Ottobre 2018

Linee guida EBA sulla Internal Governance: il ruolo del Board, del Risk Committee e della Risk Management Function

Luca Galli, Partner, Luca Ceccarelli, Senior Manager, EY

Le linee guida EBA in materia di Internal Governance (i.e. *"EBA Guidelines on Internal Governance under Directive 2013/36/EU"*, nel seguito, più brevemente, "Linee Guida"), pubblicate il 26 settembre 2017 e recentissimamente entrