui aggiornamenti e revisioni, anche tenendo conto delle specificità dei singoli stati membri, al fine di consentire la costante e tempestiva individuazione di aree da correggere o migliorare.

- Principio 2 - Integrità e decentramento

  L'obiettivo di ogni partecipante all'MVU è quello di perseguire risultati di elevata qualità in materia di vigilanza. Conseguentemente, è fondamentale per l'MVU far leva su processi e procedure accentrate e su informazioni qualitative approfondite e coerenti e, naturalmente, su una conoscenza consolidata degli enti creditizi. Nel contempo, i processi di decentramento, facilitando lo scambio costante di informazioni tra la BCE e le ANC, consentono di salvaguardare da un lato l'unità del sistema di vigilanza evitando la duplicazione di attività, dall'altro di avvantaggiarsi della prossimità delle autorità di vigilanza nazionali agli enti creditizi vigilati.

- Principio 3 - Omogeneità nell'ambito dell'MVU

  Per consentire che le azioni di vigilanza siano applicate in maniera coerente, tutti gli enti creditizi degli Stati membri partecipanti, sono destinatari dei principi e delle procedure di vigilanza, il che consente di evitare disparità di trattamento e frammentazione. Questo, in buona sostanza, è il principio a fondamento dell'MVU quale sistema di vigilanza unico. L'applicazione di questo principio è strettamente correlata al principio di proporzionalità (cfr. principio 7).

[67]I criteri per stabilire la significatività di un ente sono previsti nel regolamento sull'SSM (Regolamento UE N. 1024/2013) e il regolamento quadro sull'SSM (Regolamento BCE/2014/17).

[68]Banca Centrale Europea, "Guida alla vigilanza bancaria" in www.bankingsupervision.europa.eu.

- Principio 4 - Coerenza con il mercato unico

  L'MVU, in quanto conforme al corpus unico di norme, integra la vigilanza in molte giurisdizioni e favorisce l'ulteriore sviluppo del corpus unico di norme da parte dell'ABE, così da consentire di affrontare meglio i rischi sistemici in Europa. Prendono parte all'MVU tutti gli Stati membri dell'UE la cui moneta non è l'euro e che possono instaurare una cooperazione stretta. Tenuto conto della sua centralità nell'ambito dell'MVU, la BCE rafforza ulteriormente il processo di convergenza nel mercato unico anche in relazione ai compiti di vigilanza a essa conferiti dal regolamento sull'MVU.

- Principio 5 - Indipendenza e responsabilità

  I compiti di vigilanza vengono esercitati in modo indipendente. Tuttavia, proprio per garantire agli Stati membri partecipanti la massima fiducia nell'esercizio della propria funzione pubblica, la vigilanza è anche soggetta a elevati standard di responsabilità democratica e, in linea con il regolamento sull'MVU, vi sarà responsabilità democratica a livello sia europeo sia nazionale.

- Principio 6 - Approccio basato sul rischio

  L'approccio dell'MVU alla vigilanza si fonda sull'analisi del rischio, tenendo nella dovuta considerazione da un lato l'entità dei danni che il fallimento di un ente potrebbe arrecare alla stabilità finanziaria, dall'altro la possibilità che tale fallimento si verifichi. Se taluni enti creditizi, o gruppo di essi, vengono ritenuti a rischio più elevato rispetto ad altri, l'MVU procede a sottoporli ad una vigilanza più intensa finché i rischi pertinenti non diminuiscano e non raggiungano un livello accettabile. In questo senso l'attività di vigilanza dell'MVU, fondata su approcci qualitativi e quantitativi, comporta sempre giudizi e valutazioni critiche prospettiche. Tale tipo di approccio, fondato per l'appunto sul rischio, garantisce che le risorse destinate alla vigilanza siano sempre orientate ai settori rispetto ai quali ci sia la possibilità di risultare più efficaci nel miglioramento della stabilità finanziaria.

- Principio 7 - Proporzionalità

  In ragione dell'importanza sistemica e del rischio degli enti creditizi da vigilare, l'MVU orienta le proprie prassi di vigilanza secondo il principio di proporzionalità, principio che consente di ripartire in modo efficiente risorse di vigilanza limitate. Conseguentemente, la profondità di vigilanza dell'MVU sugli enti creditizi varia, per essere maggiormente attenta nei confronti dei gruppi sistemici più grandi e più complessi e delle filiali più rilevanti

all'interno di un gruppo bancario significativo. La natura e l'ampiezza delle attività di vigilanza si adatta alle caratteristiche, alle dimensioni e alla complessità dell'ente oggetto di vigilanza. Questo principio è coerente con un approccio di vigilanza consolidato e basato sul rischio dell'MVU.

- Principio 8 - Livelli adeguati di vigilanza per tutti gli enti creditizi
  L'MVU assicura livelli minimi di vigilanza per tutti gli enti creditizi e garantisce un adeguato livello di impegno con tutti gli enti significativi, indipendentemente dal rischio di fallimento percepito. Classifica gli enti creditizi in base all'impatto del loro fallimento sulla stabilità finanziaria e stabilisce un livello minimo di impegno per ciascuna categoria.

- Principio 9 - Misure correttive efficaci e tempestive
  L'obiettivo operativo dell'MVU è quello di salvaguardare sicurezza e solidità di ogni ente creditizio e la stabilità del sistema finanziario europeo e dei sistemi finanziari degli Stati membri partecipanti. Vigila in modalità proattiva sugli enti creditizi negli Stati membri partecipanti per arginare danni potenziali e probabilità di fallimento, con particolare riguardo alla riduzione del rischio di fallimento di enti significativi. Nell'ambito di questo principio è molto importante la correlazione tra la valutazione e la misura correttiva, perciò è fondamentale promuovere un'azione di vigilanza tempestiva e un monitoraggio approfondito della risposta di un ente creditizio. Proprio in quest'ottica, le autorità di vigilanza devono intervenire repentinamente, riducendo così le potenziali perdite per i creditori dell'ente creditizio (depositanti inclusi).
  La collaborazione dell'MVU con le altre autorità di vigilanza assicura la possibilità di sfruttare completamente i meccanismi di risoluzione disponibili, conformemente al diritto nazionale e dell'UE. Nelle ipotesi di fallimento, si ricorre alle procedure di risoluzione ai sensi della direttiva sul risanamento e la risoluzione delle banche per impedire il verificarsi di rilevanti effetti avversi sul sistema finanziario e per tutelare i fondi pubblici, così minimizzando il ricorso al sostegno finanziario pubblico straordinario.

I principi sopra richiamati si riflettono negli obiettivi che il Meccanismo di Vigilanza Unico si propone di perseguire. Come anticipato, l'MVU nasce con l'intento di assicurare la stabilità finanziaria e l'armonizzazione delle misure di vigilanza negli stati membri. In tale ottica, un obiettivo fondamentale è rappresentato dalla riformulazione dell'architettura e dell'organizzazione delle attività e degli organismi di vigilanza a livello sia europeo sia dei singoli stati. Inoltre, una

supervisione accentrata consente di conseguire due ulteriori risultati fondamentali: da un lato, permette di recuperare la fiducia verso le autorità nazionali da parte degli investitori, i quali possono confidare nell'uniformità delle procedure in tutto il territorio comunitario; dall'altro lato, consente di ridurre le divergenze tra i vari ordinamenti così da prevenire le situazioni di arbitraggio normativo, in cui si decide di approfittare del regime di vigilanza di un dato paese perché meno rigido di altri. Infine, il Meccanismo di Vigilanza Unico si pone come ulteriore obiettivo la creazione di un contesto sistemico in cui vengano ridotte al minimo le pressioni locali a favore di una supervisione efficace ed indipendente che operi in un'ottica sovranazionale.

Nell'ambito del Meccanismo Unico di Vigilanza viene definito anche il processo di controllo prudenziale, conosciuto come *Supervisory Review Process* (SRP). Il SRP prevede due fasi tra loro integrate: la prima coinvolge le banche ed è costituita dal processo interno di determinazione dell'adeguatezza patrimoniale (*Internal Capital Adequacy Assessment Process* – ICAAP) e dal processo interno di valutazione della liquidità (*Internal Liquidity Adequacy Assessment* – ILAAP); la seconda fase consiste nel processo di revisione e valutazione prudenziale (Supervisory Review and Evaluation Process – SREP) che fa capo alle Autorità di vigilanza[69]. In particolare, questa seconda fase è di competenza della Banca Centrale Europea per le banche "*significant*" e delle Autorità di vigilanza nazionali per le banche "*less significant*". Per stabilire se una banca è da considerare "*significant*", e in quanto tale sottoposta alla vigilanza diretta della BCE, occorre fare riferimento ai criteri previsti nel regolamento sull'MVU e nel regolamento quadro sull'MVU. Una banca è significativa se presenta almeno uno dei seguenti requisiti[70]:

- Dimensioni: il valore totale delle sue attività supera i 30 miliardi di euro;
- Importanza economica: relativa ad un paese particolare o per l'economia dell'Unione europea nel suo insieme;
- Operatività transfrontaliera: il valore totale delle sue attività supera i 5 miliardi di euro e il rapporto tra le attività transfrontaliere in più di un altro Stato membro partecipante e le attività totali è superiore al 20% o il rapporto tra le passività transfrontaliere in più di un altro Stato membro partecipante e le passività totali è superiore al 20%;
- Assistenza finanziaria pubblica diretta: ha ricevuto o anche solo richiesto finanziamenti nel quadro del Meccanismo europeo di stabilità o della European Financial Stability Facility.

Ogni banca può subire una riclassificazione in seguito a normali attività operative o ad operazioni straordinarie come fusioni e acquisizioni; in tal caso, deve avvenire il trasferimento delle competenze

[69] Cfr. Banca d'Itala, *Disposizioni di vigilanza per le banche – Processo di controllo prudenziale*, Titolo III, Capitolo I.
[70] Cfr. Banca Centrale Europea, sito web della Vigilanza Bancaria in Supervisory practices.

alla rispettiva autorità di vigilanza. Le banche *less significant* sono quelle che non rientrano nella definizione prevista dai regolamenti sul Meccanismo di Vigilanza Unico.

2.1 Prima fase: i processi ICAAP e ILAAP

Le banche devono predisporre strategie e procedure idonee a determinare livelli di capitale e di liquidità adeguati per la copertura di tutti i rischi ai quali sono esposte. I processi ICAAP e ILAAP devono essere formalizzati, documentati e condivisi dalle strutture aziendali. In particolare, devono essere approvati e sottoposti a revisione interna e, infine, trasmessi alle autorità di vigilanza. La responsabilità di questi processi ricade, dunque, sugli organi societari (organo di amministrazione, organo di controllo e funzioni di *compliance*, risk management e internal audit).

Il processo ICAAP (*Internal Capital Adequacy Assessment Process*) è il processo attraverso il quale la banca effettua la valutazione circa l'adeguatezza patrimoniale ai sensi dell'art. 73 della Direttiva CRD IV[71].

La responsabilità di tale processo è rimessa agli organi societari. In particolare, l'ICAAP rappresenta parte integrante della gestione aziendale e della definizione delle strategie ed è, inoltre, sottoposto a revisione interna, coinvolgendo in tal modo gran parte degli organi della banca. Sulla base delle proprie caratteristiche, ogni banca individua nello specifico gli organi cui compete l'elaborazione delle varie fasi del processo[72].

A seguito di una valutazione complessiva relativa a tutti i fattori di rischio verificabili, l'ente deve definire in autonomia un processo in grado di mitigare tali rischi. La predisposizione del processo ICAAP deve avvenire nel rispetto del principio di proporzionalità in relazione alle metodologie utilizzate, agli stress test applicati, alla struttura dei sistemi di controllo, all'estensione della rendicontazione diretta alla Banca d'Italia. Affinché venga effettivamente applicato il principio di proporzionalità, le banche sono raggruppate in tre classi in base alle dimensioni e alla complessità operativa[73]. La "Classe 1" raggruppa le banche e i gruppi che utilizzano sistemi IRB per il calcolo dei requisiti a fronte del rischio di credito, il metodo AMA per il calcolo dei requisiti a fronte del rischio operativo o modelli interni per i requisiti sui rischi di mercato. Della "Classe 2" fanno parte le banche o i gruppi che si servono di metodologie standardizzate con attivo, individuale per le banche o consolidato per i gruppi, superiore a 3,5 miliardi di euro. La "Classe 3" ricomprende le banche o i gruppi che utilizzano metodologie standardizzate, con attivo, individuale per le banche o consolidato per i gruppi, uguale o inferiore a 3,5 miliardi di euro.

---

[71] Banca Centrale Europea, Vigilanza Bancaria, Guida della BCE sul processo interno di valutazione dell'adeguatezza del capitale (ICAAP).

[72] Banca d'Italia, *Nuove disposizioni di vigilanza prudenziale per le banche*, Titolo 1, Capitolo 1, Parte Quarta.

[73] Banca Centrale Europea, sito web della Vigilanza Bancaria in Supervisory practices – SREP methodology.

Il processo ICAAP è costituito da più fasi[74]:

1) Individuazione dei rischi oggetto di valutazione

In base alla propria operatività e al mercato in cui opera, la banca deve identificare i rischi cui è esposta. L'ente non deve intervenire solo sui rischi, ma deve operare a monte individuando le cause di tali rischi sia a livello dell'entità giuridica sia a livello di singola unità operativa. In tal modo, è possibile verificare se il requisito patrimoniale individuato a livello individuale sia sufficiente a limitare i rischi dell'intera entità.

2) Misurazione dei singoli rischi e del relativo capitale interno

Le metodologie da utilizzare dipendono dai rischi presi in considerazione. I rischi di credito, di controparte, di mercato ed operativi vanno misurati attraverso le metodologie individuate dai relativi sistemi regolamentari per il calcolo dei requisiti patrimoniali. Specifiche metodologie semplificate sono, invece, previste per la valutazione del rischio di concentrazione e di tasso d'interesse e per la misurazione dell'eventuale capitale interno.

Per il rischio di tasso d'interesse, è richiesto a tutte le banche di applicare una variazione ipotetica dei tassi pari a +/- 200 punti base sull'esposizione a tale rischio relativo al portafoglio bancario al fine di misurare l'impatto di tale valutazione. Se questo impatto si traduce in una riduzione del valore economico della banca superiore al 20% del patrimonio di vigilanza, la Banca d'Italia esamina con la banca interessata tali risultati e, se necessario, adotta le misure più opportune.

I criteri da utilizzare per la misurazione dei rischi rilevanti e per la determinazione dell'eventuale capitale interno differiscono in base alla classe di appartenenza. Con riferimento alle banche della Classe 3, i rischi compresi nel Primo Pilastro vengono calcolati con le metodologie di calcolo dei requisiti patrimoniali (i rischi di credito e di mercato sono calcolati con il metodo standardizzato, mentre quelli operativi con il metodo di base o standardizzato). Le banche possono applicare metodi semplificati per i rischi non inclusi nel Primo Pilastro, in particolare, per il rischio di concentrazione, il rischio di tasso d'interesse e gli altri rischi eventualmente individuati.

Anche le banche della Classe 2 possono applicare le metodologie previste per il calcolo dei requisiti patrimoniali regolamentari per i rischi di Primo Pilastro, ma possono anche decidere di adottare metodi più evoluti. Allo stesso modo, per i rischi non ricompresi nel Primo Pilastro, possono decidere di affinare gli algoritmi semplificati.

[74]Banca Centrale Europea, Vigilanza Bancaria, Guida della BCE sul processo interno di valutazione dell'adeguatezza del capitale (ICAAP) già citata.

Le banche appartenenti alla Classe 1 possono definire in piena autonomia le metodologie da utilizzare, sviluppando modelli statistici più evoluti rispetto alle metodologie semplificate, anche di tipo sperimentale, da affinare nel tempo.

Uno strumento con cui le banche possono valutare l'esposizione ai rischi e l'adeguatezza dei sistemi di controllo e del capitale interno è lo stress test[75]. Questi test possono consistere nel valutare gli effetti sui rischi della banca di eventi specifici (analisi di sensibilità) o di variazioni congiunte di variabili economico-finanzairie in ipotesi di scenari avversi (analisi di scenario). La conduzione di queste analisi consente di misurare l'esposizione al rischio in circostanze avverse e di determinare il capitale interno e gli altri interventi necessari per coprire tale rischio, ma anche di verificare l'accuratezza dei modelli di valutazione dei rischi utilizzati.

Le banche della Classe 3 devono effettuare gli stress test per i principali rischi individuati, tra i quali almeno il rischio di credito, il rischio di concentrazione del portafoglio crediti e il rischio di tasso d'interesse.

Le banche di Classe 2 svolgono le analisi di sensibilità solo con riferimento a fattori di rischio autonomamente individuati.

Le banche ricomprese nella Classe 1 utilizzano una combinazione delle tecniche di analisi di sensibilità e analisi di scenario.

3) Misurazione del capitale interno complessivo

In questa fase le banche devono valutare i benefici derivanti dalla diversificazione tra i diversi tipi di rischio. Anche per questa valutazione i criteri previsti dipendono dalla classe di appartenenza. Per le banche di Classe 2 e 3 il capitale interno complessivo è determinato attraverso un approccio semplificato che consiste nel sommare ai requisiti regolamentare per i rischi di Primo Pilastro l'eventuale capitale interno relativo agli altri rischi rilevanti.

Le banche di Classe 1 possono adottare soluzioni più avanzate, ma hanno l'obbligo di documentare e motivare la scelta di metodologie diverse da quelle regolamentari.

Tutte le banche, a prescindere dalla classe di appartenenza, nella determinazione del capitale interno complessivo devono tener conto, oltre che della necessità di copertura delle perdite dovute a tutti i rischi inattesi, anche dell'esigenza di far fronte a operazioni di carattere strategico.

4) Determinazione del capitale complessivo e riconciliazione con il patrimonio di vigilanza

Il capitale interno deve convivere con il patrimonio di vigilanza; ciò significa che le banche devono illustrare e spiegare l'utilizzo di strumenti patrimoniali a copertura del capitale interno complessivo e non computabili nel patrimonio di vigilanza.

[75] Banca Centrale Europea, sito web della Vigilanza Bancaria in Supervisory practices – SREP methodology.

Il processo ICAAP ha una periodicità annuale. Infatti, le banche devono determinare, con cadenza annuale, il livello attuale del capitale interno complessivo e del capitale complessivo calcolato con riferimento alla fine dell'ultimo esercizio chiuso e il livello prospettico del capitale interno complessivo. Questa pianificazione annuale deve avere ad oggetto anche l'individuazione di misure correttive per l'eventualità di errori o scostamenti dalle stime. In ogni caso, la valutazione dei singoli rischi può avvenire con frequenza più ravvicinata.

Le banche devono fornire alla Banca Centrale Europea e alla Banca d'Italia l'informativa relativa all'ICAAP in modo tale che queste possano effettuare una valutazione documentata e completa delle caratteristiche fondamentali. Il resoconto deve avere ad oggetto una parte descrittiva in cui la banca deve descrivere i processi di determinazione del capitale interno e di misurazione dei rischi e una parte di auto-valutazione in cui la banca valuta l'adeguatezza del proprio processo interno. La rendicontazione riferibile al 31 dicembre dell'anno precedente va trasmessa annualmente, entro il 30 aprile.

Il processo ILAAP (*Internal Liquidity Adequacy Assessment Process*) è il processo interno di valutazione della liquidità predisposto dalle banche secondo quanto previsto dall'art. 86 della Direttiva CRD IV. Questo processo ha ad oggetto l'adeguatezza del sistema di governo e di gestione del rischio di liquidità ed ha l'obiettivo di mantenere il rischio di liquidità ad un livello accettabile e, in tal modo, garantire la sopravvivenza della banca[76]. Il processo ILAAP deve prevedere la determinazione del livello di rischio considerato accettabile e la descrizione delle metodologie e dei criteri utilizzati per la misurazione del rischio e la conduzione degli stress test. Come per l'ICAAP, anche in questo caso la banca deve compiere un'auto-valutazione e dare un giudizio sull'adeguatezza della liquidità attuale e prospettica e sulla sua capacità di gestire il rischio di liquidità. I concetti di liquidità su cui si basa l'ILAAP sono quelli di:

- *counterbalancing capacity*: capacità di scongiurare il rischio di liquidità grazie al ricorso alle riserve di liquidità e alle altre attività prontamente liquidabili necessarie per fronteggiare le esigenze di liquidità future, anche in situazione di stress;
- *liquidity buffer*: liquidità disponibile in eccesso, costituita da saldi liquidi (cassa) o attività finanziarie prontamente liquidabili, da utilizzare per esigenze di liquidità dovute a condizioni di stress verificatesi in un dato orizzonte temporale;
- *survival period*: periodo di tempo in cui la banca non necessita di liquidità aggiuntiva e in cui riesce a rispettare tutte le scadenze di pagamenti anche se versa in una situazione di stress.

[76]Banca Centrale Europea, Vigilanza Bancaria, Guida della BCE sul processo interno di valutazione dell'adeguatezza della liquidità (ILAAP).

La metodologia consiste nel prendere in considerazione tutti i fattori di rischio, attuali e futuri, e nel verificare l'impatto su tali rischi di variazioni delle condizioni attraverso l'utilizzo di stress test (analisi di sensibilità e analisi di scenario). Sulla base dei rischi individuati, le banche devono determinare delle azioni di mitigazione, come, per esempio, stabilire un determinato ammontare delle riserve di liquidità sulla base della soglia di tolleranza del rischio che è stata fissata o prevedere dei limiti operativi che impediscano l'assunzione di posizioni eccedenti i limiti prefissati o, ancora, attuare una diversificazione delle fonti di finanziamento per limitarne la concentrazione. La banca deve integrare queste attività negli altri processi interni, coinvolgendo il risk management, il sistema dei controlli, l'audit (essendo l'ILAAP sottoposto a revisione interna).
Poiché può considerarsi l'equivalente dell'ICAAP in ambito liquidità, al processo ILAAP si applicano le disposizioni previste per il processo ICAAP in materia di principio di proporzionalità, di fasi di svolgimento, di differenziazione delle banche in classi e di rendicontazione alla Banca Centrale Europea e alla Banca d'Italia.

2.2 Seconda fase: Supervisory Review and Evaluation Process (SREP)

Il *Supervisory Review and Evaluation Process* è svolto dalle Autorità di vigilanza per misurare e valutare i rischi e i presidi patrimoniali adottati dalle banche, in modo da poter indicare a quest'ultime le azioni più adeguate da intraprendere. In sostanza, tale processo fotografa la situazione dell'intermediario in relazione ai requisiti patrimoniali e alla gestione dei rischi e, a conclusione del processo, attraverso la decisione SREP che l'Autorità di vigilanza invia alla banca, vengono evidenziate le criticità emerse e definiti gli obiettivi fondamentali per affrontarle. La banca, nei tempi individuati, deve apportare gli opportuni interventi correttivi[77].
Lo SREP sviluppa, dunque, un sistema di monitoraggio costante dei rischi degli istituti creditizi vigilati, dei relativi sistemi di *Risk Management* e delle strutture di *corporate governance*, sempre nel rispetto dei requisiti patrimoniali prudenziali.
Tale attività di supervisione prudenziale viene esercitata nell'intero ambito comunitario su enti di qualsiasi rilevanza e nazione, con il proposito di assicurare un sistema coerente di vigilanza, sebbene sempre nel rispetto del principio di proporzionalità. Sulla base di questo principio, la natura e l'entità della vigilanza devono essere adattate alla dimensione, alle caratteristiche e ai profili di criticità della singola banca.
In tale scenario, le autorità competenti, BCE e ANC , ai sensi dell' art. 97, par.1, della direttiva CRD IV "*riesaminano i dispositivi, le strategie, i processi e i meccanismi messi in atto dagli enti per conformarsi alla presente direttiva e al regolamento (UE) n. 575/2013 e valutano: a) i rischi ai quali*

[77] Banca Centrale Europea, sito web della Vigilanza Bancaria in Supervisory practices – SREP methodology.

gli enti sono o possono essere esposti; b) i rischi che un ente pone al sistema finanziario, tenendo conto dell'individuazione e della misurazione del rischio sistemico di cui all'articolo 23 del regolamento (UE) n. 1093/2010 o, se del caso, delle raccomandazioni del CERS; e c) i rischi rivelati dalle prove di stress, tenendo conto della natura, dell'ampiezza e della complessità delle attività dell'ente[78]".

Questa disposizione individua gli strumenti fondamentali attraverso i quali lo SREP valuta l'andamento della gestione condotta dagli enti, anche in considerazione dell'adeguatezza della copertura dei rischi cui sono esposti.

Per quanto riguarda l'individuazione dei criteri tecnici da seguire, il successivo art. 98 della citata direttiva CRD IV, prevede che la valutazione e la revisione abbiano ad oggetto, oltre ai rischi di credito, di mercato e operativo: "*a) i risultati delle prove di stress effettuate in base ai principi dettati dall'articolo 177 del regolamento (UE) n. 575/2013 dagli enti che applicano il metodo basato sui rating interni; b) l'esposizione al rischio di concentrazione degli enti e la relativa gestione, ...; c) la solidità, l'appropriatezza e l'applicazione delle politiche e delle procedure attuate dagli enti per la gestione del rischio residuale associato all'uso di tecniche riconosciute di attenuazione del rischio di credito; d) la misura in cui i fondi propri detenuti dall'ente a fronte delle attività che ha cartolarizzato siano adeguati al contenuto economico dell'operazione, considerata anche l'entità del rischio trasferito; e) l'esposizione al rischio di liquidità e la sua misurazione e gestione da parte degli enti, compresa l'elaborazione di analisi di scenari alternativi, la gestione dei fattori di attenuazione del rischio (in particolare il livello, la composizione e la qualità delle riserve di liquidità) e di piani di emergenza efficaci; f) l'impatto degli effetti di diversificazione e il modo in cui detti effetti sono presi in considerazione nel sistema di misurazione del rischio; g) i risultati delle prove di stress effettuate dagli enti che utilizzano un modello interno per calcolare i requisiti in materia di fondi propri a fronte del rischio di mercato di cui alla parte tre, titolo IV, capo 5, del regolamento (UE) n. 575/2013; h) la localizzazione geografica delle esposizioni dell'ente; i) il modello imprenditoriale dell'ente; j) la valutazione del rischio sistemico, in conformità ai criteri fissati all'articolo 97*"[79].

Si delineano in questo modo i tre elementi imprescindibili sui quali redigere lo SREP:

- un sistema di analisi dei rischi, ulteriori rispetto ai rischi di credito, di mercato e operativo idoneo a valutarne i livelli, *Risk Assessment System* – RAS-;
- una revisione dei processi interni di valutazione dell'adeguatezza patrimoniale e della liquidità (ICAAP e ILAAP) per ottenere una valutazione circa la bontà delle quantificazioni effettuate da ciascun istituto;

[78] Direttiva 2013/36/UE, art. 97, par. 1 in www. eur-lex.europa.eu.
[79] Direttiva 2013/36/UE, art. 98, par. 1 in www. eur-lex.europa.eu.

- una metodologia di quantificazione prudenziale di livelli di capitale e di liquidità che soddisfino il fabbisogno degli istututi, tenuto conto dei risultati della valutazione dei rischi.

Per quanto riguarda il *Risk Assessment System*, lo SREP consente di valutare lo stato di salute delle banche, misurandone i profili di rischi secondo quattro diverse angolazioni.
Il ricorso a questi quattro profili consente di garantire una parità di condizioni per tutte le banche e di fornire ai responsabili della vigilanza uno strumentario armonizzato che agevola nell'esame dei profili di rischio delle banche[80].
Le quattro dimensioni considerate nello SREP sono:
1) Modello imprenditoriale
Le autorità di vigilanza valutano la sostenibilità dell'assetto imprenditoriale delle singole banche, per individuare le specifiche aree di operatività, i relativi rischi da gestire e i profili di criticità che potrebbero intervenire negativamente sulla capacità dell'ente di generare crescita e utili.
L'analisi del modello imprenditoriale o *business model analysis* (BMA) può essere svolta sull'intero ente oppure su un singolo *business* o prodotto. La BMA va condotta regolarmente e ha come obiettivo, oltre a quello di individuare i rischi connessi al modello imprenditoriale o alla strategia, quello di determinare l'andamento del *business* anche in un'ottica prospettica sulla base della previsione dei profitti nei futuri 12 mesi e la sostenibilità della strategia sulla base della capacità dell'ente di generare profitti accettabili entro i successivi 3 anni.
Sul piano della vigilanza, è necessario verificare che i profitti vengano realizzati grazie all'esistenza di un'adeguata struttura finanziaria e patrimoniale e ad una corretta propensione al rischio.
L'analisi del modello imprenditoriale deve fornire informazioni sui principali profili di vulnerabilità dell'ente in modo tale da consentire l'individuazione di rischi specifici per la solvibilità e la liquidità.
Il processo di valutazione del *business model* si articola in tre fasi:
- la prima consiste nell'individuare il modello di *business* e la materialità delle relative aree di *business* e nel raccogliere tutte le informazioni necessarie per fornire un quadro aggiornato di tali aree;
- la seconda fase prevede l'assegnazione di un punteggio agli enti sulla base di indici di profittabilità per valutare la capacità delle singole *business-line* di realizzare profitti;
- nella terza fase si valuta l'adeguatezza del modello imprenditoriale più nel medio termine al fine di individuare quali effetti potrebbe avere una crisi economica sulle aree di *business* e di aggiustare, se

[80]European Banking Authority, Guidelines on common procedures and methodologies for Srep and supervisory stress testing – EBA/GL/2014/13.

necessario, il punteggio attribuito nella seconda fase in relazione ad una valutazione complessiva sul rischio associato al *business model*[81].

2) *Governance* e gestione del rischio

I responsabili della vigilanza analizzano la *governance* dell'ente per valutarne l'adeguatezza rispetto ai profili di rischio, al modello di *business*, alla dimensione e alla complessità della banca. In particolare, devono verificare l'esistenza di una sana gestione dei rischi e di adeguati controlli interni e stabilire se vi sono rischi connessi all'inadeguatezza della *governance* e quale impatto possono avere sulla sostenibilità dell'ente.

La valutazione deve avere ad oggetto:

- il quadro complessivo dell'*internal governance*;
- la composizione e le responsabilità dell'organo di gestione e dei suoi comitati, se presenti;
- le politiche di remunerazione;
- il sistema di controllo interno, con specifico riferimento alla struttura e ai requisiti di indipendenza delle funzioni di gestione dei rischi, di *compliance* e di *internal audit*;
- il sistema di *risk management*, inclusi i processi ICAAP e ILAAP;
- le procedure amministrative e contabili;
- il sistema informativo.

Il processo di valutazione dell'*internal governance* si sviluppa in tre fasi. La prima fase è costituita da un'analisi preliminare sulla base delle prime informazioni raccolte e fornite direttamente dall'ente. Tali informazioni possono riguardare, tra l'altro, la composizione e le attribuzioni dell'organo di gestione, il *risk appetite framework* e le politiche di remunerazione. La seconda fase consiste nel controllo circa la conformità dell'*internal auditing* e del *risk management* alle disposizioni previste dalla direttiva CRD. La terza fase prevede una valutazione complessiva del sistema di *governance* per verificare come questo opera nella pratica e se garantisce il rispetto della normativa[82].

3) Rischi di capitale

Le autorità di vigilanza determinano il capitale necessario per coprire i rischi correlati al capitale in relazione a tre differenti angolazioni, c.d. *"building blocks".*

Il primo "blocco" prevede la valutazione dei rischi connessi al capitale. Tali rischi sono quattro:

- Il rischio di credito, che è connesso alle perdite causate da un debitore che non è in grado di rimborsare i prestiti o di adempiere ad un'obbligazione secondo i termini contrattuali. Questo tipo di rischio deriva, oltre che dai prestiti, anche da altri strumenti finanziari, tra cui transazioni in valuta

[81]Per maggiori dettagli sul modello imprenditoriale, cfr. European Banking Authority, Guidelines on common procedures and methodologies for srep and supervisory stress testing – EBA/GL/2014/13, Title 4.

[82]Per maggiori dettagli sull'elemento della governance e della gestione del rischio, cfr. European Banking Authority, Guidelines on common procedures and methodologies for Srep and Supervisory stress testing – EBA/GL/2014/13, Title 5.

estera, opzioni, azioni, contratti a termine. Quando valutano l'entità del rischio di credito di una banca, le autorità di vigilanza devono prendere in considerazione alcuni elementi come: le dimensioni dell'esposizione creditizia; la natura, la composizione e la qualità del portafoglio di crediti; le misure di mitigazione e copertura di tali rischi.

- Il rischio di mercato è il rischio di perdite in bilancio o fuori bilancio derivanti da cambiamenti nei prezzi di mercato che si ripercuotono sul conto economico o sulla situazione patrimoniale dell'ente. In particolare, ricomprende i rischi derivanti dagli strumenti finanziari posseduti (es. rischio di tasso di interesse e rischio di tasso di cambio), dalle caratteristiche delle posizioni assunte (es. posizioni complesse e con poca liquidità), dai rapporti con le controparti e dalle politiche di gestione del rischio.
- Il rischio di tasso di interesse sul portafoglio bancario è correlato all'esposizione dell'ente a movimenti sfavorevoli del tasso di interesse e deve essere valutato analizzando gli effetti dei cambiamenti del tasso di interesse sul valore attuale dei flussi di cassa futuri e sui guadagni di medio termine.
- Il rischio operativo è il rischio di perdite causate da processi interni, personale e sistemi inadeguati e dannosi o anche da fattori esterni. Di tale categoria fanno parte, tra gli altri, il rischio legale, il rischio di *compliance* e il rischio di modelli non correlati alle altre categorie di rischi SREP. Per ogni categoria di rischio, la valutazione dei livelli e dei controlli dei rischi si sviluppa in tre fasi: la prima fase consiste nella raccolta di dati e di informazioni; la seconda fase prevede l'assegnazione di un punteggio (sulla base di indicatori prestabiliti per i livelli di rischio e sulla base di un test di conformità per i controlli dei rischi); nella terza fase viene effettuata una valutazione complessiva che può portare ad una modifica dei punti assegnati nella seconda fase.

Nel secondo "blocco" le autorità di vigilanza devono valutare i processi ICAAP sia su un piano quantitativo sia su un piano qualitativo. È necessario stabilire se tali processi sono affidabili e proporzionati alla natura, alle dimensioni e alla complessità delle attività dell'ente. A tal fine, si controlla come i rischi vengono identificati e misurati e come i processi ICAAP vengono inclusi nei processi di gestione, di controllo interno e di audit. Per la valutazione dei processi ICAAP è necessario fare riferimento ai sette principi individuati dalla BCE nella guida sul processo ICAAP.

Il terzo "blocco" prevede una valutazione della copertura del capitale secondo una prospettiva futura e assumendo la presenza di situazioni di stress economico e finanziario. I livelli di rischio ICAAP dovrebbero rimanere gli stessi anche in situazioni di stress.

La valutazione su questi tre blocchi consente di analizzare l'adeguatezza del capitale secondo tre diverse angolazioni, valutando anche la conformità ai requisiti patrimoniali previsti dal primo pilastro e dal secondo pilastro[83].

4) Rischi di liquidità

Le autorità di vigilanza verificano l'adeguatezza della liquidità della banca in termini di copertura dei rischi correlati alla liquidità e ai finanziamenti. La liquidità rappresenta la capacità dell'ente di finanziarie le attività e di adempiere alle obbligazioni, mantenendo le perdite ad un livello accettabile. Il rischio di liquidità è un rischio a cui le banche sono particolarmente esposte dato il loro ruolo fondamentale consistente nel trasformare depositi di breve - medio termine in prestiti di lungo termine. È, dunque, indispensabile una gestione efficace di tale rischio per garantire l'abilità di adempiere a tutte le obbligazioni, nonostante eventi esterni e cambiamenti nei comportamenti degli altri agenti del mercato. Come per il rischio di capitale, anche per la valutazione del rischio di liquidità le linee guida della BCE sullo SREP hanno previsto l'analisi di tre "blocchi". Come visto sopra, il primo "blocco" consiste nella valutazione dei rischi connessi alla liquidità. In particolare, si tratta del rischio di liquidità di breve periodo - che consiste nel rischio che la banca si renda inadempiente alle proprie obbligazioni a causa dell'incapacità di generare sufficiente liquidità in un orizzonte temporale fino ad un anno - e del rischio di finanziamento – che è rappresentato dal rischio che l'ente non sia in grado di finanziarsi in modo sostenibile nel lungo periodo. La valutazione ha ad oggetto i livelli e i controlli di tali rischi e prevede l'assegnazione di punteggi per ogni singolo rischio che vanno poi sommati definendo il punteggio finale relativo al rischio di liquidità nel complesso.

Il secondo "blocco" è costituito dalla valutazione dei processi interni di analisi della liquidità (ILAAP) al fine di stabilire se tali processi sono adeguati ed efficienti. Anche sulla base di questa valutazione vengono assegnati dei punti che si aggiungono al punteggio complessivo sulla liquidità.

Come già visto riguardo al rischio di capitale, nel terzo "blocco" la valutazione viene svolta in un'ottica prospettica per verificare come varia il rischio di liquidità a seguito di situazioni di stress economico e finanziario. Queste analisi, definite stress test, hanno l'obiettivo di mettere alla prova i test interni posti in essere dalla banca, ma, soprattutto, di stabilire se è necessario imporre alla banca delle misure relative alla liquidità.

I risultati delle valutazioni relative ai tre "blocchi" vengono combinati per assegnare un punteggio complessivo al rischio di liquidità[84].

---

[83] Per maggiori dettagli sull'elemento del rischio di capitale, cfr. European Banking Authority, Guidelines on common procedures and methodologies for srep and supervisory stress testing – EBA/GL/2014/13, Title 6-7.

[84] Per maggiori dettagli sul rischio di liquidità, cfr. European Banking Authority, Guidelines on common procedures and methodologies for srep and supervisory stress testing – EBA/GL/2014/13, Title 8-9.

Per ognuno dei quattro elementi sopra richiamati (modello imprenditoriale, *governance* e gestione del rischio, rischio di capitale e rischio di liquidità), lo SREP si sviluppa secondo un processo di tre fasi: una fase di preparazione, una fase di valutazione e una fase di decisione[85].

La fase di preparazione è la fase in cui le autorità di vigilanza raccolgono un gran numero di informazioni su cui basare la successiva valutazione. Le informazioni di natura quantitativa sono importanti perché consentono analisi coerenti e comparabili, ma sono indispensabili anche informazioni di natura qualitativa[86].

La fase di valutazione è strettamente collegata al *Risk Assessment System* (RAS), necessario per l'analisi dei quattro elementi sopra richiamati e si articola a sua volta in tre step. Nel primo step i responsabili della vigilanza devono reperire le informazioni più specifiche riferibili ai rischi connessi a ciascuno dei quattro elementi. Il secondo step consiste nel valutare tutti gli elementi sulla base di indicatori e criteri prestabiliti secondo una prospettiva quantitativa, avente ad oggetto i livelli di rischio, e una prospettiva qualitativa, avente ad oggetto i controlli dei rischi. L'esito della valutazione si riflette in un punteggio provvisorio, assegnato all'ente, compreso tra 1 e 4.

Per quanto riguarda i livelli dei rischi, la valutazione può avere tali esiti:

- 1 punto (rischio basso): il livello di rischio è tale per cui non può determinare effetti significativi sugli elementi prudenziale dell'ente;
- 2 punti (rischio medio-basso): il livello di rischio è presente, ma è basso tanto da non rappresentare una minaccia;
- 3 punti (rischio medio-alto): il livello di rischio è tale da poter avere con buona probabilità effetti negativi sui requisiti prudenziale della banca;
- 4 punti (rischio alto): vi è un elevato rischio di impatto sugli elementi prudenziali.

Con riferimento ai controlli dei rischi, a valutazioni di carattere qualitativo corrispondono punteggi numerici. In particolare, si possono verificare le seguenti situazioni:

- 1 punto (controllo rigoroso): tale punteggio viene assegnato alle banche che presentano dei sistemi di gestione e di controllo particolarmente efficaci tali da scongiurare il rischio di effetti sui requisiti prudenziali;
- 2 punti (controllo adeguato): anche in questa ipotesi i rischi sono ritenuti poco significativi grazie alla presenza di controlli adeguati e accettabili;
- 3 punti (controllo debole): in questa situazione, sussiste il rischio, considerato di medio livello, di impatti significativi sugli elementi prudenziali a causa di un sistema dei controlli debole e che necessita di miglioramenti;

---

[85] Banca Centrale Europea, sito web della Vigilanza Bancaria in Supervisory practices – SREP methodology

[86] Cfr. European Banking Authority, Guidelines on common procedures and methodologies for srep and supervisory stress testing – EBA/GL/2014/13, paragraph 151.

- 4 punti (controllo inadeguato): questo punteggio rispecchia un elevato rischio per i requisiti prudenziali e dipende da controlli inesistenti o inadeguati. Tali controlli sono indefiniti e incompatibili rispetto alla struttura e alla complessità dell'ente.

Nel terzo step, sulla base di una valutazione complessiva dello stato di salute dell'ente, viene assegnato il punteggio definitivo in seguito ad eventuali aggiustamenti apportati attraverso l'applicazione del c.d. "*constrained judgement*". Queste modifiche possono consistere nella riduzione di due punti al massimo o nell'aggiunta di un punto al massimo basandosi su alcuni elementi, tra cui: la conoscenza della banca; il confronto con enti comparabili; l'ambiente in cui l'ente opera; le misure su capitale e liquidità attuate dalla banca per assicurare la conformità al contesto normativo e regolamentare (in particolare, al pacchetto CRR/CRD IV); il livello di rischio ritenuto accettabile.

In questo modo, le autorità di vigilanza ottengono una visione complessiva dell'ente e dei suoi profili di rischi e, se necessario, individuano le misure di vigilanza più appropriate[87].

La terza fase è quella della decisione delle autorità di vigilanza e si basa sulla valutazione SREP complessiva[88]. In relazione a quest'ultima, le autorità di vigilanza decidono quali sono le misure necessarie ad affrontare i profili critici della banca. In questa fase finale i gruppi di vigilanza congiunti, prima di predisporre la decisione SREP, possono richiedere un confronto con l'organo di amministrazione dell'ente vigilato. I progetti di decisione devono essere approvati dal Consiglio di vigilanza e poi inviati alle banche vigilate in modo tale che queste possano presentare delle osservazioni e, entro il termine di due settimane, chiedere di essere sentite. Scaduto questo termine e valutate le osservazioni eventualmente presentate dai soggetti vigilati, il progetto di decisione viene sottoposto nuovamente al Consiglio di Vigilanza per l'approvazione. La decisione SREP viene adottata con la procedura di non obiezione e comunicata al collegio di vigilanza e all'ente interessato, il quale può chiederne il riesame alla Commissione amministrativa del riesame o impugnarla davanti alla Corte di giustizia dell'Unione europea.

Le decisioni SREP possono riguardare:

- Requisiti di fondi propri: requisito patrimoniale SREP complessivo composto dai requisiti minimi di fondi propri (8%, di cui almeno il 56,25% sotto forma di capitale primario di classe 1 (Common Equity Tier 1, CET1)) e dai requisiti aggiuntivi di fondi propri (P2R, soltanto CET1); requisiti di riserva combinati (soltanto CET1).
- Requisiti quantitativi di liquidità a livello del singolo ente: LCR (*liquidity coverage ratio*) più elevato del minimo previsto dalle disposizioni; periodo di sopravvivenza più elevato; misure a livello nazionale.

[87] European Banking Authority, Guidelines on common procedures and methodologies for srep and supervisory stress testing – EBA/GL/2014/13, Title 2 (Section 2.1.4) e Title 10.

[88] V. artt. 16 e 22 del Regolamento sull' MVU e Linee guida BCE sullo SREP, Titolo II.

- Altre misure qualitative di vigilanza: ulteriori misure previste dal regolamento sul Meccanismo di Vigilanza unico o da altre fonti normative, come quelle sulle restrizioni delle attività, sulle riduzioni dei rischi, sulle limitazioni relative alla distribuzione dei dividendi o altre misure correttive; verifiche sull'applicazione dei rilievi delle ispezioni in loco (follow-up).

A conclusione del processo SREP, le decisioni vengono pubblicate sul sito internet della BCE dedicato alla vigilanza bancaria.

CAPITOLO 3

Il ruolo del Sistema di Controllo Interno e della funzione di *Internal Audit* nell'ambito dello SREP

1. Il ruolo del Sistema di Controllo Interno nelle banche e nello SREP

L'importanza di un adeguato governo societario e di un efficiente sistema di controlli interni è ormai un dato incontrovertibile per tutte le imprese. Ciò è ancor più vero per le banche, data la particolare attività svolta e che vede coinvolti interessi pubblici tutelati dal nostro ordinamento. Gli assetti organizzativi delle banche, infatti, se da un lato devono mirare a realizzare gli interessi dell'impresa, dall'altro devono essere volti ad una sana e prudente gestione della banca e alla stabilità del sistema finanziario[89].

A tal fine è necessario che il *top management* sia in grado di individuare e gestire tutti i rischi correlati all'attività della banca, che il SCI operi in modo indipendente e coerente con le necessità della stessa e che sia garantito un adeguato sistema di flussi informativi.

Le banche devono predisporre un sistema dei controlli interni che sia conforme alla normativa comunitaria e nazionale definita dal Comitato di Basilea, dalla direttiva Mifid e dalle disposizioni di Banca d'Italia.

Quest'ultima, nella Circolare n. 285 del 2013, prevede un set regolamentare relativo al governo societario e ad alcuni elementi tipici dei sistemi di amministrazione e controllo[90]. Viene riproposta l'ormai assodata distinzione tra le funzioni di supervisione strategica, di gestione e di controllo e vengono introdotti specifici requisiti dimensionali e qualitativi per la composizione e l'organizzazione interna degli organi sociali. In particolare, la Circolare individua come elemento fondamentale per una *governance* efficace ed equilibrata la presenza di comitati endoconsiliari, i quali, almeno per le banche di maggiori dimensioni e complessità operativa, devono essere: comitato nomine, comitato rischi e comitato remunerazioni. Questi comitati devono scegliere il proprio presidente tra i membri indipendenti e non esecutivi.

---

[89] La sana e prudente e gestione è uno dei principi cardine della vigilanza contenuti nell'art. 5 del T.U.B., assieme alla stabilità complessiva, all'efficienza e competitività del sistema finanziario e all'osservanza delle disposizioni in materia creditizia. FAZIO, in "*Concorrenza e mercato*" (1995) definisce "sana" «*una gestione che si ispiri a criteri di piena efficienza funzionale, perseguendo il profitto in base a decisioni indipendenti da interessi estranei all'impresa bancaria e conformi a canoni di correttezza*». La "prudenza", secondo l'autore, «*va invece ricercata nella particolare avversione al rischio che deve caratterizzare la condotta di chi, direttamente o indirettamente, impegna nell'attività di impresa non solo il proprio capitale, ma soprattutto la disponibilità dei risparmiator*i».

[90]Banca d'Italia, *Disposizioni di vigilanza per le banche*, Circ. n. 285 del 17 dicembre 2013, primo capitolo del Titolo IV, introdotto con l'aggiornamento del 6 maggio 2014, della quale si è offerto un breve inquadramento nel capitolo che precede.

Questa normativa propone un'architettura interna articolata per funzioni e non per organi, in tal modo adottando un principio di neutralità rispetto ai tre diversi sistemi di amministrazione e controllo (tradizionale, monistico e dualistico).

Si concentra, inoltre, su una più compiuta definizione dell'organo con funzione di supervisione strategica e con funzione di gestione, secondo una netta distinzione di competenze e ambiti operativi anche in materia di controlli interni. In relazione a quest'ultimo tema, la Circolare individua le finalità che il SCI deve perseguire, tra cui si possono citare:

- Il contenimento dei rischi entro i limiti indicati nel *Risk Appetite Framework* (RAF);
- Verifica dell'attuazione e dell'efficacia delle politiche e dei processi aziendali;
- Sicurezza e affidabilità delle informazioni e dei sistemi informatici;
- Rispetto della legge e della normativa di vigilanza, nonché di politiche, procedure e regolamenti interni.

A questo punto, sembra opportuno richiamare i profili applicativi e organizzativi previsti dalla normativa sul tema dei controlli interni al fine di esaminarne le dinamiche operative. In particolare, si fa riferimento agli organi e alle unità di controllo individuati dalla Circolare come elementi indispensabili per la solidità del sistema e che, quindi, la banca dovrebbe necessariamente implementare.

Le banche devono istituire funzioni aziendali di controllo indipendenti e permanenti secondo i tre livelli tipici di controllo. Queste funzioni devono essere formalizzate e separate sul piano organizzativo. Nel rispetto del principio di proporzionalità, le banche possono decidere di affidare ad un'unica struttura le funzioni di *Risk Management* e di *Compliance*, ma in nessun caso è ammissibile una sovrapposizione di queste con la funzione di *Internal Audit*, essendo quest'ultima responsabile delle verifiche sulle prime.

Come detto in precedenza i controlli di secondo livello comprendono la funzione di *Risk Management* e la funzione di *Compliance*. Quest'ultima si afferma nel nostro ordinamento a seguito del recepimento delle indicazioni del Comitato di Basilea. In particolare, le regole di Basilea II introducono, tra l'altro, l'obbligo per le banche di individuare anche quei rischi non rientranti nei requisiti patrimoniali minimi di Primo pilastro, tra cui i rischi legali e di reputazione oggetto proprio delle attività di *Compliance*. La funzione di *Compliance*, infatti, ha il compito di verificare che tutti i settori operativi della banca operino in conformità a tutte le norme riferibili all'attività bancaria.

Questa funzione viene disciplinata anche dalla normativa europea: in particolare, dalle direttive 2004/39/CE (MiFID) e 2006/73/CE (recante modalità di esecuzione della MiFID) che sottolineano la necessità che la funzione di *Compliance* sia istituita in modo tale da rispettare l'indipendenza e il principio di proporzionalità. Queste direttive contengono disposizioni di grande rilevanza per il

sistema dei controlli interni, recepite da Banca d'Italia[91] e dal c.d. Regolamento Congiunto emanato da Banca d'Italia e Consob[92].

Le motivazioni che hanno spinto le Autorità a disciplinare la *Compliance* sono principalmente due: la prima deriva dalla varietà di attività che una banca può svolgere e che espone la stessa ad una serie di rischi "nuovi" che possono inficiare anche l'attività di altri operatori legati alla banca, come rischi reputazionali, legali e di non conformità alle norme[93]; la seconda è relativa alla difficoltà di garantire la conformità a tutti gli interventi normativi che regolano la materia (normativa nazionale e comunitaria, norme primarie e secondarie, autoregolamentazione, codici di condotta e procedure interne) e che fa aumentare significativamente il rischio di non conformità[94].

Le Disposizioni di Banca d'Italia definiscono il rischio di non conformità alle norme come "*il rischio di incorrere in sanzioni giudiziarie o amministrative, perdite finanziarie rilevanti o danni di reputazione in conseguenza di violazioni di norme imperative (leggi, regolamenti), ovvero di autoregolamentazione (statuti, codici di condotta, codici di autodisciplina)*"[95].

La funzione di *Compliance* è prevista proprio per verificare e garantire che la banca metta in atto tutte le misure per arginare questo rischio.

A tal fine, i compiti richiesti a tale funzione possono essere:

- Contribuire alla definizione delle politiche di valutazione dei rischi di non conformità alle norme effettuata dalle singole strutture aziendali;
- Implementare procedure per la gestione del rischio di non conformità e garantire che siano idonee e correttamente applicate;
- Individuare le normative relativa all'attività bancaria, inclusi aggiornamenti, novelle e modifiche, e valutarne gli effetti su processi e procedure aziendali;
- Predisporre le modifiche organizzative e procedurali necessarie per un adeguato presidio del rischio di non conformità e verificarne l'efficacia;
- Organizzare flussi informativi diretti a tutti gli organi aziendali e alle strutture coinvolte.

Il rischio di non conformità è diffuso in tutti i livelli dell'organizzazione, perciò, è necessario sensibilizzare tutto il personale all'importanza della prevenzione di tale rischio e diffondere una cultura aziendale fondata sull'onestà, la correttezza e il rispetto delle norme.

---

[91] Si fa riferimento alle Disposizioni di Vigilanza di Banca d'Italia del 10 luglio 2007. Oggi la normativa di riferimento è la circolare n.285/2003.

[92]Emanato il 27 ottobre 2007, in attuazione della direttiva di "secondo livello" 2006/73/CE, a sua volta di attuazione della direttiva MiFId. Al capo III disciplina le "Funzioni aziendali di controllo" per quanto concerne i soggetti abilitati ai servizi e alle attività di investimento e alla gestione collettiva del risparmio. In particolare, l'art.16 fa riferimento specificatamente al controllo di conformità.

[93]CENDERELLI E., BRUNO E."*La Banca. Aspetti normativi e gestionali*", pag.132.

[94] BOCUZZI G, "*La funzione di compliance: il presidio dei rischi aziendali e l'evoluzione della normativa Basilea 2 e Mifid"*, Bancaria n.2/2008.

[95] Circolare n.285/2003, titolo IV, capitolo 3, sezione III.3.2.

Dal punto di vista organizzativo, la funzione di *Compliance* può essere istituita secondo un modello accentrato o secondo un modello decentrato[96].

Il primo modello prevede che la funzione operi in totale autonomia e tramite risorse idonee a controllare l'attività di ogni unità organizzativa. Proprio la necessità di dover usufruire di un gran numero di risorse rende questo modello particolarmente oneroso e, per questo motivo, più adatto a banche di maggiori dimensioni. Le banche che adottano tale modello devono limitare il rischio di duplicazioni di attività e di un'eccessiva rigidità nei processi burocratici.

Nel modello decentrato la figura centrale è quella del *Compliance Officer* al quale viene affidata la funzione di *Compliance.* Il *Compliance Officer* può richiedere il supporto delle altre funzioni aziendali di controllo o affidare delle attività di *compliance* esternamente. In questo secondo caso, le attività devono essere formalizzate in contratti di servizi che definiscano con precisione gli obiettivi della funzione e la frequenza dei flussi informativi verso il *Compliance Officer* e verso gli altri organi aziendali. Questo modello viene di solito utilizzato da banche di piccole dimensioni che svolgono attività semplici.

Dei controlli di secondo livello fa parte anche la funzione di *Risk Management.* Questa funzione, già richiamata nel primo capitolo, assume ancor più rilevanza per le banche. Queste, infatti, svolgono attività in cui è insita l'assunzione di rischi, non solo per la banca stessa ma anche per la clientela; ciò comporta che in tali organizzazioni il governo dei rischi debba essere particolarmente efficace ed evoluto[97]. La funzione di *Risk Management* assume un'importanza fondamentale in relazione al capitale della banca e, in particolare, all'individuazione del livello di capitale adeguato per fronteggiare i rischi[98]. La funzione di *Risk Management* nelle banche va delineata richiamando le Disposizioni di Basilea. L'importanza del ruolo del *Risk manager*, infatti, si può comprendere pienamente con riferimento al Secondo Pilastro. In tale ambito, il *Risk manager* deve definire le metodologie di misurazione dei rischi consistenti, nel dettaglio, nel calcolo del capitale regolamentare a fini di vigilanza e nel calcolo del capitale economico a fini gestionali[99]. Il responsabile della funzione di *Risk Management* è protagonista del processo ICAAP, cioè del processo consistente nella definizione dell'ammontare adeguato di capitale, che rappresenta una componente fondamentale del processo di gestione dei rischi e, più in generale, del sistema dei controlli interni. Nell'ambito dei processi ICAAP/ILAAP, il *Risk manager* deve definire metodologie di identificazione anche per i

---

[96]ANOLLI M., RAJOLA F. "*Il rischio di reputazione e di non conformità. Strumenti per la governance e la gestione operativa*" (2010) pagg. 92,93.

[97]TARANTOLA, "*Il ruolo del risk management per un efficace presidio dei rischi: le lezioni dalla crisi*", 2011.

[98] cfr. A. RESTI (2008), "*Il secondo pilastro e la sfida del capitale economico*", Roma.

[99] E. DELLAROSA, R. RAZZANTE, *"Il nuovo sistema dei controlli interni della banca*".

rischi non misurabili combinando un approccio quantitativo e un approccio qualitativo e deve condurre le prove di stress testing.

Nella stessa ottica, le Disposizioni di Banca d'Italia prevedono che il ruolo principale della funzione di controllo dei rischi è quello di definire ed applicare il *Risk Appetite Framework* (RAF) e le relative politiche di gestione dei rischi[100].

Nelle banche di maggiori dimensione, la funzione di *Risk Management*, relativamente a particolari profili di rischio, può essere affidata a specifici comitati purché vengano definiti chiaramente i compiti e venga comunque garantita una visione complessiva dell'esposizione ai rischi della banca.

Oltre ai compiti relativi al RAF, il *Risk manager* deve:

- contribuire alla valutazione del rischio strategico svolta dagli altri organi aziendali;
- valutare i rischi correlati a nuovi prodotti, nuovi servizi o nuovi segmenti di mercato;
- monitorare costantemente la coerenza dei rischi rispetto agli obiettivi aziendali;
- valutare il rischio reputazionale coordinandosi con la funzione di *compliance*;
- verificare l'idoneità delle misure correttive applicate.

I controlli di terzo livello sono quelli attribuiti alla funzione di *Internal Audit* che è volta a monitorare l'andamento dell'operatività e ad individuare eventuali anomalie e violazioni, nonché a valutare la complessiva funzionalità del sistema dei controlli interni[101].

Nell'ambito degli accertamenti di natura ispettiva e secondo le Disposizioni di Banca d'Italia, la funzione di revisione interna deve verificare:

- il corretto funzionamento dei meccanismi di delega e l'utilizzo delle informazioni da parte di tutte le attività aziendali;
- le metodologie di monitoraggio della conformità alle norme;
- l'evoluzione dei rischi e la regolarità di tutte le attività aziendali;
- l'adeguatezza e la sicurezza del sistema informativo;
- la rimozione delle anomalie riscontrate (attività di follow-up).

Nel processo di gestione dei rischi, il ruolo *dell'Internal Auditing* consiste nel valutare:

- la funzione di *Risk Management* con riferimento all'organizzazione, alle responsabilità e all'adeguatezza delle risorse a questa assegnate;
- la correttezza degli stress test e delle analisi di sensitività/scenario;
- la conformità alle best practices del settore.

Con particolare riferimento al processo ICAAP, i ruoli dell'*Internal Auditing* variano in base alla tipologia di banca. Infatti, nelle banche che adottano "metodi base" per la determinazione dei requisiti

[100] Circolare n.285/2013, titolo IV, capitolo 3, sezione III.3.3.

[101] Circolare n.285/2013, Titolo IV, Capitolo 3, Sezione III, "Funzione di revisione interna (internal audit)"

di Primo pilastro, l'IA deve limitarsi a monitorare i processi di definizione e implementazione delle misure di mitigazione dei rischi; nel caso in cui vengano attuate metodologie evolute di determinazione dei requisiti di capitale, l'IA deve valutare le procedure di esecuzione di tali metodologie. Nel caso di banche che adottano "modelli interni" di determinazione dei requisiti di primo e secondo pilastro, la portata dei compiti dell'*Internal Auditing* si amplia rispetto a quelli citati sopra. In particolare, l'IA deve svolgere, oltre ad un'analisi documentale dei controlli eseguiti e dei risultati, delle verifiche anche di tipo quantitativo sull'accuratezza dei modelli stessi. Le verifiche sull'adeguatezza dei modelli interni vengono effettuate attraverso specifici test.

Nell'ambito dell'ICAAP, l'IA deve valutare:

- che gli organi aziendali siano correttamente coordinati con particolare riferimento ai rapporti tra l'Alta Direzione e le diverse funzioni aziendali;
- che il processo ICAAP sia definito e formalizzato in modo idoneo;
- che la normativa ICAAP sia adeguatamente recepita ed applicata;
- che la documentazione ICAAP destinata alle Autorità di vigilanza sia correttamente predisposta ed approfondita.

L'IA è coinvolto in ogni fase del processo ICAAP. Con riferimento alle singole fasi le verifiche da svolgere riguardano:

- nella prima fase di determinazione degli elementi di capitale, la coerenza tra le decisioni in merito agli obiettivi di capitale e gli obiettivi strategici e l'adeguatezza del *risk appetite* cioè della propensione al rischio rispetto al capitale interno;
- nella fase dell'individuazione dei rischi da valutare, la correttezza del processo di identificazione dei rischi e della classificazione degli stessi in rischi gestibili, misurabili e mitigabili, nonché l'applicazione di un idoneo criterio di materialità nell'identificazione dei rischi;
- nella fase della valutazione dei rischi, la qualità dei dati e delle ipotesi sottostanti alla valutazione, l'idoneità delle metodologie di valutazione e di stress testing e degli scenari ipotizzati, nonché la correttezza dei risultati conseguiti e della loro interpretazione;
- nella fase di determinazione del capitale interno complessivo, la correttezza delle metodologie e delle ipotesi sottostanti e la robustezza dei risultati conseguiti;
- nella fase di determinazione degli elementi patrimoniali e di riconciliazione con il patrimonio di vigilanza, le decisioni in merito alle poste patrimoniali da imputare a capitale complessivo e il processo di riconciliazione del capitale complessivo con il patrimonio di vigilanza (solo nel caso di adozione di una definizione di capitale complessivo diversa da quella di patrimonio di vigilanza);

- nella fase di autovalutazione, la correttezza delle criticità individuate dalle singole unità organizzative e delle misure correttive previste.

2. Valutazione della governance di Unicredit, UBI Banca, Mediobanca e Intesa Sanpaolo

2.1 Premessa

A questo punto della trattazione, si ritiene utile procedere con l'analisi, in ottica SREP, di quattro banche italiane sotto il profilo delle strutture di *governance* e di controllo interno. L'obiettivo del lavoro consiste nell'assegnazione di una valutazione finale, anche numerica, che possa riflettere l'adeguatezza e l'efficienza di tali strutture. Oggetto della valutazione sono quattro banche italiane, tutte quotate nel mercato di Milano (FTSE Mib) e "*significant*", quindi soggette alla vigilanza diretta della Banca Centrale Europea: Intesa Sanpaolo, Mediobanca, UBI banca e UniCredit.

Come rilevato nel secondo capitolo, il *Supervisory Review and Evaluation Process* valuta lo stato di salute delle banche da quattro angolazioni, tra cui la *governance* dell'organizzazione. In questo ambito l'autorità di vigilanza deve verificare l'esistenza di una sana gestione dei rischi e di un adeguato sistema dei controlli interni e deve stabilire se vi sono rischi connessi all'inadeguatezza della *governance* e quale impatto questi possono avere sulla sostenibilità dell'ente.

In particolare, la valutazione deve avere ad oggetto:

- il quadro complessivo dell'*internal governance*;
- la composizione e le responsabilità dell'organo di gestione e dei suoi comitati, se presenti;
- le politiche di remunerazione;
- il sistema di controllo interno, con specifico riferimento alla struttura e ai requisiti di indipendenza delle funzioni di gestione dei rischi, di *compliance* e di *internal audit*;
- il sistema di *risk management*, inclusi i processi ICAAP e ILAAP;
- le procedure amministrative e contabili;
- il sistema informativo.

Il processo di valutazione dell'*internal governance* si sviluppa in tre fasi. La prima fase è costituita da un'analisi preliminare sulla base delle prime informazioni raccolte e fornite direttamente dall'ente. Tali informazioni possono riguardare, tra l'altro, la composizione e le attribuzioni dell'organo di gestione, il *risk appetite framework* e le politiche di remunerazione. La seconda fase consiste nel controllo circa la conformità dell'*internal auditing* e del *risk management* alle disposizioni previste dalla direttiva CRD IV. La terza fase prevede una valutazione complessiva del sistema di *governance* per verificare come questo opera nella pratica e se garantisce il rispetto della normativa e nell'assegnazione alla *governance* della banca di un punteggio da 1 a 4 (un punteggio pari a 1

corrisponde ad un "rischio basso" mentre un punteggio pari a 4 corrisponde ad un "rischio elevato")[102].

2.2 Individuazione dei criteri di valutazione

I criteri di valutazione della *governance* sono quelli individuati dalle Linee guida della BCE sullo SREP e richiamati nel precedente paragrafo. In particolare, si è valutata la conformità delle banche oggetto di valutazione alle disposizioni relative al governo societario e al SCI contenute nella circolare 285/2013, negli "Orientamenti sulla Governance" emanati dall'EBA il 21 marzo 2018 e nello "Schema per i sistemi di controllo interno nelle organizzazioni bancarie" del Comitato di Basilea[103].

I criteri utilizzati ai fini della valutazione sono i seguenti:

1) Composizione e responsabilità dell'organo di gestione e di supervisione strategica

   Il primo criterio in base al quale si è svolta la valutazione è quello della composizione dell'organo collegiale.

   Innanzitutto, è necessaria una netta distinzione tra le funzioni di gestione e quelle di supervisione strategica sia nel caso in cui tali funzioni siano attribuite a due organi distinti sia nel caso in cui ricadano in capo ad un unico organo.

   Ai sensi delle disposizioni sopra richiamate, tale organo non dovrebbe avere membri in numero superiore a 15 per le banche che adottano il sistema tradizionale, a 19 per le banche con sistema monistico e a 22 per le banche con sistema dualistico. Queste misure sono previste per le banche di maggiori dimensioni o più complesse dal punto di vista operativo; le altre banche devono prevedere componenti in misura inferiore.

   È necessario poi verificare la presenza di consiglieri non esecutivi che sono indispensabili per garantire l'equilibrio e per controbilanciare i componenti esecutivi e il management della banca.

   La valutazione dell'organo con funzione di supervisione strategica deve poi avere ad oggetto i consiglieri indipendenti che devono rappresentare almeno un quarto dei componenti del consiglio. Questi devono possedere elevati livelli di professionalità ed autorevolezza così da poter aver un certo peso all'interno del collegio e contribuire alle procedure decisionali dello stesso.

   Nell'ottica dell'indipendenza, è anche necessario limitare il numero di incarichi attribuibili a ciascun membro nel rispetto dei limiti previsti dalla direttiva CRD IV.

---

[102] cfr. European Banking Authority, Guidelines on common procedures and methodologies for Srep and Supervisory stress testing – EBA/GL/2014/13, Title 5.

[103] Cfr. Allegato 1 e Allegato 2.

Secondo tale Direttiva, ciascun Consigliere può ricoprire complessivamente:

- 1 incarico esecutivo e 2 incarichi non esecutivi
- 4 incarichi non esecutivi

con le seguenti precisazioni e fatte salve le diverse prescrizioni della normativa nazionale:

a) per incarichi si intendono quelli presso il Consiglio di amministrazione, il Consiglio di sorveglianza, il Consiglio digestione, il Collegio sindacale e di Direttore Generale: nelle società estere, si considerano gli incarichi equivalenti agli stessi, in base alla normativa applicabile alla società;
b) sono considerati come un unico incarico, fra l'altro, l'insieme degli incarichi ricoperti: i) nell'ambito dello stesso gruppo; ii) in società non rientranti nel gruppo, in cui la banca detenga una partecipazione qualificata, come definita dall'art. 4 del Regolamento (UE) n. 575/2013.

Va verificato, inoltre, che i consiglieri dedichino tempo adeguato alle funzioni tenuto conto della natura e delle caratteristiche di tali funzioni, nonché di altri incarichi, impegni e attività lavorative.

Un ulteriore requisito che le banche devono tenere in considerazione nella composizione dell'organo di gestione è la diversificazione: per garantire che le decisioni siano ponderate sulla base di posizioni e visioni diverse è necessario che i componenti siano scelti rispettando la diversificazione non solo in termini di competenze, capacità ed esperienze, ma anche in termini di età, genere, provenienza geografica[104].

2) Procedure di nomina

Nella valutazione dell'adeguatezza della struttura di *governance*, devono tenersi in considerazione le modalità di nomina e di revoca degli organi aziendali. Queste devono emergere in modo trasparente dallo statuto e devono coinvolgere il consiglio di amministrazione, l'assemblea e, se previsto, il comitato nomine. Le procedure di nomina devono condurre alla selezione di soggetti con i necessari requisiti di professionalità e competenze definiti ex ante. Infatti, il Consiglio di amministrazione deve individuare in via preventiva la propria composizione ideale dal punto di vista qualitativo e quantitativo, specificando e motivando quale deve essere il profilo dei consiglieri. La modalità più adatta al fine di garantire la corretta composizione dell'organo di gestione è quella basata sulla presentazione di liste di candidati[105].

3) Politiche di remunerazione

[104] Cfr. Banca d'Italia, Circolare 285/2013, Titolo IV, Capitolo 1, 2.2.1.
[105] Cfr. Banca d'Italia, Circolare 285/2013, Titolo IV, Capitolo 1, Sezione IV.

È necessario valutare se le banche definiscono le proprie politiche di remunerazione nel rispetto delle Disposizioni di Vigilanza per le banche allineate e degli Orientamenti in materia di sane politiche di remunerazione emanate dall'EBA in attuazione della direttiva 2013/36/UE. Buone politiche di remunerazione ed incentivazione dei consiglieri e del management sono fondamentali per la competitività e il buon governo della banca, nonché per attirare e mantenere soggetti di elevate professionalità e capacità. In ogni caso tali politiche devono essere predisposte nei limiti della propensione al rischio, delle politiche di gestione del rischio e del livello di capitale e di liquidità necessari. Le banche devono verificare che il personale, soprattutto quello più rilevante, non sia remunerato attraverso modalità o strumenti elusivi delle disposizioni sopra richiamate e, a tal fine, conducono delle verifiche a campione sui conti interni di custodia e amministrazione.

È necessario garantire il giusto bilanciamento tra componenti variabile e componente fissa e definire anticipatamente l'incidenza della componente variabile su quella fissa. Il rapporto tra la componente variabile e quella fissa del personale più rilevante non deve superare il 100% (rapporto di 1:1); se previsto dallo statuto e deciso dall'assemblea, il limite può essere elevato a 200% (rapporto di 2:1) o modificato per singoli individui o categorie di personale, sempre nel limite del 200%.

Per quanto riguarda la remunerazione dell'organo con funzione di controllo, è esclusa la componente variabile o, se presente, è contenuta e assoggettata con particolare rilievo alle Disposizioni.

4) Comitati endoconsiliari

   Un ulteriore elemento da sottoporre a valutazione è la costituzione di comitati endoconsiliari. Le Disposizioni di Vigilanza prevedono, per le banche di maggiori dimensioni e complessità operativa, l'obbligo di costituire almeno il comitato nomine, il comitato remunerazioni e il comitato rischi, mentre per le banche "intermedie" solo il comitato rischi.

   I comitati possono essere costituiti da un minimo di 3 a un massimo di 5 componenti tutti non esecutivi e in maggioranza indipendenti; i comitati devono scegliere il loro presidente tra gli indipendenti e devono distinguersi per almeno un componente. Nel modello monistico, il "comitato per il controllo sulla gestione" deve avere almeno 3 componenti al fine di assicurare l'efficacia dei controlli[106].

5) Sistema di controllo interno

   La valutazione deve avere ad oggetto la qualità del sistema di controllo interno.

[106] Cfr. Banca d'Italia, Circolare 285/2013, Titolo IV, Capitolo 1, Sezione IV, 2.3.

È necessario verificare, innanzitutto, la presenza di una solida cultura dei controlli affermata dal Consiglio di amministrazione e dall'Alta direzione e diffusa a tutti i livelli dell'organizzazione. A tal fine, si deve verificare se l'Alta direzione abbia dato sufficiente rilevanza alla necessità di un efficiente sistema dei controlli interni nelle sue dichiarazione, nelle sue azioni e, soprattutto, nella scelta dei criteri di remunerazione e promozione e se abbia definito con chiarezza la struttura e le responsabilità manageriali.

In secondo luogo, elemento di valutazione deve essere il processo di individuazione e valutazione del rischio. È necessario verificare se la banca ha dedicato risorse sufficienti al monitoraggio dei rischi associati agli obiettivi aziendali e se ha modificato il processo di valutazione dei rischi coerentemente con il mutare del contesto operativo. Va valutata l'adeguatezza della funzione di *Risk Management* sia dal punto di vista dell'organizzazione e dell'indipendenza sia dal punto di vista delle metodologie utilizzate per l'identificazione e il controllo dei rischi. Queste valutazioni vanno svolte nello specifico con riferimento ai processi ICAAP e ILAAP.

In terzo luogo, deve verificarsi se la banca abbia provveduto alla chiara e netta separazione delle funzioni di controllo. A tal fine, la banca deve evitare di attribuire ad un unico soggetto più responsabilità relative ad attività in potenziale conflitto di interesse. In particolare, si deve valutare se sono ben definite le funzioni di *Compliance*, di *Risk Management* e di *Internal Audit*. Come anticipato nella prima parte del capitolo, infatti, tali funzioni aziendali di controllo devono essere indipendenti e separate sul piano organizzativo. Nel rispetto del principio di proporzionalità, le banche possono decidere di affidare ad un'unica struttura le funzioni di *Risk Management* e di *Compliance*, ma in nessun caso è ammissibile una sovrapposizione di queste con la funzione di *Internal Audit*, essendo quest'ultima responsabile delle verifiche sulle prime.

Inoltre, deve essere oggetto di valutazione anche il flusso di informazioni tra le funzioni di controllo. Il sistema di informazione deve garantire che vengano adeguatamente comunicati compiti e responsabilità di controllo del personale nonché che vengano predisposte idonee linee di comunicazione, soprattutto verso l'alto, per la segnalazione di irregolarità da parte di dipendenti.

Infine, è necessario che i sistemi di controllo interno vengano sottoposti ad un monitoraggio continuo attraverso procedure automatizzate. Tali procedure consentono di individuare tempestivamente carenze nel sistema informativo o nella valutazione dei rischi.

Una modalità per individuare l'inadeguatezza del sistema di controllo interno consiste nel valutare l'operato della funzione di *Internal Auditing* della banca esaminando le metodologie di individuazione e gestione dei rischi e la documentazione.

In particolare, va verificato se la banca ha evitato un'eccessiva frammentazione dell'attività di revisione interna. Infatti, per garantire una valutazione complessiva dei processi gestionali e dell'adeguatezza del sistema di controllo interno ad ogni fase del processo è necessario un approccio che consenta al revisore di seguire interamente i processi e le funzioni.

Si deve valutare anche se i revisori interni siano in possesso della professionalità e delle competenze tecniche necessarie per rilevare la presenza di problemi e, eventualmente, mettere in discussione le risposte date in proposito dalla banca.

Oggetto di valutazione deve essere, inoltre, la tempestività con cui la direzione pone rimedio alle problematiche rilevate dai revisori; in caso di ritardi, è necessario verificare se siano dovuti ad una sottovalutazione da parte della direzione del ruolo e della rilevanza della funzione di revisione interno oppure ad una mancanza del revisore stesso che non ha trasmesso prontamente la documentazione necessaria[107].

6) Sistema informativo

Oggetto di specifica valutazione è la predisposizione di adeguati flussi informativi tra gli organi aziendali. È necessario verificare che la banca adotti procedure di scambio delle informazioni tempestive, accurate ed efficienti tra gli organi e all'interno di questi. A tal fine, la banca deve formalizzare con appositi regolamenti l'individuazione dei soggetti che devono regolarmente inviare i flussi informativi nonché la documentazione da inviare, le modalità e le tempistiche[108].

[107] Cfr. Comitato di Basilea, "Schema per i sistemi di controllo interni delle organizzazioni bancarie" come riportati, in sintesi, nell'Allegato 2.

[108] Cfr. Banca d'Italia, Circolare 285/2013, Titolo IV, Capitolo 1, Sezione V.

2.3 Valutazione delle banche

Unicredit

Unicredit ha adottato il sistema di amministrazione e controllo "tradizionale" basato sulla presenza di un organo di gestione e supervisione strategica, il Consiglio di amministrazione, e un organo con funzione di vigilanza, il Collegio sindacale, entrambi nominati dall'Assemblea, come rappresentato nella Figura 3.

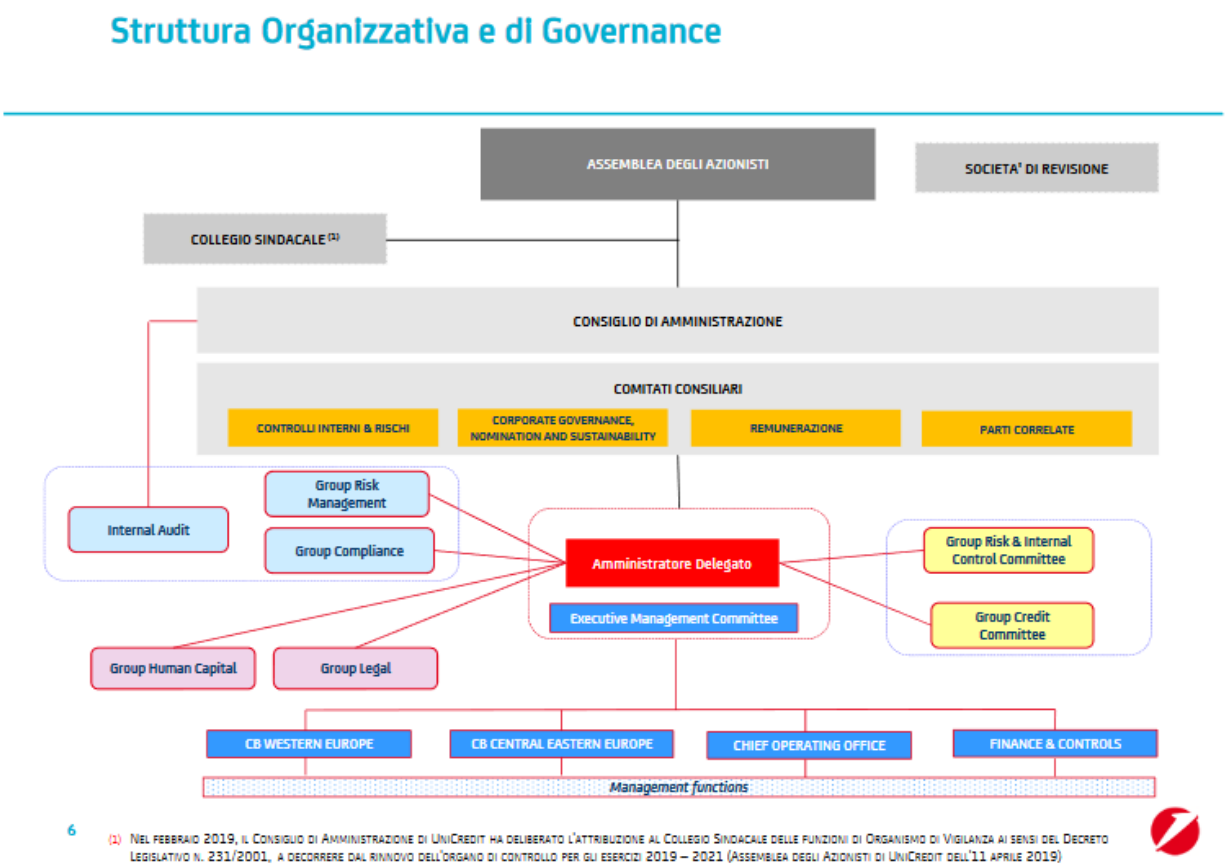


Figura 3: Unicredit Corporate Governance Overview 2020

1) Per quanto riguarda il primo criterio di valutazione, cioè la composizione del Consiglio di amministrazione, è necessario rilevare che Unicredit, in ottemperanza a quanto previsto dalle Disposizioni di Vigilanza per le banche, ha un Consiglio di amministrazione composto da 15 membri di cui un presidente e un vice presidente.

L'unico membro esecutivo del Consiglio è l'Amministratore Delegato; dunque, la componente non esecutiva rappresenta il 93% del Consiglio.

Con riferimento al numero di amministratori indipendenti, nel rispetto delle previsioni della Circolare 285/2013, Unicredit ha individuato nell'art. 20 dello Statuto i criteri di indipendenza, in attuazione dell'art. 3 del Codice di autodisciplina e dell'art. 148 del Testo Unico della Finanza. Gli

amministratori indipendenti risultano essere 11 ai sensi dello Statuto e del Codice di autodisciplina e 13 ai sensi del TUF, rappresentando complessivamente il 79% del Consiglio di amministrazione.
Per quanto riguarda i requisiti di esperienza professionale e di competenza, i consiglieri devono essere scelti tra candidati che abbiano competenze acquisite ricoprendo posizioni dirigenziali (Amministratore Delegato, Direttore Generale e altre posizioni inferiori a queste di un livello gerarchico al massimo) per almeno tre anni negli ultimi dieci nelle aree di *banking business*, *banking governance*, governo dei rischi e sistemi di controllo, competenze legali e societarie, contabilità e bilancio, *audit*, mercati finanziari e internazionali.
Unicredit rispetta i limiti al cumulo di incarichi previsti dalla direttiva CDR IV: 8 amministratori ricoprono più di un incarico; il massimo di incarichi ricoperti è 3.
Riguardo al tempo dedicato agli incarichi, si rileva che nel 2019 la media delle riunioni è stata di 18 riunioni del Consiglio di amministrazione, 15 riunioni del Comitato Corporate Governance, Nomination and Sustainability, 17 riunioni del Comitato per i Controlli Interni & Rischi, 12 riunioni del Comitato Remunerazione e 11 riunioni del Comitato Parti Correlate ed Investimenti in Equity, con una partecipazione media del 95%.
Per la valutazione del requisito della diversificazione, si rileva che il Consiglio di amministrazione presenta il 64% di amministratori con età compresa tra 50 e 65 anni, il 22% di amministratori con più di 65 anni e il 14% di amministratori con meno di 50 anni. Sotto il profilo dell'età, sembrerebbe che la percentuale di consiglieri con età compresa tra i 50 e i 65 anni sia troppo ampia, mentre risulti troppo bassa quella dei consiglieri con meno di 50 anni; sotto tale aspetto, l'organo di gestione potrebbe essere diversificato in modo più efficiente.
Sotto il profilo della diversificazione di genere, il Consiglio di amministrazione di Unicredit è composto per il 64% da uomini e per il 36% da donne, rispettando il requisito minimo previsto dalla Legge n. 120 del 12 luglio 2011, che ha modificato l'art. 147 –ter del TUF.
Anche il profilo della diversificazione per area geografica potrebbe essere migliorato essendo il Consiglio di amministrazione attualmente costituito per il 71% da consiglieri italiani e per il 29% da consiglieri di altri paesi (tra cui Austria, Emirati Arabi e Spagna).
Dal punto di vista delle competenze, gli amministratori risultano possedere le competenze prestabilite dal Consiglio: in particolare, ogni consigliere possiede competenze in almeno 4 aree di competenza individuate dal Consiglio (*banking business*, *banking governance*, governo dei rischi e sistemi di controllo, competenze legali e societarie, contabilità e bilancio, *audit*, mercati finanziari e internazionali).
2) Il secondo criterio di valutazione è relativo alle procedure di nomina. Si rileva che le procedure di nomina risultano in modo chiaro dallo Statuto di Unicredit. Gli amministratori sono nominati

dall'Assemblea e restano in carica per tre esercizi. La nomina avviene sulla base di liste presentate dal Consiglio di amministrazione o dagli azionisti in possesso di almeno lo 0,5% del capitale; i candidati presentati devono rispettare i profili quantitativi e qualitativi individuati ex ante dal Consiglio di amministrazione.

3) In relazione alle politiche di remunerazione, Unicredit prevede, nel rispetto delle Disposizioni di Banca d'Italia, che il rapporto tra componente variabile e componente fissa sia pari a 2:1. In ottemperanza alle Disposizioni, la remunerazione dei consiglieri non esecutivi e del Collegio sindacale è rappresentata solo dalla componente fissa; per l'Amministratore Delegato è prevista una remunerazione con componente fissa e componente variabile nel limite del rapporto pari a 2:1.

4) Come previsto dalla normativa, Unicredit ha istituito 4 comitati diversificati per settore di competenza: il Comitato per i Controlli interni e Rischi, il Comitato Corporate Governance, Nomination and Sustainability, il Comitato Remunerazione e il Comitato Parti Correlate. Nel rispetto delle Disposizioni di Vigilanza, tutti comitati sono composti da 3 o 4 membri tutti non esecutivi e indipendenti.

5) Per quanto riguarda la valutazione del sistema di controllo interno, è articolato sui tre livelli tipici di controllo: controlli di primo livello, controlli di secondo livello (*Compliance* e *Risk Management*) e controlli di terzo livello (*Internal Audit*). Coinvolge tutti gli organi societari, ognuno per le rispettive competenze. Le funzioni di controllo sono ben distinte e tutte riportano direttamente al Consiglio di amministrazione. Il processo di gestione dei rischi è ben definito in tutte le sue fasi anche con riguardo ai processi ICAAP e ILAAP.

6) L'ultimo aspetto oggetto di valutazione è relativo al funzionamento dei flussi informativi. Unicredit garantisce un flusso di informazioni regolare tra gli organi aziendali, in particolare tra il Consiglio di amministrazione e il Collegio sindacale e tra i Comitati e il Consiglio di amministrazione. L'Amministratore delegato riferisce al Consiglio tutte le informazioni che gli pervengono dalle varie strutture della banca e dal management che ha ricevuto deleghe dallo stesso.

Il *Group Compliance*, il *Group Risk Management* e l'*Internal Auditing* devono trasmette relazioni periodiche al Collegio sindacale e flussi periodici agli altri organi aziendali in base alle rispettive competenze[109].

[109]Per approfondimenti sui dati e le informazioni riportate cfr. Documenti societari di Unicredit: Relazione sul governo societario, Composizione qualitativa e quantitativa di Unicredit, Regolamento degli organi aziendali e dei comitati e Statuto sociale.

UBI Banca

UBI Banca ha adottato il sistema di amministrazione e controllo "monistico" che si basa sulla presenza di un Consiglio di amministrazione e di un Comitato per il controllo sulla gestione, costituito da alcuni dei membri del Consiglio di amministrazione, come rappresentato in Figura 4.

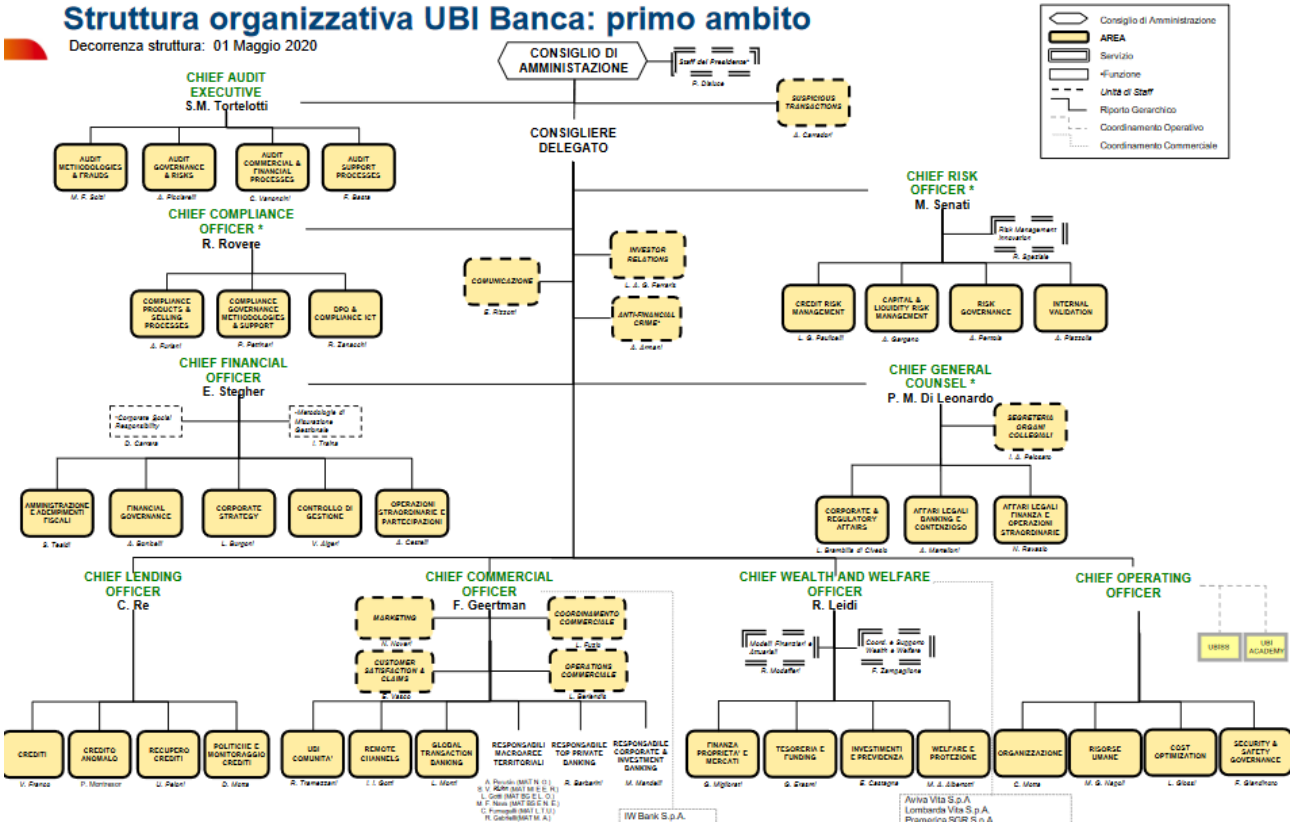


Figura 4: Corporate Governance, Organigramma in www.ubibanca.it

1) In riferimento al primo criterio di valutazione, il Consiglio di amministrazione di UBI Banca è composto da 15 membri tra cui sono ricompresi i 5 membri del Comitato per il controllo sulla gestione, in ottemperanza alle Disposizioni di Vigilanza che per il sistema monistico prevedono un limite di 19 membri.

I consiglieri non esecutivi sono 14 su 15, essendo l'Amministratore delegato l'unico consigliere esecutivo, mentre 10 su 15 sono i consiglieri indipendenti ai sensi dell'art. 148 del TUF e 26 del TUB, nel rispetto delle Disposizioni di Vigilanza che prevedono che almeno un quarto dei componenti sia in possesso dei requisiti di indipendenza. I membri del Comitato per il controllo sulla gestione sono tutti indipendenti.

In relazione ai requisiti di professionalità e competenza, si rileva che gli amministratori devono aver ricoperto il ruolo di presidente per almeno un triennio o svolto per almeno un quinquennio attività di amministrazione e/o supervisione strategica, direzione o controllo in

- banche, società finanziarie, società di gestione del risparmio o compagnie di assicurazione;
- autorità pubbliche indipendenti;
- imprese finalizzate alla produzione e/o allo scambio di beni o servizi che abbiano superato, per i periodi di carica previsti dal presente comma, due dei seguenti limiti: (a) 20 milioni di euro di attivo dello stato patrimoniale; (b) 40 milioni di euro di ricavi delle vendite e delle prestazioni; (c) 250 dipendenti occupati in media durante l'esercizio calcolati sui dati dell'ultimo bilancio approvato ovvero, se redatto, del bilancio consolidato;
- società con azioni negoziate in un mercato regolamentato italiano o estero.

In alternativa ai requisiti sopra richiamati, possono essere eletti anche candidati che siano professori universitari di ruolo da almeno un quinquennio in materie giuridiche o economiche o scienze matematiche/statistiche/ingegneria gestionale; o ancora che siano o siano stati iscritti da almeno un decennio nell'Albo professionale dei Dottori Commercialisti, Notai o Avvocati. Per il presidente del Consiglio di amministrazione e del Comitato per il controllo sulla gestione e per l'Amministratore delegato i limiti temporali sopra richiamati si innalzano a dieci anni.

Per quanto riguarda i limiti al numero degli incarichi, UBI Banca applica i limiti previsti dalla direttiva CRD IV (1 incarico esecutivo e 2 non esecutivi o 4 incarichi non esecutivi).

In relazione al tempo dedicato all'incarico, si rileva che nel 2019 le riunioni sono state 22 per il Consiglio di amministrazione con un tasso di partecipazione del 99,1%, 26 per il Comitato per il controllo sulla gestione con un tasso di partecipazione del 98,5%, 16 per il Comitato nomine con un tasso di partecipazione del 98,8%, 10 per il Comitato remunerazione con un tasso di partecipazione del 100%, 21 per il Comitato rischi con un tasso di partecipazione del 96,8% e 12 per il Comitato parti correlate e soggetti collegati con un tasso di partecipazione del 100%.

Con riguardo alla diversificazione, la quota che deve essere riservata al genere meno rappresentato viene rispettata in quanto il Consiglio di amministrazione è composto per il 40% da donne e il Comitato per il controllo sulla gestione è composto per il 60% da donne.

Anche dal punto di vista dell'età, gli organi collegiali sembrano ben diversificati: il Consiglio di amministrazione è composto per il 26,7% da consiglieri di età compresa tra 30 e 50 anni, per il 40% da consiglieri con età compresa tra 50 e 60 anni e per il 33,3% da consiglieri con età superiore a 60 anni; per il Comitato per il controllo sulla gestione le percentuali sono rispettivamente del 40%, del 50% e dello 0%.

Dal punto di vista della diversificazione geografica, vi è un solo componente non italiano.

2) Il secondo criterio di valutazione è relativo alle procedure di nomina. Si rileva che tali procedure sono esplicate in modo chiaro e trasparente nello Statuto di UBI Banca e che le nomine degli amministratori avvengono ad opera dell'Assemblea sulla base di liste presentate dai Soci.

3) Le politiche di remunerazione prevedono per l'Amministratore delegato una componente fissa per il 48% e una componente variabile, legata alla performance e ad obiettivi annuali e di medio-lungo termine, del 52%. Per gli altri organi la remunerazione è stabilita in misura fissa.
4) In conformità con quanto previsto dalle Disposizioni di Vigilanza, UBI Banca ha previsto 4 comitati. Il primo è il Comitato nomine composto da 5 membri tutti non esecutivi e 3 di questi (tra cui il presidente) indipendenti. Il secondo è il Comitato remunerazioni costituito da 3 membri non esecutivi e 2 di questi (tra cui il presidente) indipendenti. Il terzo Comitato è quello rischi che è composto da tre membri tutti non esecutivi e indipendenti. Il quarto è il Comitato parti correlate e soggetti collegati composto da tre membri tutti indipendenti.
5) Il sistema dei controlli interni risulta nel complesso adeguato ed efficiente. Innanzitutto, la struttura dei controlli consente di diffondere a tutti i livelli dell'organizzazione una corretta cultura dei rischi e dei controlli in quanto non coinvolge solo le funzioni di controllo ma anche tutti gli organi aziendali e il personale ai vari livelli. Si rileva una netta separazione di ruoli tra i tre livelli delle funzioni di controllo. I controlli di secondo livello, che comprendono *Risk Management*, *Compliance* e funzione Antiriciclaggio, sono di responsabilità, rispettivamente, del *Chief Risk Officer* (CRO), del *Chief Compliance Officer* (CCoO) e del Responsabile Antiriciclaggio, tutti con riporto gerarchico al Consigliere delegato e riporto funzionale al Consiglio di amministrazione. La funzione di *Risk Management* prevede tante strutture quante sono le aree di rischio (es. *Credit Risk Management*, *Capital and Liquidity Risk Management*, *Risk Governance*) e i responsabili di ciascuna di tali aree di rischio riportano direttamente al CRO. Quest'ultimo è responsabile dell'attuazione delle politiche di governo e gestione del rischio nel rispetto della propensione al rischio declinata nel RAF e deve presidiare i processi ICAAP e ILAAP, che risultano ben definiti, e in generale il processo di valutazione dei rischi ai fini del *Supervisory Review and Evaluation Process* (SREP).
I controlli di terzo livello (*Internal Auditing*) sono affidati al Responsabile della funzione di *Internal Audit* che riporta gerarchicamente al Consiglio di Amministrazione e funzionalmente al Comitato per il controllo sulla gestione. Gli esiti degli interventi di *audit* sono oggetto di rendicontazione da inviare al Consiglio di amministrazione e al Collegio sindacale, anche delle controllate.
6) Per quanto riguarda il sistema informativo, si rileva che sono garantiti regolari flussi informativi tra il Consiglio di amministrazione e il Consigliere Delegato e tra il Consiglio e gli altri organi e funzioni di controllo. Nell'ambito del sistema dei controlli interni sono previsti specifici sistemi informativi e modalità di coordinamento[110].

[110] Per approfondimenti sui dati riportati cfr. UBI Banca – Relazione sul governo societario e gli assetti proprietari, UBI Banca – Statuto sociale, Relazione sulle politiche di remunerazione, Documento sulla composizione quali-quantitativa del Consiglio di amministrazione.

Mediobanca

Mediobanca ha adottato il modello tradizionale di corporate *governance* basato sul Consiglio di amministrazione e sul Collegio sindacale, nominati dall'Assemblea, come rappresentato il Figura 5.

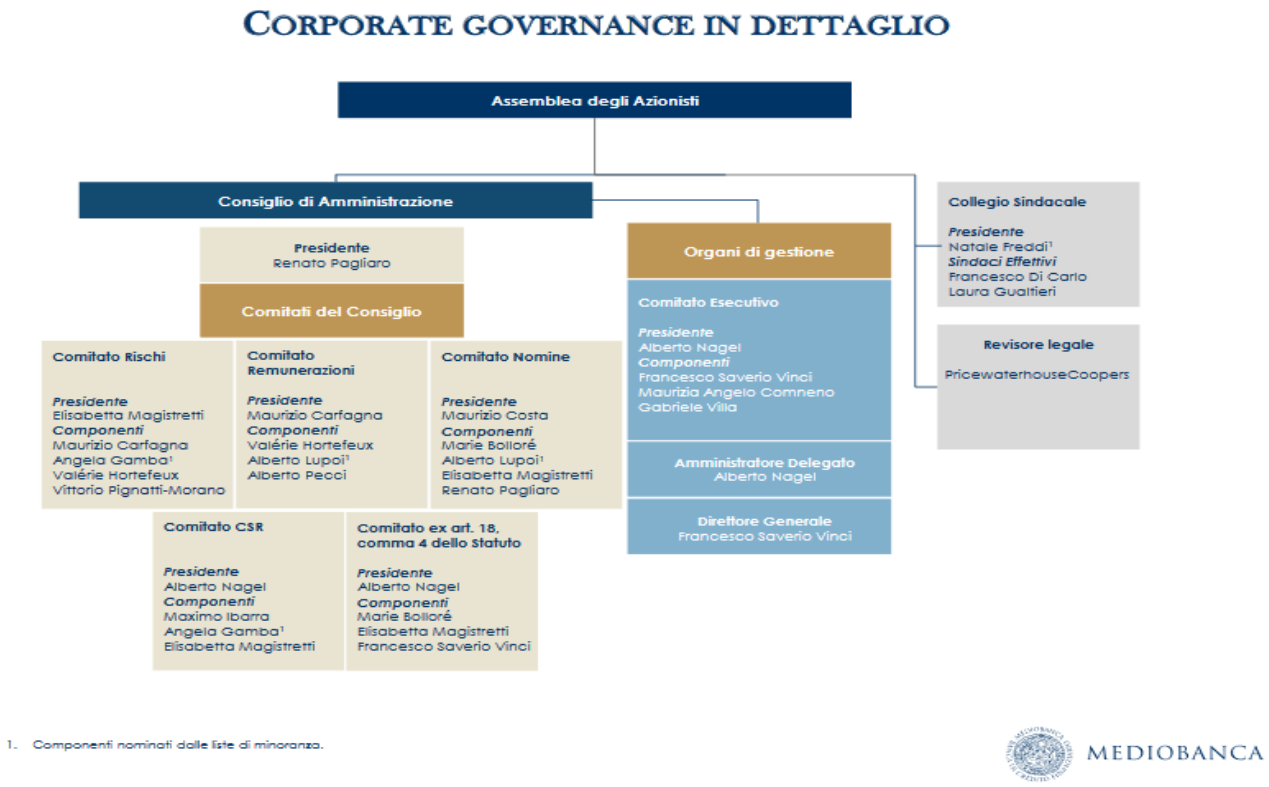


Figura 5: "Mediobanca Corporate Governance – Executive summary 2019"

1) Il Consiglio di amministrazione è composto da 15 membri di cui un presidente, due vice presidenti, un amministratore delegato e un direttore generale (gli ultimi due, insieme ad un vice presidente e ad un amministratore, compongono il comitato esecutivo). Gli amministratori non esecutivi sono 11 su 15 e quelli indipendenti sono 8 ai sensi dell'art. 19 dello Statuto e 11 ai sensi dell'art. 148 del TUF. Con riferimento ai requisiti di professionalità e alle competenze, gli amministratori devono essere in possesso di conoscenze di base in materia di mercati finanziari; contesto normativo di riferimento e obblighi giuridici derivanti; programmazione strategica, consapevolezza degli indirizzi strategici aziendali o del piano industriale di un ente creditizio e relativa attuazione; gestione e monitoraggio dei rischi (individuazione, valutazione, monitoraggio, controllo e metodi di attenuazione delle principali tipologie di rischio di un ente creditizio); contabilità e bilancio; valutazione dell'efficacia dei meccanismi di *governance* dell'ente creditizio, finalizzati ad assicurare un efficace sistema di supervisione, direzione e controllo; interpretazione dei dati finanziari di un ente creditizio, individuazione delle principali problematiche nonché degli adeguati presidi e misure sulla base di tali

informazioni. Per l'Amministratore delegato e il Presidente sono richiesti dieci anni di esperienza professionale recente maturata in settori attinenti ai servizi bancari e finanziari, esperienza che deve includere una proporzione significativa di posizioni dirigenziali di alto livello. Per i non esecutivi sono sufficienti tre anni di esperienza professionale specifica maturata di recente in posizioni dirigenziali di alto livello.

Per quanto riguarda il numero di incarichi, sono rispettati i limiti previsti dalla direttiva CRD IV. Infatti, gli incarichi ulteriori a quello in Mediobanca sono ricoperti o in società del Gruppo Mediobanca o collegate al Gruppo oppure in società che non perseguono principalmente obiettivi commerciali; in tali ipotesi, vengono considerati come un unico incarico.

Con riferimento al tempo dedicato agli incarichi, va rilevato che nel 2019 il numero di riunioni è stato: 10 per il Consiglio di amministrazione con una partecipazione del 96%, 31 per il Collegio sindacale con una partecipazione del 97%, 11 per il Comitato esecutivo con una partecipazione del 100%, 11 per il Comitato rischi con una partecipazione del 91%, 8 per il Comitato remunerazione con una partecipazione del 94%, 9 per il Comitato nomine con una partecipazione del 96% e, infine, 10 per il Comitato parti correlate con una partecipazione del 77%.

In relazione alla diversificazione di genere, le donne rappresentano il 33% del Consiglio di amministrazione (5 membri su 15 sono donne). Sotto il profilo dell'età, invece, si rileva che l'età media è 59 anni e che consiglieri con un'età compresa tra i 71 e gli 80 anni sono il 27%, quelli tra 61 e 70 anni sono il 20%, quelli tra 51 e 60 anni sono il 27%, quelli tra 41 e 50 anni sono il 20% e quelli con meno di 40 anni sono il 6%.

2) Le procedure per la nomina degli amministratori sono definite all'art. 15 dello statuto. Il Consiglio di amministrazione viene nominato dall'Assemblea sulla base di liste presentate dal Consiglio o dai soci titolari di almeno l'1% del capitale sociale e tenendo conto della composizione ottimale individuata preventivamente dal Consiglio di amministrazione sia sul piano qualitativo che su quello quantitativo.

3) Per quanto riguarda le politiche di remunerazione, la remunerazione del Consiglio di amministrazione e del presidente è determinata solo in misura fissa senza incentivi legati alle performance della banca. La remunerazione degli amministratori esecutivi (Amministratore delegato e Direttore generale) prevede una componente fissa, una variabile di breve termine ed eventualmente di lungo termine nonché gli altri benefit previsti per il personale (fondo pensione integrativo, polizza sanitaria, welfare aziendale etc.). I Consiglieri dirigenti del Gruppo ricevono, infine, l'emolumento per la carica di amministratore ma non quello per la partecipazione ai Comitati endoconsiliari.

4) Con riferimento ai Comitati endoconsiliari, si rileva che il Comitato esecutivo è composto da 4 membri di cui la metà indipendenti ai sensi dell'art. 148 del TUF. Il Comitato rischi e parti correlate

è composto da 5 consiglieri non esecutivi e indipendenti ai sensi dell'art. 148 del TUF e dell'art. 19 dello Statuto. Il Comitato per le remunerazioni è composto da 4 membri non esecutivi tre dei quali indipendenti (tra cui il presidente). Il Comitato nomine è costituito da 5 consiglieri non esecutivi di cui tre indipendenti (compreso il presidente).

5) Il sistema di controllo interno risulta basato sulle tre linee di controllo: controlli di linea, controlli di secondo livello (*Risk Management*, *Compliance*, funzione Antiriciclaggio) e controlli di terzo livello (*Internal Audit*). Le tre funzioni sono ben definite e indipendenti. Le funzioni di *Compliance* e di Antiriciclaggio sono sottoposte ad un unico responsabile che riporta all'Amministratore delegato. La funzione di *Risk Management* è presieduta dal *Chief Risk Officer* che riporta all'Amministratore delegato e definisce le politiche di gestione dei rischi, comprese quelle relative ai processi ICAAP e ILAAP. La funzione di *Internal Audit* è accentrata in Mediobanca ma si estende a tutte le società del gruppo o direttamente oppure coordinando le corrispondenti funzioni delle controllate. Il Responsabile della funzione di *Audit* riporta direttamente al Consiglio di amministrazione.

6) Per quanto riguarda i flussi informativi, tutti gli organi societari devono garantire un buon flusso di informazioni soprattutto verso il vertice. Il Consiglio di amministrazione deve garantire che le informazioni vengano trasferite dall'Amministratore delegato e dai Comitati e deve assicurare le informazioni necessarie all'Organismo di vigilanza[111].

[111] I dati provengono dalla Relazione sul governo societario e gli assetti proprietari, Corporate Governance executive summary 2019, Statuto sociale di Mediobanca, Relazione sulla composizione quali-quantitativa del Consiglio di amministrazione, Remuneration Policy Executive Summary 2019.

Intesa Sanpaolo

Intesa Sanpaolo ha adottato, a partire dal 27 aprile 2016, il modello monistico di amministrazione e controllo, caratterizzato dalla presenza di un Consiglio di amministrazione e di un Comitato per il controllo sulla gestione costituito al suo interno, entrambi nominati in sede assembleare, come rappresentato nella Figura 6.

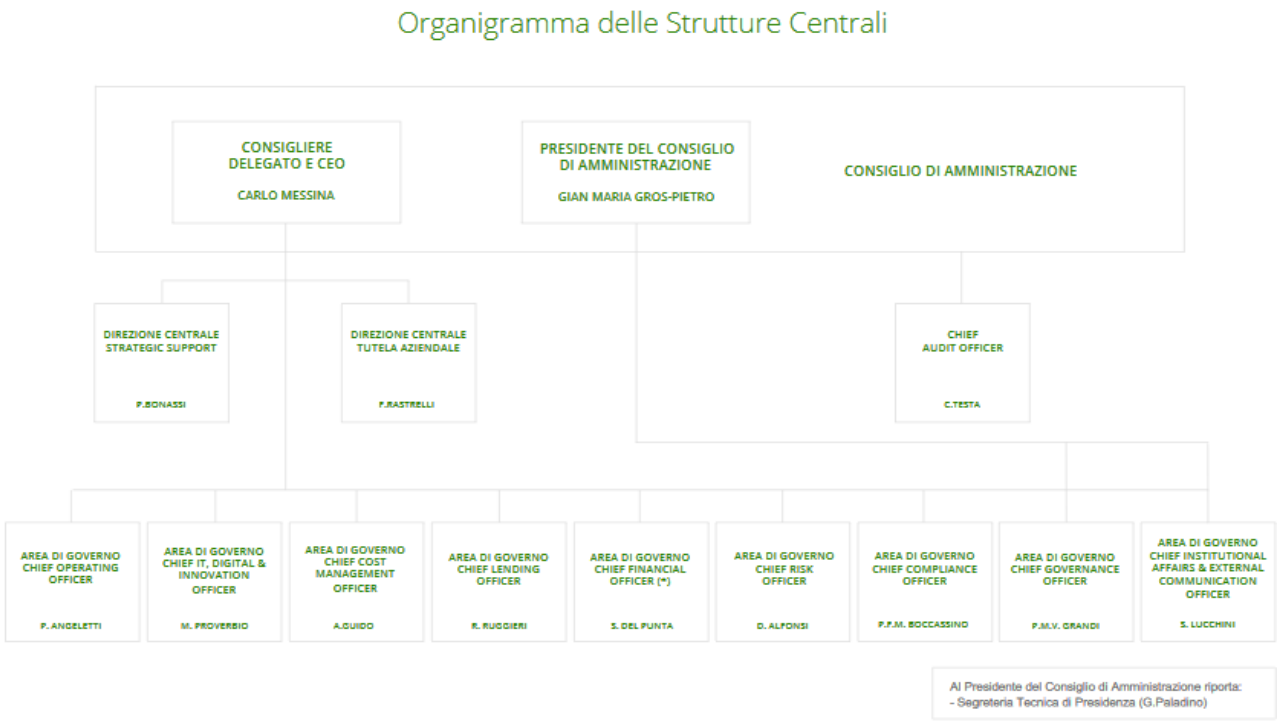


Figura 6: "Intesa Sanpaolo Struttura organizzativa e Top Management"

1) In relazione al primo criterio sulla composizione del Consiglio di amministrazione, si rileva che questo è composto da 19 membri tra cui sono compresi anche i 5 membri del Comitato per il controllo sulla gestione. L'unico amministratore esecutivo è l'Amministratore delegato, mentre gli indipendenti sono 15 su 19 (i membri del Comitato per il controllo sulla gestione sono tutti indipendenti).

Con riferimento alla professionalità e alle competenze richieste, si ha riguardo a conoscenze complessive del business bancario e delle strategie tipiche del settore e delle tecniche di valutazione e di gestione dei rischi connessi all'esercizio dell'attività bancaria, adeguata alla complessità della Banca; dei mercati finanziari e del sistema economico-finanziario; della regolamentazione nel settore bancario e nelle attività finanziarie; di orientamento e programmazione strategica (capacità di comprensione dello scenario di medio-lungo termine della Banca e del settore e relative opzioni strategiche); esperienza di gestione imprenditoriale e/o manageriale ed aziendale. Oltre alle esperienze, conoscenze e competenze sopra indicate si privilegiano esperienze internazionali e/o di

multinazionali e/o conoscenze dei mercati esteri nonché di figure professionali di eccellenza del mondo dei docenti universitari, dei consulenti aziendali o dei liberi professionisti.
Per i componenti del Comitato per il Controllo sulla Gestione sono previsti requisiti addizionali che riguardano conoscenza e capacità applicative di modelli e metodologie di individuazione e misurazione quantitativa dei rischi che caratterizzano l'attività della banca e, ancora, conoscenza dei temi e esperienza di vigilanza su aspetti statutari, di *governance*, regolatori e normativi.
Per quanto riguarda i limiti al cumulo degli incarichi, vi sono consiglieri che hanno più di un incarico ma si ritengono rispettati i limiti di cui alla direttiva CRD IV in quanto si tratta di incarichi ricoperti o in società del Gruppo o collegate al Gruppo oppure in società che non perseguono principalmente obiettivi commerciali; in tali ipotesi, vengono considerati come un unico incarico.
Il tempo dedicato all'incarico da parte degli amministratori si può rilevare sulla base delle riunioni svolte che nell'ultimo anno sono state 26 per il Consiglio di amministrazione, 48 per il Comitato per il controllo sulla gestione, 42 per il Comitato rischi, 19 per il Comitato per le operazioni con parti correlate, 22 per il Comitato remunerazioni e 6 per il Comitato nomine.
Il Consiglio di amministrazione risulta composto da 7 donne e 12 uomini e, sotto il profilo dell'età, è costituito per il 10,5% da consiglieri con meno di 50 anni, per il 58% da consiglieri con un'età compresa tra 51 e 65 anni e per il 31,5% da consiglieri con più di 65 anni.
2) Le procedure di nomina, ben definite nello statuto di Intesa Sanpaolo, prevedono che i componenti del Consiglio di amministrazione sono nominati dall'assemblea sulla base di liste presentate dai soci titolari di almeno lo 0,5% del capitale rappresentato da azioni ordinarie. I candidati presentati nelle liste devono essere in possesso dei requisiti di professionalità, onorabilità, competenza, correttezza, dedizione di tempo e limiti al cumulo di incarichi.
3) La remunerazione è determinata dall'Assemblea in misura fissa per i componenti del Consiglio di amministrazione, per l'intero loro periodo di carica, e, inoltre, prevedendo un compenso additivo per la carica di Presidente e di Vice-Presidente. Spetta al Consiglio di amministrazione, su proposta del Comitato remunerazioni, stabilire, in aggiunta al compenso determinato dall'Assemblea, la remunerazione dei componenti il Consiglio che ricoprono ulteriori particolari cariche in conformità dello Statuto. La remunerazione spettante al Consigliere delegato e al Direttore generale, oltre alla componente fissa prevede anche una misura variabile, in coerenza con le politiche di remunerazione approvate dall'Assemblea.
4) Nel rispetto delle Disposizioni di Vigilanza per le banche, Intesa Sanpaolo presenta quattro comitati endoconsiliari. Si tratta del Comitato nomine costituito da 5 componenti di cui, oltre il Presidente, altri 2 indipendenti. Il Comitato remunerazioni è costituito da 5 componenti di cui, oltre il Presidente, altri 2 indipendenti. Il Comitato rischi costituito da 5 componenti di cui, oltre il

Presidente, altri 2 indipendenti. Infine, il Comitato per le operazioni con parti correlate e soggetti correlati del Gruppo costituito da 5 componenti tutti indipendenti.

5) Il sistema di controllo interno è caratterizzato dalla separazione dei tre livelli delle funzioni di controllo. I controlli di secondo livello - funzione di *Risk Management* e funzione di *Compliance* - fanno capo rispettivamente al *Chief Risk Officer* e al *Chief Compliance Officer*, i quali operano a diretto riporto del Consigliere delegato e hanno accesso diretto agli organi aziendali. La funzione di *Internal Auditing* è presieduta dal Responsabile dell'IA che riporta direttamente al Consiglio di amministrazione e funzionalmente al Comitato per il controllo sulla gestione.

6) Per quanto riguarda il sistema informativo, anche in Intesa Sanpaolo vengono garantiti flussi informativi che si diffondono a tutti i livelli dell'organizzazione. Soprattutto le funzioni di controllo necessitano di un forte coordinamento tra loro e con gli organi aziendali e a tal fine vengono implementati strumenti di informazione che operano in continuità sia in senso verticale che in senso trasversale[112].

2.4 Risultati della valutazione a confronto

Sulla base della valutazione svolta, si rileva che la struttura di governo societario e dei controlli interni delle quattro banche esaminate non presenta profili critici di rilevante gravità. Nonostante questo, è possibile individuare diversi elementi che influenzano negativamente la complessiva valutazione sulla *governance* e che sono suscettibili di miglioramento.

Il primo profilo è rappresentato dalle dimensioni del Consiglio di amministrazione. A tal proposito, pur prendendo atto della tendenza delle banche analizzate a diminuire il numero di componenti del Consiglio (es. Mediobanca è passata da 18 a 15 membri e Unicredit da 17 a 15 membri), si ritiene che possano esservi ulteriori margini di miglioramento. Infatti, 3 delle 4 banche oggetto di valutazione presentano un numero di amministratori corrispondente al limite massimo previsto dalle Disposizioni di Vigilanza: Mediobanca e Unicredit presentano un Consiglio di amministrazione di 15 membri pari al limite previsto per le banche che adottano il sistema tradizionale, mentre Intesa Sanpaolo ha un Consiglio di 19 membri corrispondente al limite previsto per il sistema monistico. Questi numeri, se da un lato risultano giustificati dalle dimensioni e dalla complessità operativa delle banche in questione, dall'altro lato a lungo andare possono causare problemi di coordinamento e comunicazione tra i membri nonché prolungamenti delle procedure decisionali. In conclusione, nella consapevolezza che non sia possibile individuare preventivamente un numero ottimale di amministratori, dovendo questo essere adattato alle caratteristiche specifiche della banca, si ritiene che, con specifico

[112] I dati riportati provengono dalla Relazione su governo societario e assetti proprietari di Intesa Sanpaolo, Statuto sociale, Relazione sulla composizione qualitativa e quantitativa del Consiglio di amministrazione.

riferimento alle quattro banche analizzate, il numero dei componenti sia da ridurre ulteriormente per evitate riflessi negativi sulla funzionalità delle banche.

Il secondo elemento che presenta margini di miglioramento è relativo alla diversificazione del Consiglio di amministrazione. Sotto il profilo della diversità di genere, si rileva che nelle 4 banche esaminate viene rispettato il requisito minimo, pari a 1/3, previsto dalla Legge n. 120 del 12 luglio 2011, che ha modificato l'art. 147 –ter del TUF. Tuttavia, si può osservare che la percentuale di donne nei Consigli si attesta intorno alla percentuale minima richiesta dalla normativa e solo in un caso vi è una donna a ricoprire la carica di presidente del Consiglio di amministrazione (UBI Banca), mentre nessuna donna ricopre la carica di amministratore delegato. Anche sotto il profilo dell'età, la composizione del Consiglio di amministrazione potrebbe essere meglio diversificata. Dall'osservazione delle percentuali delle banche, risulta che l'età media si attesta intorno ai 59 anni, mentre si ritiene troppo elevata la percentuale di amministratori con più di 65 anni e troppo ridotta la percentuale di amministratori con meno di 50 anni. Infatti, se da una parte gli amministratori con un'età superiore a 65 anni sono garanzia di professionalità ed esperienza, dall'altra col tempo la loro influenza potrebbe compromettere l'indipendenza. Nello stesso tempo, una percentuale più elevata di amministratori più giovani può contribuire ad apportare competenze ed esperienze più prossime al presente e relative a contesti finanziari più attuali. L'affiancamento di queste competenze a figure di vertice con esperienze più significative, maturate sia sotto il profilo strategico che sotto il profilo professionale, potrebbe rappresentare un reale fattore di successo della *governance* delle banche.

Con riguardo al sistema dei controlli interni, si è osservato che nelle banche oggetto di valutazione risultano ben definite e separate le funzioni di controllo sia sul piano organizzativo che sul piano delle responsabilità. Tuttavia, si ritiene che per quanto riguarda la gestione dei rischi, soprattutto in ottica SREP, vadano ulteriormente implementati meccanismi di individuazione dei rischi di liquidità e di capitale che rappresentano una delle principali cause di perdite registrate dalle banche. Allo stesso modo, tali banche devono costantemente migliorare i propri flussi informativi attraverso l'adozione di sistemi, anche informatici, aggiornati ed evoluti che consentano di comunicare in maniera celere e diretta con i vertici.

A seguito di tali osservazioni, si può concludere che le quattro banche oggetto di valutazione, pur presentando un buon grado di adeguatezza ed efficienza della *governance* e del sistema dei controlli interni, evidenziano diversi spazi di miglioramento, come sopra individuati. Tale valutazione si riflette, in termini numerici, in un punteggio "SREP" pari a 3.

3. Considerazioni conclusive

Le osservazioni delineate nelle pagine che precedono hanno l'obiettivo di verificare come la normativa relativa alla vigilanza prudenziale e al *Supervisory Review and Evaluation Process* abbia influito sui sistemi di governo e di controllo delle banche. Si è osservato, innanzitutto, che le banche vengono coinvolte direttamente nella prima fase di tale processo relativa ai processi di valutazione dell'adeguatezza patrimoniale (ICAAP) e di valutazione dell'adeguatezza della liquidità (ILAAP). In relazione a tali processi si è evidenziato, in particolare, il ruolo del sistema di controllo interno e della funzione di *Internal Auditing*. Si è visto poi che la valutazione condotta nell'ambito dello SREP ha ad oggetto quattro aree della banca: il modello imprenditoriale, la *governance* e la gestione del rischio, i rischi di capitale e i rischi di liquidità. In particolare, la *governance* e il sistema dei controlli interni sono stati descritti nel dettaglio e selezionati come criterio di valutazione di quattro banche italiane *significant* e quotate. Queste banche sono state analizzate con specifico riferimento agli aspetti di governo societario e di controllo interno e valutate sulla base dei requisiti SREP relativi alla *governance*. Come visto nel paragrafo riguardante i risultati della valutazione, i sistemi di governo e di controllo delle quattro banche esaminate evidenziano diverse aree con margini di miglioramento, pur non presentando profili di estrema gravità. Questa valutazione ha condotto all'assegnazione di un punteggio in ottica SREP pari a 3. Si tratta, dunque, di un punteggio che rileva aree di rischio associate a profili di criticità delle strutture di *governance*.

Il punteggio assegnato sembrerebbe coerente con i risultati SREP relativi al 2019 che hanno evidenziato profili di deterioramento della *governance* e lacune nei sistemi di controllo interno tanto che a tre banche su quattro è stato assegnato un punteggio pari a 3 e solo il 18% delle banche ha ottenuto un punteggio pari a 2, facendo registrare un peggioramento rispetto al 2018.

Nonostante i punteggi non del tutto positivi, i risultati della valutazione svolta testimoniano una tendenza delle banche ad adeguare i propri assetti di *governance* alle previsioni della normativa di vigilanza bancaria e rispecchiano la crescente attenzione posta dalle banche al rispetto dei requisiti SREP.

In conclusione, si ritiene che la vigilanza svolta nell'ambito dello SREP possa rappresentare un incentivo affinché le banche implementino strutture di governo societario e di controllo interno sempre più adeguate ed efficienti.

RIFERIMENTI BIBLIOGRAFICI

AA. VV., *L'interesse sociale tra valorizzazione del capitale e protezione degli stakeholders, In ricordo di Pier Giusto Jaeger*. Atti del Convegno. Milano, 9 ottobre2009, *Quaderni di Giurisprudenza Commerciale*, Milano, 2010.

AA.VV., *Commento agli artt. 2409-octies-2409-quaterdecies*, in MARCHETTI P.,BIANCHI L.A., GHEZZI F., NOTARI M., (diretto da), *Commentario alla riforma del diritto societario*, Milano, 2005.

ABRIANI N., *Collegio sindacale e «Comitato per il controllo interno e la revisione contabile» nel sistema policentrico dei controlli*, in TEDESCHI C. (a cura di), *Saggi sui grandi temi della Corporate Governance,* Milano, 2013 e in Riv. dir. soc., 2013.

ABRIANI N., voce Sistema monistico, in ABRIANI N. (a cura di), *Società e fallimento*, Milano, 2008.

ALVARO S., CICCAGLIONI P., SICILIANO G., *L'autodisciplina in materia di corporate governance,* in *Quaderni giuridici della Consob*, 2013.

ALVARO S., D'ERAMO D., GASPARRI G., *Modelli di amministrazione e controllo nelle società quotate*, in Quaderni Giuridici Consob, 2015.

AMBROSINI S., *Commento sub artt. 148-154,* in COTTINO G., *La legge Draghi e le società quotate in borsa*, Torino, 1999.

ABBADESSA P. (a cura di), *Dialogo sul sistema dei controlli nelle società*, Torino, 2015.

ASSOCIAZIONE BANCARIA ITALIANA, Disposizioni Banca d'Italia. Nuovo sistema dei controlli interni. Riflessioni sul capitolo VII per la Gap Analysis, Roma, 30 ottobre 2013.

ASSOCIAZIONE DEI COMPONENTI DEGLI ORGANISMI DI VIGILANZA, Osservazioni dell'Associazione dei Componenti degli Organismi di Vigilanza ex D. Lgs. 231/2001 in relazione al ruolo dell'Organismo di Vigilanza, Milano, 31 ottobre 2012.

BANCA D'ITALIA, Istruzioni di vigilanza per le banche, Circ. n. 229 del 21/4/1999.

BANCA D'ITALIA, Nuove disposizioni di vigilanza prudenziale per le banche, Circ. n. 263 del 27/12/2006.

BANCA D'ITALIA, Disposizioni di vigilanza in materia di organizzazione e governo societario delle banche, 4 marzo 2008.

BANCA D'ITALIA, Nota di chiarimenti in materia di governance, 19 febbraio 2009.

BANCA D'ITALIA, Applicazione delle disposizioni di vigilanza in materia di organizzazione e governo societario delle banche, 11 gennaio 2012.

BANCA D'ITALIA, Documento per la consultazione. Disposizioni di vigilanza prudenziale per le banche. Sistema dei controlli interni, sistema informativo e continuità operativa, 4 settembre 2012.

BANCA D'ITALIA, Disposizioni di vigilanza prudenziale per le banche in materia di sistema dei controlli interni, sistema informativo e continuità operativa. Relazione sull'analisi d'impatto, giugno 2013.

BANCA D'ITALIA, Bollettino di vigilanza n. 7, luglio 2013.

BANCA D'ITALIA, Sintesi per gli utenti. Nuove disposizioni di vigilanza prudenziale per le banche (Circ. n. 263 del 27 dicembre 2006) - 15° aggiornamento sistema dei controlli interni, sistema informativo e continuità operativa, 24 gennaio 2014.

BANCA D'ITALIA, Il sistema dei controlli interni, il sistema informativo e la continuità operativa. Nota di chiarimenti, 24 gennaio 2014 aggiornata il 6 giugno 2014.

COLA C., *Le novità per la funzione di compliance e la gestione ed il controllo del rischio fiscale*, intervento al Convegno Unione Fiduciaria S.p.a., "*Provvedimento di Banca d'Italia del 2 luglio 2013. Le nuove regole sul sistema dei controlli interni, sistemi informativi e continuità operativa*", Milano, 1 ottobre 2013.

COMMITTEE OF EUROPEAN BANKING SUPERVISORS, Guidelines on outsourcing, 14 dicembre 2006.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION, Internal Control. Integrated Framework, New York, dicembre 1992.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION, Enterprise Risk Management. Integrated Framework: Executive Summary and Framework, New York, settembre 2004.

COMITATO DI BASILEA, Schema per i sistemi di controllo interno nelle organizzazioni bancarie, Basilea, settembre 1998.

COMITATO DI BASILEA, Compliance and the compliance function in banks, Basilea, aprile 2005.

DELLAROSA E., RAZZANTE R., *Il nuovo sistema dei controlli interni della banca*, Milano, Franco Angeli, 2010.

EUROPEAN BANKING AUTHORITY, Guidelines on Internal Governance, settembre 2011.

FERRANDO M., *Banche italiane fuori dal podio nella classifica della governance*, Il Sole 24 ORE, 11 dicembre 2013.

FINANCIAL STABILITY BOARD, Thematic Review on Risk Governance, 12 febbraio 2013.

FINANCIAL STABILITY BOARD, Principles for An Effective Risk Appetite Framework, 18 novembre 2013.

FUMAGALLI M., *Il documento di gap analysis da inviare a Banca d'Italia entro il 31 dicembre 2013 ed il regime transitorio*, intervento al Convegno Unione Fiduciaria S.p.a., "*Provvedimento di Banca d'Italia del 2 luglio 2013. Le nuove regole sul sistema dei controlli interni, sistemi informativi e continuità operativa*", Milano, 1 ottobre 2013.

INSTITUTE OF INTERNAL AUDITORS, Standard for the professional practice of Internal Auditing, Florida, 2004.

INTESA SANPAOLO, Relazione su governo societario e assetti proprietari 2019.

MARANGONI M., *Il provvedimento di Banca d'Italia sul sistema dei controlli interni, impatti e novità*, intervento al Convegno Unione Fiduciaria S.p.a., "*Provvedimento di Banca d'Italia del 2 luglio 2013. Le nuove regole sul sistema dei controlli interni, sistemi informativi e continuità operativa*", Milano, 1 ottobre 2013.

MEDIOBANCA, Relazione su governo societario e assetti proprietari 2019.

METELLI F., FSB: *Principles for An Effective Risk Appetite Framework*, articolo tratto dal sito www.aifirm.it.

METELLI F., *Il sistema di controllo e governo dei rischi. Le novità in materia di Risk Appetite Framework, il ruolo di organi e funzioni aziendali*, intervento al Convegno Unione Fiduciaria S.p.a., "*Provvedimento di Banca d'Italia del 2 luglio 2013. Le nuove regole sul sistema dei controlli interni, sistemi informativi e continuità operativa*", Milano, 1 ottobre 2013.

PRIORI M., GUGLIELMETTI R., *Gli assetti di governo e controllo delle banche: la circolare di Banca d'Italia*, in Osservatorio di diritto bancario del Sole 24 ORE, 11 ottobre 2013.

PRIORI M., GUGLIELMETTI R., *Sistema dei controlli interni: l'organo con funzione di supervisione strategica*, in Osservatorio di diritto bancario del Sole 24 ORE, 23 ottobre 2013.

PRIORI M., GUGLIELMETTI R., *Istituzione e nomina delle funzioni di controllo*, in Osservatorio di diritto bancario del Sole 24 ORE, 19 novembre 2013.

QUASSO F., *L'Internal Audit alla luce delle nuove disposizioni di Vigilanza. Novità ed opportunità*, intervento al Convegno Unione Fiduciaria S.p.a., "*Provvedimento di Banca d'Italia del 2 luglio 2013. Le nuove regole sul sistema dei controlli interni, sistemi informativi e continuità operativa*", Milano, 1 ottobre 2013.

SOTTORIVA C., *Collegio sindacale e sistema dei controlli interni nell'ambito delle aziende di credito alla luce delle nuove disposizioni di vigilanza prudenziale (Banca d'Italia 2 luglio 2013) e della Direttiva 2013/36/UE*, in Rivista di Diritto Bancario, n. 12/2013.

TARANTOLA A. M., *Il sistema dei controlli interni nella governance bancaria*, intervento al Convegno DEXIA Crediop 4° Incontro Compliance, "*Il sistema dei controlli aziendali: alla ricerca di una governance*", Roma, 6 giugno 2008.

UBI BANCA, Relazione sul governo societario e assetti proprietari 2019.

UNICREDIT, Relazione sul governo societario 2019.

Allegato 1

Orientamenti EBA sulla corporate governance

Gli orientamenti sulla governance interna, pubblicati dall'Eba nel 2018 (EBA/GL/2017/11 del 21 marzo 2018) per essere applicati a partire dal 30 giugno 2018, emanati in applicazione dell'articolo 16 del regolamento UE n. 1093/2010, esprimono le prassi di vigilanza che secondo la posizione dell'EBA devono essere seguite all'interno del sistema europeo di vigilanza finanziaria e alle modalità di applicazione del diritto . A tali orientamenti le istituzioni sono tenute a conformarsi salvo comunicare formalmente i motivi di scostamento che, se non giustificatamente motivati, comportano la conseguente valutazione di non conformità dell'istituzione interessata.

In applicazione dell'articolo 74, paragrafo 1 della direttiva 2013/36 UE gli orientamenti dell'EBA delineano i processi, i dispositivi e i meccanismi di governance che gli enti devono attuare con particolare riferimento alla loro struttura organizzativa e alle rispettive linee di responsabilità, nei processi di identificazione, gestione e monitoraggio dei rischi nel quadro di controllo interno.

Il complesso delle linee fornite non esprime valutazioni sulle diverse strutture di consigli né sulla ripartizione generale delle competenze, ed è proprio per questa ragione che esse devono essere seguite dagli organi di amministrazione, così come definiti dalla direttiva 2013/36/UE (articolo 3 paragrafo 1 punti 7 e 8 della direttiva 2013/36/UE) a prescindere dalla tipologia di consiglio adottata monistica, dualistica o altro, organi di amministrazione che sono da considerarsi titolari delle funzioni di gestione , esecutive, e di supervisione strategica , non esecutive.

Negli Stati membri gli organi di amministrazione o i loro delegati alle funzioni esecutive , quindi, agiscono comunque come parte della funzione di gestione dell'organo di amministrazione (ad esempio un amministratore delegato, un team di gestione, un comitato esecutivo), salvo i casi in cui tali funzioni vengano esercitate direttamente dagli azionisti o dai proprietari dell'ente e devono attenersi a tale orientamenti , applicando taluni principi cardine come il principio di proporzionalità previsto dall'articolo 74 paragrafo 2 della direttiva 2013/36 UE, affinchè i dispositivi di governance interna siano coerenti con il principio di rischio individuale, il modello di business dell'ente e perseguire efficacemente gli obiettivi imposti dagli obblighi regolamentari.

Nell'applicazione del principio di proporzionalità, gli enti e le autorità competenti dovrebbero tenere conto delle dimensioni dell'ente, in ottica di totale di bilancio, la collocazione geografica e il volume di attività in ogni paese, la forma giuridica dell'ente e, quando è parte di un gruppo, la proporzionalità in relazione al gruppo di cui è parte. Vanno inoltre valutate le eventuali quotazioni in borsa dell'ente e, se questo è autorizzato a far ricorso a modelli interni per la misurazione dei requisiti patrimoniali, come nelle ipotesi di modelli basati su rating interni. Nell'applicare il principio di proporzionalità

altri criteri da tenere in considerazione sono la tipologia di attività e di servizi autorizzati oggetto dell'attività dell'ente, il modello di business e la strategia di base, la strategia in materia di rischio, la propensione al rischio e l'effettivo profilo di rischio dell'ente, gli assetti proprietari e la struttura di finanziamento dell'ente, la tipologia di clienti (al dettaglio, società, piccole imprese, enti pubblici), eventuali attività esternalizzate e i canali di distribuzione e il complesso dei sistemi informatici cui l'ente fa leva inclusi i sistemi di continuità e le esternalizzazioni di queste aree.

La responsabilità generale dell'ente è attribuita espressamente all'organo di amministrazione dell'ente medesimo dall'articolo 88 della direttiva 2013/36/UE, disposizione che lo chiama a sorvegliare e a rispondere dell'attuazione dei dispositivi di governance all'interno della struttura per garantirne una gestione efficace e prudente. I compiti dell'organo di amministrazione, da definire con chiarezza e trasparenza, dovrebbero confluire in documenti formali approvati dall'organo di amministrazione, i cui componenti dovrebbero avere contezza delle responsabilità e della suddivisione di compiti tra le diverse funzioni dell'organo di amministrazione e dei suoi comitati, anche nell'ottica di assicurare un sistema articolato secondo un sicuro equilibrio di poteri perché il processo decisionale non venga assorbito da un singolo membro o da un nucleo ristretto di suoi membri.

Sinteticamente, le responsabilità dell'organo di gestione dovrebbero incentrarsi sulla definizione, approvazione e sorveglianza della strategia aziendale nel suo complesso e sulle politiche fondamentali dell'ente, anche con riguardo all'ambito dei rischi, alla loro propensione e alla loro gestione; tali responsabilità comportano anche che sia garantita una struttura organizzativa chiara, una gestione dei rischi interna indipendente ed efficiente e che tali responsabilità siano esercitate con autorità, peso e risorse conformi; è inoltre fondamentale che la responsabilità dell'organo di amministrazione valuti e sorvegli il processo di selezione e di idoneità dei titolari di posizione chiave anche in relazione al ruolo la composizione e i compiti di ciascuno di loro e sorvegli per verificare che corra un adeguato flusso di informazioni tra organo di amministrazione, ciascun comitato, autorità competenti e altre parti, compresa la circolazione delle documentazioni riguardanti raccomandazioni, conclusioni e linee di segnalazione. Come accenneremo anche in seguito, altrettanto importante è che un'attenzione particolare sia riservata alla cultura del rischio elaborata dall'ente e a una cultura di valori aziendali che valorizzi il comportamento responsabile ed etico dell'ente medesimo.

Sotto questo profilo, per esempio, è primario sorvegliare affinchè un membro dell'organo di amministrazione preposto al controllo interno non riceva ulteriori mandati che comprometterebbero la sua indipendenza nelle sue attività di controllo interno.

All’organo di amministrazione è inoltre conferita anche una specifica funzione di supervisione strategica volta a sorvegliare e monitorare il processo decisionale, l’attività dell’organo di amministrazione nelle sue funzioni di gestione, l’efficacia della governance interna, l’attuazione degli obiettivi strategici, anche in materia di rischi e l’integrità delle funzioni del controllo interno e delle relazioni finanziarie.

L’organo di amministrazioni, anche nelle sue funzioni di sorveglianza (anche in questo caso si ribadisce dovrebbe essere costituito da membri che dovrebbero essere scelti, fatto salvo il diritto nazionale , secondo gli orientamenti congiunti dell’ESMA e dell’ABE sulla valutazione dell’idoneità dei membri dell’organo gestorio e del personale che riveste ruoli chiave , in conformità delle direttive 2013/36/UE e 2014/65/UE) deve garantire l’indipendenza dei responsabili delle funzioni del controllo interno e monitorare l’attuazione del piano di audit interno.

Il compito di guidare l’organo di amministrazione in questa molteplicità di competenze è attribuito al suo Presidente, responsabile, nella sua complessità, dell’efficacia del suo funzionamento. Dovrebbe trattarsi di un membro non esecutivo che, nella sua funzione di supervisione strategica non deve, contestualmente, esercitare funzioni di amministratore delegato in seno allo stesso ente salvo espressa giustificazione da parte dell’ente medesimo e autorizzazione delle autorità competenti.

All’organo di amministrazione, nella sua funzione di supervisione strategica, è fornita idonea consulenza da parte di specifici comitati , quale il comitato rischi, il comitati nomine (sul punto si rinvia agli orientamenti congiunti dell’ESMA e dell’ABE sulla valutazione dell’idoneità dei membri dell’organo gestorio e del personale che riveste ruoli chiave , in conformità delle direttive 2013/36/UE e 2014/65/UE) e i comitati remunerazioni comitati da costituirsi, , in tutti gli enti rilevanti in considerazione dei loro livelli individuali, sub-consolidati e consolidati; gli enti non rilevanti, invece, anche quando rientrano nell’ambito del consolidamento prudenziale di un ente significativo in una situazione sub-consolidata o consolidata , non sono obbligati ad istituire tali comitati. Dovrebbero essere presieduti da un membro non esecutivo dell’organo di amministrazione per esprimere un giudizio obiettivo. In questa direzione, i membri indipendenti dell’organo di amministrazione nella sua funzione di supervisione strategica dovrebbero essere attivamente coinvolti nei comitati.

Tali comitati dovrebbero avere, a cura dei rispettivi enti, una chiara ripartizione di doveri, compiti e competenze esplicitati in un adeguato mandato documentato da parte dell’organo di amministrazione nella sua veste di supervisore strategico.

Quanto al ruolo peculiare dell’organo di amministrazione in relazione allo specifico quadro di governance dell’ente, innanzitutto dovrebbe garantire, tramite un documento scritto che ne faccia valere anche la imprescindibile trasparenza, una adeguata struttura organizzativa e operativa. In quest’ottica, l’organo di amministrazione dovrebbe assicurare che le funzioni di controllo interno

siano indipendenti dalle linee di business destinatarie del loro controllo, e, a tal fine, preservare un'adeguata separazione delle funzioni, oltre che garantire risorse finanziarie e umane idonee. Anche in questo contesto, le linee di segnalazione e l'attribuzione delle responsabilità dovrebbero essere condotte in modo chiaro, definito, coerente e opportunamente formalizzate in maniera documentale.
Si è detto innanzi, dell'importanza, per l'ente, di una idonea cultura del rischio, relativa all'ente nella sua globalità e sviluppata secondo una completa consapevolezza e in una chiave olistica dei rischi da fronteggiare e da gestire alla luce della propensione dell'ente al rischio.
Accanto a tale aspetto, altro scenario che deve essere attentamente sorvegliato dall'organo di amministrazione è quello del valore aziendale e del codice etico dell'ente, affinchè siano coltivati per l'appunto, elevati standard di professionalità e di etica, e, ove necessario promuovere , tenuto conto delle specifiche caratteristiche dell'ente, ogni iniziativa e misura capace , al meglio di garantire tali valori.
E' precipuo compito dell'organo di amministrazione, inoltre, definire e monitorare il perseguimento di efficaci politiche di contrasto di conflitti di interesse a livello di ente, derivanti dall'attività e dai vari ruoli dell'ente stesso, attraverso , lo abbiamo visto, una conforme separazione dei compiti (esempio affidando a soggetti diversi attività confliggenti in determinate operazioni e/o servizi) e incaricando soggetti diversi di compiti di vigilanza e di informativa sulle possibili attività confliggenti.
Più in generale, gli enti dovrebbero porre in essere procedure interne di segnalazione rivolte al personale per comunicare violazioni effettive o potenziali agli obblighi o interni, compresi quelli di cui al regolamento UE/ 575/2013 e delle leggi nazionali che recepiscono la direttiva 2013/36/UE.
In relazione agli effettivi meccanismi di controllo interno, gli enti dovrebbero allestire un quadro di controlli interni solido e globale, gestendo responsabilmente le linee di business e assicurando un'efficace gestione dei rischi che si presentano nell'espletamento delle loro attività, contrastandoli con la previsione di controllo atti a garantire la conformità delle attività poste in essere nel rispetto dei requisiti interni ed esterni. Il quadro di controllo dovrebbe attraversare l'intera organizzazione e assicurare l'efficace ed efficiente gestione di tutte le operazioni poste in essere, secondo norme di comportamento prudenti, capaci di fronteggiare ogni possibile rischio secondo sane procedure amministrative, tenendo conto di ogni opportuna informazione finanziaria e non finanziaria sia interna che esterna e il rispetto di leggi regolamenti e obblighi di vigilanza.
Il quadro di gestione dei rischi, in particolare, dovrebbe essere disposto a livello dell'intero ente, consolidato e sub-consolidato, per prevedere procedure politiche e misure che garantiscano l'individuazione e quindi i contenimenti dei rischi ove non ne sia possibile la prevenzione ed essere

sottoposto ad una revisione interna indipendente, svolta per esempio dalla funzione di audit interno e rivalutata costantemente.

In sostanza le funzioni di controllo interno dovrebbero essere in grado di assicurare una funzione di gestione dei rischi, una funzione di conformità e una funzione di audit interno e le prime due dovrebbero essere regolarmente revisionate dalla funzione di audit interno.

Anche ove le attività di audit interno dovessero essere esternalizzate, parzialmente o completamente, il responsabile della funzione di controllo interno interessata e l'organo di amministrazione restano responsabili di tali attività del mantenimento di una funzione di controllo interno dell'ente. Fra l'altro i responsabili della funzione di controllo interno dovrebbero rivestire un adeguato livello gerarchico, tale da conferire la giusta autorità adeguata ad esercitare le proprie responsabilità con peso adeguato. Proprio a tal fine è indispensabile garantire l'indipendenza delle funzioni di controllo interno attraverso personale non impiegato in compiti operativi, separando dal punto di vista organizzativo le attività da monitorare e da controllare, evitando che non ci sia subordinazione da parte del responsabile della funzione di controllo interno ed evitando che la remunerazione del personale addetto alla funzione di controllo interno sia associata alle prestazioni delle attività controllata. La funzione di controllo interno, inoltre, non dovrebbe essere combinata con un'altra funzione di controllo interno.

Altro ambito di portata altamente significativa è quello della funzione di gestione dei rischi che dovrebbe operare a livello di intero ente e disporre di sufficiente peso, autorità e risorse in virtù di quei criteri di proporzionalità che abbiamo già visto, per attuare corrette ed efficaci politiche di gestione dei rischi medesimi. Per questi motivi, tale funzione dovrebbe essere indipendente dalle linee e unità di business di cui controlla i rischi ed essere un elemento organizzativo centrale dell'ente per fornire informazioni, analisi e pareri di specialisti sull'esposizione dei possibili rischi partecipando attivamente alla predisposizioni di strategie il più possibile efficaci, capaci di individuare quelli emergenti, monitorare e gestirei rischi delle unità dell'ente che potrebbero esserne interessate per consigliarle in modo semplice e lineare. Sarebbe fondamentale che il responsabile della funzione della gestione dei rischi disponesse di competenze e professionalità tali da consentirgli interventi, nelle decisioni, immediati e qualificati e, quando questi non è un membro dell'organo di amministrazione, dovrebbe essere nominato un responsabile indipendente che non abbia responsabilità in altre funzioni e che riferisca direttamente all'organo di amministrazione. Qualora non sia possibile individuare una persona che si dedichi in via esclusiva alla funzione di gestione dei rischi, questa funzione potrebbe essere combinata con quella di responsabile delle funzioni di conformità assicurando sempre la assenza di possibili conflitti di interesse tra le funzioni combinate. Certamente dovrebbe trattarsi di

soggetti con adeguate autorità, peso e indipendenza (talvolta si individua il responsabile dell'ufficio legale).

Una funzione specifica è l'ulteriore funzione di conformità che dovrebbe essere esercitata da persona altrettanto esperta, ugualmente indipendente dalle linee di business e dalle unità interne che controlla, capace di gestire i rischi di conformità e quindi di consigliare l'organo di amministrazione in merito agli opportuni interventi idonei ad assicurare la conformità a leggi, regolamenti norme e standard applicabili, insieme ad un valido programma di monitoraggio delle conformità, in sostanza vigilare che la politica di conformità sia rispettata.

Passando alla funzione di audit interno, che dovrebbe del pari essere istituita all'interno dell'ente con carattere di indipendenza ed efficacia e dalle funzioni di gestione dei rischi e di conformità. secondo i criteri di proporzionalità già precedentemente richiamati, essa, secondo un approccio basato sul rischio, dovrebbe garantire la conformità di tutte le attività e le unità dell'ente, anche esternalizzate, alle procedure e politiche dell'ente medesimo. Tale funzione dovrebbe valutare l'adeguatezza del quadro di governance dell'ente, la conformità delle politiche adottate alle leggi e ai regolamenti applicabili, se le procedure siano attuate in modo corretto e i controlli esercitati siano stati condotti in maniera adeguata rispetto segnalazioni effettuate dalle unità operative.

Per essere esercitata correttamente, nel rispetto di standard professionali nazionali ed internazionali , tale funzione dovrebbe avere accesso a tutti i dati, i documenti e le informazioni e gli immobili dell'ente, anche tramite accesso ai sistemi informativi ivi compresi verbali di tutti i comitati e di ogni organo decisionale.

Almeno annualmente dovrebbe essere redatto un piano di audit interno, formulato secondo un approccio basato sul rischio, sulla base degli obiettivi annuali di controllo di audit interno. Tutte le raccomandazioni oggetto di audit dovrebbero essere poi sottoposte ad un formale follow-up da parte dei rispettivi livelli di dirigenza per garantire la loro applicazione corretta e tempestiva.

Con riguardo alla trasparenza, gli indirizzi strategici, le politiche e le procedure dovrebbero essere oggetto di comunicazione a tutto il personale interessato, nel senso che, nell'ottica della trasparenza l'organo di amministrazione dovrebbe informare chiaramente il personale in merito agli indirizzi strategici e alle politiche dell'ente, ricorrendo ad opportune pubblicazioni. Tali documenti dovrebbero esprimere, in linea di massima, l'organizzazione interna degli enti, della struttura del gruppo, come previsto dalla direttiva 2013/34/UE, incluse le principali linee di segnalazione e responsabilità; indicare le nuove strutture giuridiche, di governance o organizzative, incluso il numero dei membri dell'organo di amministrazione e le specifiche responsabilità dell'organo di amministrazione; comunicare la composizione dei comitati di cui l'organo di amministrazione si

avvale nella sua funzione di supervisione strategica, una rassegna della politica adottata in materia di conflitto di interessi, di controllo interno e di gestione della continuità operativa.

Allegato 2

Schema per i sistemi di controllo interno nelle organizzazioni bancarie – Comitato di Basilea

Il Comitato giunge alla pubblicazione di questo documento dopo aver analizzato la situazione di diverse banche problematiche ed essere arrivato alla conclusione che, nella maggior parte dei casi, le perdite registrate da tali banchi sono state causate da inefficienze dei sistemi di controllo interni.
Come anticipato nel secondo capitolo, questo schema individua i criteri e i principi che le autorità di vigilanza devono utilizzare per la valutazione dei sistemi di controllo interno di una banca. In particolare si tratta di tredici principi divisi in tre sezioni.
A - Sorveglianza da parte degli organi direttivi e cultura dei controlli
1) Principio 1: "*Rientra nella responsabilità del consiglio di amministrazione approvare e riesaminare periodicamente le strategie operative globali e le politiche rilevanti dell'istituzione; conoscere i principali rischi assunti dalla banca, stabilire i livelli accettabili di tali rischi e assicurarsi che l'alta direzione adotti le misure necessarie per individuare, misurare, monitorare e controllare i rischi stessi; approvare la struttura organizzativa; assicurarsi che l'alta direzione verifichi l'efficacia del sistema di controllo interno. Al consiglio di amministrazione spetta in ultima istanza il compito di assicurare che sia istituito e mantenuto un sistema adeguato ed efficace di controlli interni*".
Il primo principio prevede i poteri del consiglio di amministrazione il quale tra i suoi compiti di gestione e supervisione strategica deve ricomprendere anche il controllo sull'istituzione di un adeguato sistema dei controlli interni. Il consiglio di amministrazione dovrebbe essere costituito da membri con conoscenze o competenze tecniche relative alle attività svolte dalla banca e ai rischi da essa assunti e dovrebbe ricomprendere anche competenti funzioni finanziarie, legali e di revisione interna. La composizione del CdA rappresenta un importante strumento per assicurare l'eliminazione di problemi che potrebbero menomare l'efficacia del sistema di controllo interno. Per garantire tale efficacia, il consiglio dovrebbe esaminare tempestivamente le valutazioni dei controlli interni effettuate dalla direzione, dai revisori interni e da quelli esterni e assicurarsi che la direzione dia attuazione alle raccomandazioni espresse dai revisori e dalle autorità di vigilanza a riguardo delle debolezze presenti nel sistema di controllo interno. Un modo per garantire che l'organo di gestione riesca a svolgere in modo idoneo tali compiti è la previsione di un comitato di revisione che supporti il consiglio nell'esercizio delle sue funzioni. Questo comitato dovrebbe essere responsabile della sorveglianza del processo di "reporting" finanziario e del sistema di controllo interno.
Nel quadro di questa responsabilità, esso rappresenta l'interlocutore diretto sia della revisione interna sia dei revisori esterni, che vengono nominati dallo stesso comitato. Il comitato di revisione dovrebbe essere composto prevalentemente o integralmente da amministratori esterni (ossia membri del

consiglio di amministrazione che non fanno parte dell'organico della banca o di una delle sue filiali), competenti in materia di "reporting" finanziario e controlli interni. In ogni caso, la costituzione di tale comitato non deve comportare la delega a questo di poteri del consiglio, il quale resta il solo ad essere giuridicamente investito del potere decisionale.

2) Principio 2: "*Rientra nella responsabilità dell'alta direzione dare attuazione alle strategie e alle politiche approvate dal consiglio di amministrazione; istituire processi atti a individuare, misurare, monitorare e controllare i rischi assunti dalla banca; mantenere una struttura organizzativa che individui chiare responsabilità, competenze e relazioni gerarchiche; assicurarsi che le funzioni delegate siano efficacemente assolte; definire appropriate politiche di controllo interno; verificare l'adeguatezza e l'efficacia del sistema di controllo interno*".

Il secondo principio disciplina le responsabilità dell'alta direzione che ha il compito fondamentale di istituire un efficace ed idoneo sistema di controllo interno. L'alta direzione nella pratica opera attraverso un articolato meccanismo di deleghe; per tale motivo, ha la responsabilità di sorvegliare l'attività dei funzionari ai quali ha delegato e di garantire che questi applichino procedure e politiche adeguate. Le linee di responsabilità e competenza devono essere definite con chiarezza e trasparenza e, allo stesso tempo, deve essere garantita un'efficace comunicazione a livello dell'intera organizzazione; a tali elementi è correlata la conformità con il sistema di controllo interno adottato.

L'alta direzione deve selezionare personale altamente qualificato, la cui formazione professionale venga aggiornata regolarmente, e deve prevedere politiche di remunerazione che premino comportamenti appropriati e riducano il rischio di elusioni dei meccanismi di controllo interno.

3) Principio 3: "*Il consiglio di amministrazione e l'alta direzione hanno la responsabilità di promuovere elevati standard etici e di integrità e di creare una cultura aziendale che valorizzi e dimostri a tutto il personale l'importanza dei controlli interni. È necessario che tutto il personale di un'organizzazione bancaria abbia chiara cognizione del proprio ruolo nel processo di controllo interno e sia pienamente impegnato nel processo medesimo*".

Affinché il sistema di controllo interno funzioni adeguatamente è indispensabile una solida cultura dei controlli. I membri dell'alta direzione e del consiglio di amministrazione sono da esempio per l'intera organizzazione; perciò, devono dare prova di conformarsi a solidi valori etici in tutti i loro atti, atteggiamenti e parole. È fondamentale che la rilevanza di un efficiente sistema di controllo interno venga appresa a tutti i livelli dell'organizzazione in quanto tutto il personale della banca contribuisce alla produzione di informazioni necessarie ad effettuare i controlli. A tal fine è necessario che tutte le procedure operative vengano indicate in documenti chiari e disponibili per tutto il personale.

Per consolidare i valori etici, vanno evitate attività inappropriate come: mettere in secondo piano i rischi di lungo periodo ponendo un'eccessiva enfasi su obiettivi di performance o altri risultati operativi di breve termine; separare le funzioni e i controlli in modo inadeguato, così da causare un cattivo uso delle risorse o la dissimulazione di risultati insoddisfacenti; prevedere sanzioni ingiuste, perché insignificanti o eccessivamente pesanti, per comportamenti scorretti. La previsione e la diffusione di una solida cultura dei controlli non comporta l'automatico conseguimento di tutti gli obiettivi dell'organizzazione, ma sicuramente fa diminuire il rischio che non vengano individuati errori o irregolarità.

B - Individuazione e valutazione del rischio

4) Principio 4: "*Un efficace sistema di controllo interno richiede che siano individuati e costantemente valutati i rischi sostanziali che potrebbero influire negativamente sul conseguimento degli obiettivi aziendali. La valutazione deve estendersi a tutti i rischi cui sono esposte la banca e l'organizzazione bancaria consolidata (ossia, il rischio di credito, il rischio paese e di trasferimento valutario, il rischio di mercato, il rischio di tasso d'interesse, il rischio di liquidità, il rischio operativo, il rischio legale e il rischio di reputazione). Può essere necessaria una revisione dei controlli interni in modo che essi tengano adeguatamente conto dei rischi nuovi o precedentemente non soggetti a controllo*".

Il sistema di controllo interno è fondamentale per l'individuazione e la valutazione di tutti i fattori di rischio, interni ed esterni, che possono avere effetti negativi sul conseguimento degli obiettivi.

Questo processo di valutazione si differenzia dal processo di gestione del rischio, il quale ha come obiettivo primario il riesame delle strategie operative elaborate per massimizzare il trade-off rischio/rendimento all'interno delle varie aree della banca. Nell'ambito di un processo di valutazione del rischio occorre distinguere i rischi che sono controllabili dalla banca dai rischi che non lo sono. Per quanto riguarda i primi, la banca deve decidere se accettarli oppure in che misura essa desidera ridurli attraverso le procedure di controllo. Invece, per i rischi che non possono essere controllati la banca deve decidere se accettarli o se ritirarsi dall'attività ad essi collegata. In presenza di determinate circostanze, ad esempio di un'innovazione finanziaria, può essere necessaria una revisione dei controlli interni per tenere in considerazione rischi nuovi o precedentemente non soggetti a controllo. Un modo per considerare tutti i rischi consiste nel creare diversi scenari ed esaminare tutti i possibili problemi che potrebbero verificarsi così da mettere in evidenza gli aspetti critici del controllo.

C - Attività di controllo e separazione delle funzioni

5) Principio 5: "*Le attività di controllo devono essere parte integrante dell'operatività quotidiana di una banca. Un efficace sistema di controllo interno richiede che sia istituita una struttura appropriata, in cui le attività di controllo sono definite ad ogni livello dell'azienda. Queste*

dovrebbero prevedere: verifiche ai massimi livelli; adeguati controlli sull'operatività dei vari dipartimenti o divisioni; controlli fisici; verifica dell'osservanza dei limiti all'esposizione e azioni correttive in caso di mancata osservanza; un sistema di approvazioni e autorizzazioni; un sistema di verifiche e riscontri".

Attraverso il processo di valutazione sopra descritto, la banca individua dei rischi che vanno poi affrontati con le attività di controllo. Queste ultime consistono in una prima fase di definizione delle politiche e delle procedure di controllo e in una seconda fase di verifica del rispetto di tali politiche e procedure.

Le attività di controllo coinvolgono tutti i livelli dell'organico della banca e possono consistere in:

• Verifiche ai massimi livelli: il consiglio di amministrazione e l'alta direzione possono richiedere documentazioni e rendiconti gestionali per verificare i progressi compiuti dalla banca nella realizzazione dei propri obiettivi. Ad esempio, l'alta direzione può esaminare i rapporti che aggiornano i risultati finanziari effettivi a fronte del budget. Si tratta di attività di controllo i cui risultati potrebbe far emergere problemi, come debolezze nel sistema di controllo, errori nelle segnalazioni finanziarie o attività fraudolente.

• Controlli dell'attività: i dirigenti a livello di dipartimento o di divisione effettuano verifiche sui rapporti regolari o straordinari su base giornaliera, settimanale o mensile ricevuti. Tali verifiche risultano più analitiche e approfondite di quelle svolte dall'alta direzione.

• Controlli fisici: queste attività di controllo sono volte a limitare l'accesso ad attività materiali, come contante e titoli. Possono consistere in restrizioni fisiche, la duplice custodia e inventari periodici.

• Osservanza dei limiti all'esposizione: i rischi devono essere gestiti anche attraverso la fissazione di prudenti limiti all'esposizione per ridurre la concentrazione del rischio creditizio della banca e contribuire alla diversificazione del suo profilo di rischio.

• Approvazioni e autorizzazioni: le transazioni superiori a determinati limiti necessitano dell'approvazione e dell'autorizzazione da parte dei livelli direttivi, in questo modo si garantisce che i vertici vengano informati della transazione e vengono anche definite le varie responsabilità.

• Verifiche e riscontri: importanti attività di controllo sono i riscontri periodici, come il raffronto tra i flussi di cassa e i documenti contabili, che possono evidenziare attività e registrazioni incorrette. In questo caso, i risultati di queste verifiche devono essere segnalati all'appropriato livello direttivo.

La cultura dei controlli sopra richiamata è indispensabile anche per diffondere una concezione delle attività di controllo come parte integrante e non accessoria, dell'operatività quotidiana della banca. Se svolti giornalmente, i controlli consentono di reagire rapidamente al variare delle condizioni ed evitano costi inutili. Non è sufficiente definire le politiche e le procedure appropriate per le varie attività e divisioni della banca, ma è necessario assicurarsi regolarmente che tutte le aree della banca

operino in conformità con tali politiche e procedure, questo compito rappresenta uno dei ruoli principali della funzione di revisione interna.

6) Principio 6: "*Un efficace sistema di controllo interno richiede che vi sia un'adeguata separazione delle funzioni e che al personale non vengano assegnate responsabilità contrastanti. Le aree di potenziale conflitto di interessi devono essere individuate, ridotte al minimo, nonché sottoposte a sorveglianza accurata e indipendente*".

Una separazione delle funzioni inadeguata rappresenta una delle principali cause, tra quelle relative a carenze nei controlli interni, di gravi perdite bancarie. In particolare, laddove vi può essere il rischio di manipolazione di dati finanziari o di indebita appropriazione di attività i compiti devono essere ripartiti, per quanto possibile, tra varie persone. È necessaria, dunque, la presenza di una terza parte indipendente che sorvegli le aree di potenziale conflitto di interessi e che riesamini periodicamente le responsabilità e le funzioni del personale collocato in posti chiave, in modo da assicurare che esso non sia in grado di dissimulare atti inappropriati.

D - Informazione e comunicazione

7) Principio 7: "*Un efficace sistema di controllo interno richiede che siano disponibili adeguati ed esaurienti dati interni sugli aspetti finanziari, operativi e di conformità, nonché informazioni esterne di mercato su fatti e situazioni rilevanti ai fini del processo decisionale. Le informazioni devono essere affidabili, tempestive e accessibili; esse devono inoltre essere fornite con modalità uniformi*".

Un elemento indispensabile per un efficace sistema di controllo interno è costituito da sono un adeguato flusso di informazioni e un'efficace comunicazione. L'informazione deve essere significativa, affidabile, tempestiva, accessibile e fornita secondo modalità uniformi. Le informazioni possono riguardare sia dati interni, come dai finanziari, operativi e di conformità sia dati esterni di mercato su eventi e situazioni rilevanti ai fini del processo decisionale.

8) Principio 8: "*Un efficace sistema di controllo interno richiede che operino affidabili sistemi informativi comprendenti tutte le attività rilevanti della banca. Tali sistemi, inclusi quelli che contengono e utilizzano dati in forma elettronica, devono essere sicuri, sorvegliati in modo indipendente e assistiti da adeguati dispositivi di emergenza*".

Le banche devono prevedere l'istituzione e il mantenimento di sistemi di informazioni riguardanti l'intera gamma delle attività svolte. Solitamente queste informazioni, fornite sia in forma elettronica che con altri mezzi, necessitano di un adeguato processo di revisione in quanto informazioni inaffidabili o sbagliate fornite da sistemi inadeguati possono influenzare negativamente le decisioni della direzione. Un altro rischio dovuto a controlli non idonei è la perdita di dati e di programmi. La banca deve anche fare i conti con problematiche dei sistemi di informazione fuori dal loro controllo e perciò elaborare piani per la ripresa delle operazioni e la gestione delle emergenze che prevedano il

ricorso a strutture al di fuori dell'istituzione, come un fornitore esterno di servizi. I piani per la ripresa delle operazioni devono essere periodicamente sottoposti a test per assicurarne la funzionalità in caso di un evento disastroso imprevisto.

9) Principio 9: "*Un efficace sistema di controllo interno richiede che siano istituiti efficaci canali di comunicazione per assicurare che tutto il personale conosca esattamente e osservi le politiche e le procedure attinenti alle proprie funzioni e responsabilità, e che ogni altra informazione rilevante pervenga al personale appropriato*".

L'alta direzione deve garantire efficaci canali di comunicazione che consentano che le informazioni arrivino al personale appropriato sia in senso verticale che orizzontale. Il flusso informativo verso l'alto è fondamentale per permettere al consiglio di amministrazione e all'alta direzione di conoscere i rischi e i risultati operativi; il flusso informativo verso il basso consente di diffondere anche ai livelli direttivi inferiori e ai quadri esecutivi gli obiettivi, le strategie e le aspettative della banca, nonché le politiche e le procedure da essa stabilite. La comunicazione in senso orizzontale è infine necessaria per trasmettere le informazioni da una divisione o un dipartimento ad un altro.

E - Attività di monitoraggio e correzione delle carenze

10) Principio 10: "*L'efficacia complessiva dei controlli interni della banca deve essere verificata in modo continuativo. Il monitoraggio dei principali tipi di rischio, così come le valutazioni periodiche da parte dei settori operativi e dei revisori interni, devono rientrare nell'attività quotidiana della banca*".

Il sistema dei controlli interni deve essere costantemente monitorato e adattato alle mutevoli condizioni interne ed esterne. Il monitoraggio deve essere svolto sia quotidianamente, così da consentire di rilevare e correggere tempestivamente eventuali carenze dei controlli interni, sia con valutazioni periodiche separate che forniscono una visione globale ex novo dell'efficacia del sistema di controllo interno. Tali valutazioni possono essere effettuate da personale appartenente a diverse aree e possono assumere la forma di autovalutazione se i responsabili di una data funzione determinano l'efficacia dei controlli per la propria sfera di attività. Questi esami devono essere adeguatamente documentati e comunicati all'alta direzione per essere esaminati.

11) Principio 11: "*Il sistema di controllo interno deve essere sottoposto a un'efficace e completa revisione interna ad opera di personale operativamente indipendente, dotato di formazione e competenza adeguate. La funzione di revisione interna, in quanto parte del monitoraggio del sistema di controllo interno, deve dipendere direttamente dal consiglio di amministrazione (o da un comitato da esso designato) e dall'alta direzione*".

La funzione di revisione interna esprime un giudizio indipendente sull'adeguatezza delle politiche e procedure stabilite e sul loro rispetto; per tale ragione rappresenta un elemento importante del

monitoraggio continuativo del sistema di controllo interno. Data la rilevanza di questa funzione, è necessario che sia indipendente dall'operatività quotidiana della banca e abbia accesso a tutte le attività svolte dall'organizzazione bancaria, comprese le sue succursali e affiliate. Inoltre, riferisce direttamente al consiglio di amministrazione e all'alta direzione e, perciò, è in grado di fornire informazioni sulle altre funzioni aziendali attendibili e non distorte dai livelli gestionali che sono oggetto dei rendiconti. L'autonomia dei revisori interni deve essere ulteriormente rafforzata disponendo che le decisioni circa aspetti quali la loro remunerazione o le risorse assegnate in bilancio siano di competenza del consiglio di amministrazione stesso o dei più alti livelli direzionali, anziché di quadri interessati dal lavoro compiuto dai revisori interni.

12) Principio 12: "*Le deficienze individuate nei controlli interni da settori operativi, revisori interni o altro personale adibito a funzioni di controllo devono essere segnalate tempestivamente al livello direzionale appropriato ed essere affrontate con prontezza. Le deficienze rilevanti devono essere segnalate all'alta direzione e al consiglio di amministrazione*".

In caso di inefficienze nei controlli interni e nel controllo dei rischi è necessaria una segnalazione immediata ai soggetti appropriati o al consiglio di amministrazione e all'alta direzione nei casi di maggiore gravità. La direzione, avutane notizia, deve rimediare tempestivamente. Successivamente subentrano le verifiche da parte della revisione interna che deve avvisare immediatamente l'alta direzione o il consiglio di amministrazione se le deficienze non siano state eliminate.

F - Valutazione dei sistemi di controllo interno da parte delle autorità di vigilanza

13) Principio 13: "*Le autorità di vigilanza devono richiedere che ogni banca, indipendentemente dalle dimensioni, abbia un efficace sistema di controllo interno coerente con la natura, la complessità e la rischiosità delle sue operazioni, in bilancio e fuori bilancio, e capace di adeguarsi ai cambiamenti nel contesto operativo e nella situazione dell'azienda. Qualora le autorità di vigilanza stabiliscano che il sistema di controllo interno di una banca non è adeguato o efficace per il profilo di rischio specifico di quella banca (poiché, ad esempio, non soddisfa tutti i principi contenuti nel presente documento), esse devono intraprendere un'appropriata azione correttiva*".

Le autorità di vigilanza devono intraprendere tutte le misure più appropriate se accertano che il sistema di controllo interno di una banca non è adeguato o efficace per il profilo di rischio specifico di quella banca. Devono, inoltre, sorvegliare le misure adottate dalla banca per migliorare il suo sistema di controllo interno.

Vi sono alcuni cambiamenti del contesto in cui opera una banca che devono essere oggetto di attenzione particolare per verificare se sia necessaria una corrispondente revisione del sistema di controllo interno, tra questi cambiamenti figurano: mutamenti del contesto operativo; nuovo personale; rinnovo o ammodernamento dei sistemi informativi; nuove tecnologie e nuove linee,

prodotti o attività (in particolare se di natura complessa); ristrutturazioni, fusioni e acquisizioni societarie.

Per valutare la qualità dei controlli interni le autorità di vigilanza spesso analizzano l'operato, la documentazione e la metodologia impiegata dalla funzione di revisione interna della banca. Se non riscontrano anomalie, le autorità utilizzano i rapporti redatti dai revisori interni come strumento primario per individuare problemi nei controlli interni o aree di potenziale rischio non esaminate. In altri casi possono fare ricorso a un processo di autovalutazione o richiedere revisioni esterne.

In molti paesi le autorità di vigilanza effettuano ispezioni in loco, e un esame del sistema di controlli interni è parte integrante di tali ispezioni. In sostituzione delle ispezioni in loco, le autorità di vigilanza possono rivolgersi a revisori esterni che devono effettuare l'analisi del processo gestionale e i test sulle transazioni in genere svolti dalle stesse autorità di vigilanza. La qualità del lavoro svolto dai revisori è poi oggetto di valutazione da parte delle autorità.

Nel verificare l'adeguatezza del processo di controllo interno presso ogni singola organizzazione bancaria, le autorità di vigilanza del paese di origine devono accertare l'efficacia del processo in tutte le linee di attività e le affiliate dell'organizzazione, indipendentemente dalla giurisdizione. A tal fine devono incoraggiare i gruppi bancari ad avvalersi, per quanto possibile, dei medesimi revisori e a rispettare le stesse scadenze contabili in tutte le unità del gruppo.

RIASSUNTO

IL SISTEMA DEI CONTROLLI INTERNI E LA FUNZIONE DI INTERNAL AUDIT NELL'AMBITO DELLO SREP

Il presente lavoro ha inteso esaminare i risvolti che l'affermazione del *Supervisory Review and Evaluation Process* (SREP) ha avuto sulle attività delle banche e, conseguentemente, sul sistema dei controlli interni, sulla funzione di *Internal Audit* e sulla loro evoluzione.

La prospettiva dello studio è stata quella di indagare in concreto le rilevanze più significative che il sistema ha prodotto sugli enti e, nello specifico, si è guardato, comparativamente, ai risultati relativi a quattro istituti di credito.

L'elaborato si articola in tre capitoli, i cui contenuti si richiamano, sia pur brevemente, di seguito.

Nel primo capitolo si introduce il sistema dei controlli interni e la funzione di *Internal Audit*, passando in rassegna la disciplina e gli elementi essenziali sia del sistema dei controlli che dell'*Internal Audit* considerato che rappresentano le premesse essenziali nello sviluppo del tema trattato.

Il secondo capitolo sul *Supervisory Review Process* analizza, in primo luogo, l'evoluzione dell'impianto regolamentare relativo al processo di controllo prudenziale, facendo riferimento alla regolamentazione prevista in Basilea III e recepita in ambito comunitario dalla Direttiva 2013/36/UE e dal Regolamento UE/575/2013, nonché alla normativa nazionale e alle disposizioni emanate da Banca d'Italia. In secondo luogo, si sofferma sul *Supervisory Review Process* e sulle due fasi di tale processo. Si illustra, più in particolare, la prima fase che fa capo alle banche, consistente nei processi interni di valutazione dell'adeguatezza del capitale (*Internal Capital Adequacy Assessment Process*-ICAAP) e della liquidità (*Internal Liquidity Adequacy Assessment Process*-ILAAP).Viene esaminata, inoltre, la seconda fase che è quella del *Supervisory Review and Evaluation Process* in senso stretto, cioè del processo di revisione e valutazione prudenziale di competenza delle Autorità di vigilanza (la Banca Centrale Europea per le banche "significant" e le Autorità di vigilanza nazionale per le banche "less significant").

Il terzo capitolo affronta il sistema dei controlli e la funzione di *Internal Audit* nell'ambito del *Supervisory Review and Evaluation Process* attraverso l'esame degli organi aziendali coinvolti nel processo di controllo prudenziale e la rilevanza dei rispettivi ruoli.

In questa sede vengono riportate le esperienze concrete di talune banche annoverate tra le "significant" e quotate quali Intesa Sanpaolo, Mediobanca, Ubi Banca e Unicredit; la valutazione è stata in relazione al loro sistema di *governance* interna con particolare riferimento alla composizione del Consiglio di Amministrazione, alle caratteristiche di indipendenza, professionalità e competenze richieste ai loro componenti, alla diversificazione in ragione di età e di genere, alle politiche di

nomina e di remunerazione, alla presenza di comitati endoconsiliari, al funzionamento dei sistemi di controllo interno e dei sistemi informativi per addivenire ad una valutazione nell'ottica SREP dell'adeguatezza della loro struttura di *governance* e di controllo interno.
La valutazione di questi ultimi profili, alla luce delle questioni poste e degli elementi trattati nel corso del lavoro, ha condotto ad evidenze riportate nelle considerazioni conclusive unitamente a brevi cenni sulle possibili prospettive future dei meccanismi dei controlli prudenziali.

PRIMO CAPITOLO
IL SISTEMA DEI CONTROLLI INTERNI E L'INTERNAL AUDITING

Il primo capitolo muove da una sintesi delle origini e dell'evoluzione storica dei concetti di controllo interno e di *internal auditing.* Con riferimento ai controlli interni, si ripercorrono le tappe principali della loro evoluzione a partire dagli anni quaranta, durante i quali il tema dei controlli interni rappresenta un aspetto marginale, seppure non del tutto irrilevante, della revisione contabile e uno strumento per garantire la veridicità e la completezza dei documenti contabili sottoposti a revisione. Intorno alla metà degli anni ottanta il tema dei controlli interni assume progressivamente un ruolo di crescente rilievo, in particolare, nell'ambito di decisioni associate ai processi di *risk assessment* e di *risk management*.
Negli anni novanta il lavoro di ricerca del *Committee of Sponsoring Organizations of the Treadway Commission* (*CoSO*) porta alla nascita dell'"*Internal Control - Integrated Framework*", più noto come *CoSO Report*. Il *CoSO Report* viene pubblicato nel 1992 negli Stati Uniti con l'obiettivo di delineare e promuovere un concetto univoco di controllo interno e un modello di riferimento per società e management nella creazione di un sistema di controllo. In pochi anni, tale report viene adottato in numerosi paesi, tra cui l'Italia, e utilizzato come schema per la predisposizione di codici di autodisciplina, norme e altri documenti sui controlli interni.
Data la sempre maggiore importanza assunta dal tema della gestione dei rischi, il *Committee of Sponsoring Organizations of the Treadway Commission* giunge nel 2004 alla pubblicazione di un nuovo report, l'"*Enterprise Risk Management - Integrated Framework*" o *CoSO II,* che amplia la visione del concetto di controllo interno in termini di *risk management*.
Per quanto riguarda l'*Internal Auditing* (IA), l'evoluzione del suo significato e dell'attività di auditing prende le mosse dall'esperienza degli Stati Uniti e dell'Inghilterra dove tale tematica si è diffusa ed affermata tempo prima rispetto all'Italia.
La nascita dell'Internal Audit si fa risalire ufficialmente al 1941, anno in cui viene fondato in Florida l'Institute of Internal Auditors (IIA) con lo scopo di favorire la conoscenza e lo sviluppo della professione dell'internal auditor. Qualche anno dopo nel 1948 viene fondata a Londra l'associazione IIA-UK quale sede distaccata di quella statunitense; successivamente, altri organismi professionali

esistenti nel Regno Unito si sono occupati della definizione degli standard di revisione interna, mentre in Italia si dovrà attendere la seconda metà del '900.

Nel 1972, infatti, a Milano nasce l'Associazione Italiana Internal Auditors (AIIA) dietro la spinta dell'esperienza inglese e statunitense, ma anche di alcuni interventi normativi. In particolare, di alcuni progetti di legge che hanno condotto all'emanazione della legge 216/1974, cui è stata data attuazione dal D.P.R. 136/1975, concernente il controllo contabile e la certificazione obbligatoria dei bilanci delle società per azioni quotate in Borsa, decreto ormai in parte superato dalla cosiddetta "legge Draghi". Nel corso degli anni, infatti, questa funzione subisce una significativa evoluzione: da attività di raccolta di dati e verifica dei controlli avvertita dalla compagine societaria come attività "estranea" e "nemica", ad attività, anche preventiva, di analisi trasversale dei processi di business e di valutazione dei rischi svolta dagli auditors considerati membri del team.

Per quanto riguarda il contesto normativo, fino al 1998 si registrano esclusivamente interventi che non hanno natura né validità legale bensì solo di raccomandazioni per le imprese, come, ad esempio, i "*Principi di comportamento del Collegio Sindacale*" del Consiglio Nazionale dei Dottori Commercialisti e dei Ragionieri, il "*Libro Verde*" della Commissione europea e il "*Progetto Corporate Governance per l'Italia*".

La prima svolta si ha nel 1998 con l'entrata in vigore del "*Testo Unico della Finanza - TUF*" (D.lgs. n. 58 del 24 febbraio 1998, noto anche come "legge Draghi") che formalizza l'importanza del Sistema di Controllo Interno, introducendo per la prima volta nella legislazione italiana tale espressione e, seppure implicitamente, anche quella dell'*Internal Auditing*. Il TUF rappresenta il punto di partenza da cui la regolamentazione di settore e l'autoregolamentazione dei singoli emittenti quotati prendono le mosse per l'individuazione di un quadro d'insieme delle regole concernenti il buon governo d'impresa.

Proseguendo in ordine cronologico, nel 1999 nasce il Codice di Autodisciplina, conosciuto anche come "*codice Preda*", dal nome dell'allora presidente di Borsa Italiana SpA e coordinatore del Comitato per la *corporate governance*. Gli obiettivi del codice sono implementare il controllo dei rischi d'impresa, creare un adeguato sistema di deleghe, garantire la trasparenza nei flussi informativi e massimizzare la creazione di valore per gli azionisti.

Le tematiche del controllo interno hanno un ruolo centrale anche nel D.lgs n. 231 del 19 giugno 2001 in materia di responsabilità amministrativa degli Enti, con o senza personalità giuridica, per i reati commessi nel loro interesse dai soggetti impiegati nell'ente. La norma attribuisce importanza fondamentale al Sistema di Controllo Interno e all'Internal Auditing in quanto lo svolgimento di tali attività diviene strumento di valutazione della responsabilità degli amministratori.

Nell'elaborato vengono poi analizzati ulteriori interventi normativi rilevanti per il tema dei controlli interni, tra cui il D.lgs n. 6 del 17 gennaio 2003 contenente la riforma organica della disciplina delle società di capitali, la Legge sulla tutela del risparmio (Legge 28 dicembre 2005, n. 262) e il D.lgs 39 del 22 gennaio 2010.

Il primo capitolo prosegue con una disamina del Sistema dei Controlli Interni declinato in ogni sua componente, richiamando due delle definizioni di controllo interno più diffuse: si tratta delle definizioni fornite dal Codice di Autodisciplina e dal *CoSO Report I*.

Secondo il Codice di Autodisciplina, il Sistema di Controllo Interno e di Gestione dei Rischi è l'insieme delle regole, delle procedure e delle strutture organizzative volte a consentire l'identificazione, la misurazione, la gestione e il monitoraggio dei principali rischi, così da contribuire a una conduzione dell'impresa coerente con gli obiettivi aziendali e che favorisca l'assunzione di decisioni consapevoli. Un efficace Sistema di Controllo Interno (SCI) deve perseguire e garantire la salvaguardia del patrimonio sociale, l'efficienza e l'efficacia dei processi aziendali, l'affidabilità delle informazioni tra organi sociali e verso il mercato e il rispetto di leggi, regolamenti, statuto sociale e procedure interne. Nell'elaborato vengono approfonditi i ruoli che ciascun organo societario e ciascuna funzione aziendale assume nell'ambito del sistema di controllo interno.

La seconda definizione di controllo interno esaminata è quella fornita dal *CoSO Report*. Il *CoSO* viene analizzato in tutte le sue componenti e, in tale ambito, viene richiamato anche il *CoSO Report II* con particolare riferimento agli aspetti che hanno innovato rispetto al *CoSO I.*

Nello studio della funzione di Internal Auditing (IA) si riscontra la mancanza di fonti normative contenenti definizioni univoche. Per questo motivo, è indispensabile fare riferimento ad una delle più significative fonti di informazioni circa la natura e le attività di Internal Auditing, che è rappresentata dall' "*International Professional Practices Framework – IPPF*" pubblicato dall'IIA (*The Institute of Internal Auditors*). L'analisi della funzione di IA prosegue con l'esame degli elementi principali di tale *Framework*: la *mission*, le *guidance*, i Principi fondamentali, il Codice etico, la definizione di IA e gli Standard Internazionali per la pratica professionale.

CAPITOLO 2
IL SUPERVISORY REVIEW PROCESS

Nel secondo capitolo si analizza il contesto normativo e regolamentare del *Supervisory Review Process* (SRP) a partire dalla costituzione del Comitato di Basilea nel 1974 quando i Governatori delle Banche Centrali appartenenti al G10 fondano all'interno della Banca dei Regolamenti Internazionali (BRI) tale comitato con l'intento di perseguire la stabilità economica e finanziaria

attraverso la cooperazione tra le Banche Centrali e l'armonizzazione dei processi nazionali di vigilanza.

Un primo contributo in tema di vigilanza prudenziale da parte del Comitato di Basilea si ha nel 1988 con il cosiddetto "Accordo di Basilea I". Nell'ottica dell'armonizzazione delle regole prudenziali rivolte alle banche dei diversi paesi, tale accordo si pone come obiettivi quello di migliorare la stabilità e la solvibilità delle banche a livello internazionale e quello di ridurre eventuali elementi di disparità sia sul piano concorrenziale sia sul piano regolamentare. Viene affrontato, a tal proposito, il tema dell'adeguatezza patrimoniale della banca rispetto al rischio di credito assunto.

Negli anni seguenti i parametri stabiliti da Basilea I si rivelano troppo rigidi e statici rispetto a vari profili, tra cui le diverse tipologie di rischio, i diversi livelli di solvibilità e le diverse scadenze e tali limiti fanno nascere l'esigenza di un nuovo schema di adeguatezza patrimoniale e di valutazione dei rischi che, nel 2004, viene trasfuso nel "*Nuovo accordo sul capitale o Convergenza internazionale della misurazione del capitale e dei coefficienti patrimoniali*", conosciuto anche come Basilea II. Il Nuovo accordo sul capitale (NAC) si fonda su tre punti focali, i cosiddetti pilastri, riguardanti i requisiti patrimoniali minimi, il processo di controllo prudenziale e la disciplina di mercato.

Così come per Basilea I, anche per il Nuovo accordo emergono alcuni limiti tra cui l'impossibilità di plasmare lo schema di vigilanza previsto alle varie realtà delle banche, a discapito, in particolare, di quelle di minori dimensioni; il fenomeno della prociclicità finanziaria, causa dell'aumento del costo di approvvigionamento al credito; l'ignorare il rischio di liquidità correlato alla creazione di un "cuscinetto" di capitale come salvagente nei casi di insolvenza.

I punti critici di Basilea II, resi ancor più evidenti dalla crisi finanziaria del 2007/2008, portano il Comitato di Basilea a considerare l'eventualità di una riforma di tale accordo. Dopo alcune variazioni apportate a Basilea II, nel 2010 viene approvato un nuovo accordo, conosciuto come Basilea III che mantiene lo schema della regolamentazione precedente richiamando dunque i tre pilastri, ma, allo stesso tempo, introduce alcuni aspetti innovativi.

Le regole sino ad ora richiamate, in particolare quelle previste da Basilea III, sono recepite dalla normativa europea attraverso il c.d. "pacchetto CRR-CRD IV" contenente la direttiva 36/2013/UE – *Capital Requirements Directive* (CRD IV) – e il regolamento UE/575/2013 – *Capital Requirements Regulation* (CRR). L'obiettivo principale di queste disposizioni è ridurre la discrezionalità degli Stati nell'applicazione delle regole di vigilanza prudenziale, che è causa di distorsioni della concorrenza e di arbitraggi regolamentari.

Infine, si richiama la circolare n. 285 del 17 dicembre 2013, entrata in vigore il 1 gennaio 2014, con cui la Banca d'Italia illustra le nuove disposizioni di vigilanza per le banche e le imprese di investimento, recependo il "pacchetto CRR-CRD IV", costituito, come già detto, dalla direttiva

2013/36/UE e dal regolamento UE 575/2013. Con la circolare n. 285/2013 vengono rivisitate ed aggiornate le diposizioni in tema di vigilanza prudenziale, sicché dalla data di entrata in vigore della circolare, alle banche e ai gruppi bancari restano applicabili solo alcuni capitoli della precedente circolare n. 263/2006.

Il capitolo prosegue con una analisi dettagliata del *Supervisory Review Process* che prevede due fasi tra loro integrate: la prima coinvolge le banche ed è costituita dal processo interno di determinazione dell'adeguatezza patrimoniale (*Internal Capital Adequacy Assessment Process* – ICAAP) e dal processo interno di valutazione della liquidità (*Internal Liquidity Adequacy Assessment* – ILAAP); la seconda fase consiste nel processo di revisione e valutazione prudenziale (Supervisory Review and Evaluation Process – SREP) che fa capo alle Autorità di vigilanza.

Le fasi del *Supervisory Review Process* vengono analizzate nel dettaglio. Per quanto riguarda i Processi ICAAP e ILAAP vengono declinate le responsabilità degli organi e delle funzioni di controllo che sono coinvolti in tali processi. Per quanto riguarda lo SREP in senso stretto vengono richiamate tutte le aree oggetto di valutazione da parte delle Autorità di vigilanza (modello imprenditoriale, *governance*, rischi di capitale e rischi di liquidità) e tutte le fasi del processo con specifico riferimento alle modalità di assegnazione dei punteggi.

CAPITOLO 3

IL RUOLO DEL SISTEMA DI CONTROLLO INTERNO E DELLA FUNZIONE DI *INTERNAL AUDIT* NELL'AMBITO DELLO SREP

Nel terzo capitolo si affronta il tema del Sistema di Controllo Interno e della funzione di *Internal Audit* in relazione agli specifici ruoli che questi assumono nelle banche e nell'ambito dello SREP. A tal fine, si richiama la normativa speciale, nazionale e comunitaria, definita dal Comitato di Basilea, dalla direttiva Mifid e dalle disposizioni di Banca d'Italia.

In particolare, vengono richiamate le Disposizioni di Vigilanza di Banca d'Italia di cui alla Circolare 285 del 2013 che prevedono un set regolamentare relativo al governo societario e ad alcuni elementi tipici dei sistemi di amministrazione e controllo delle banche. Nell'elaborato vengono declinate dettagliatamente le responsabilità in capo a ciascun organo e a ciascuna funzione di controllo. In particolare, si richiamano i ruoli del SCI e dell'IA con riferimento alla gestione del rischio e ai processi ICAAP E ILAAP.

Nella seconda parte del capitolo si procede con l'analisi, in ottica SREP, di quattro banche italiane sotto il profilo delle strutture di *governance* e di controllo interno. L'obiettivo del lavoro consiste nell'assegnazione di una valutazione finale, anche numerica, che possa riflettere l'adeguatezza e l'efficienza di tali strutture. Oggetto della valutazione sono quattro banche italiane, tutte quotate nel mercato di Milano (FTSE Mib) e "*significant*", quindi soggette alla vigilanza diretta della Banca

Centrale Europea: Intesa Sanpaolo, Mediobanca, UBI banca e UniCredit. Il *Supervisory Review and Evaluation Process* valuta lo stato di salute delle banche da quattro angolazioni, tra cui la *governance* dell'organizzazione. In questo ambito l'autorità di vigilanza deve verificare l'esistenza di una sana gestione dei rischi e di un adeguato sistema dei controlli interni e deve stabilire se vi sono rischi connessi all'inadeguatezza della *governance* e quale impatto questi possono avere sulla sostenibilità dell'ente. Il capitolo prosegue con l'individuazione dei criteri sulla base dei quali viene svolta la valutazione della *governance* delle quattro banche. Tali criteri si riferiscono alla composizione del Consiglio di amministrazione (numero di componenti, componenti esecutivi, componenti indipendenti, requisiti di professionalità e competenze, numero di incarichi ricoperti, tempo dedicato agli incarichi, diversificazione della composizione del Consiglio), alle procedure di nomina degli amministratori, alle politiche di remunerazione, alla presenza di comitati endoconsiliari, al funzionamento del sistema di controllo interno e all'adeguatezza del sistema informativo. Questi aspetti vengono esaminati per ciascuna banca e, infine, si giunge al risultato della valutazione in un'ottica comparativa.

Sulla base della valutazione svolta, si rileva che la struttura di governo societario e dei controlli interni delle quattro banche esaminate non presenta profili critici di rilevante gravità. Nonostante questo, è possibile individuare diversi elementi che influenzano negativamente la complessiva valutazione sulla *governance* e che sono suscettibili di miglioramento. In particolare, margini di miglioramento si individuano nella composizione del Consiglio di amministrazione delle quattro banche. Si ritiene, infatti, che il numero dei componenti sia troppo elevato. Questi numeri, se da un lato risultano giustificati dalle dimensioni e dalla complessità operativa delle banche in questione, dall'altro lato a lungo andare possono causare problemi di coordinamento e comunicazione tra i membri nonché prolungamenti delle procedure decisionali. In conclusione, nella consapevolezza che non sia possibile individuare preventivamente un numero ottimale di amministratori, dovendo questo essere adattato alle caratteristiche specifiche della banca, si ritiene che, con specifico riferimento alle quattro banche analizzate, il numero dei componenti sia da ridurre ulteriormente per evitate riflessi negativi sulla funzionalità delle banche.

Il secondo elemento che presenta margini di miglioramento è relativo alla diversificazione del Consiglio di amministrazione. Sotto il profilo della diversità di genere, si rileva che nelle 4 banche esaminate viene rispettato il requisito minimo, pari a 1/3, previsto dalla Legge n. 120 del 12 luglio 2011, che ha modificato l'art. 147 –ter del TUF. Tuttavia, si può osservare che la percentuale di donne nei Consigli si attesta intorno alla percentuale minima richiesta dalla normativa e solo in un caso vi è una donna a ricoprire la carica di presidente del Consiglio di amministrazione (UBI Banca), mentre nessuna donna ricopre la carica di amministratore delegato. Anche sotto il profilo dell'età, la

composizione del Consiglio di amministrazione potrebbe essere meglio diversificata. Dall'osservazione delle percentuali delle banche, risulta che l'età media si attesta intorno ai 59 anni, mentre si ritiene troppo elevata la percentuale di amministratori con più di 65 anni e troppo ridotta la percentuale di amministratori con meno di 50 anni. Infatti, se da una parte gli amministratori con un'età superiore a 65 anni sono garanzia di professionalità ed esperienza, dall'altra col tempo la loro influenza potrebbe compromettere l'indipendenza. Nello stesso tempo, una percentuale più elevata di amministratori più giovani può contribuire ad apportare competenze ed esperienze più prossime al presente e relative a contesti finanziari più attuali. L'affiancamento di queste competenze a figure di vertice con esperienze più significative, maturate sia sotto il profilo strategico che sotto il profilo professionale, potrebbe rappresentare un reale fattore di successo della *governance* delle banche.

Con riguardo al sistema dei controlli interni, si è osservato che nelle banche oggetto di valutazione risultano ben definite e separate le funzioni di controllo sia sul piano organizzativo che sul piano delle responsabilità. Tuttavia, si ritiene che per quanto riguarda la gestione dei rischi, soprattutto in ottica SREP, vadano ulteriormente implementati meccanismi di individuazione dei rischi di liquidità e di capitale che rappresentano una delle principali cause di perdite registrate dalle banche. Allo stesso modo, tali banche devono costantemente migliorare i propri flussi informativi attraverso l'adozione di sistemi, anche informatici, aggiornati ed evoluti che consentano di comunicare in maniera celere e diretta con i vertici.

A questo punto dell'elaborato si giunge alla conclusione secondo cui le quattro banche oggetto di valutazione, pur presentando un buon grado di adeguatezza ed efficienza della *governance* e del sistema dei controlli interni, evidenziano diversi spazi di miglioramento. Tale valutazione si riflette, in termini numerici, in un punteggio "SREP" pari a 3 che rileva aree di rischio associate a profili di criticità delle strutture di *governance*.

Il punteggio assegnato sembrerebbe coerente con i risultati SREP relativi al 2019 che hanno evidenziato profili di deterioramento della *governance* e lacune nei sistemi di controllo interno tanto che a tre banche su quattro è stato assegnato un punteggio pari a 3 e solo il 18% delle banche ha ottenuto un punteggio pari a 2, facendo registrare un peggioramento rispetto al 2018.

Il terzo capitolo si conclude con alcune considerazioni che, ripercorrendo gli obiettivi posti all'inizio della trattazione e le osservazioni svolte nello sviluppo dell'elaborato, conducono ad una riflessione finale sulla correlazione tra processo SREP e *governance* delle banche. Infatti, nonostante i punteggi non del tutto positivi, i risultati della valutazione svolta testimoniano una tendenza delle banche ad adeguare i propri assetti di *governance* alle previsioni della normativa di vigilanza bancaria e rispecchiano la crescente attenzione posta dalle banche al rispetto dei requisiti SREP.

In conclusione, si ritiene che la vigilanza svolta nell'ambito dello SREP possa rappresentare un incentivo affinché le banche implementino strutture di governo societario e di controllo interno sempre più adeguate ed efficienti.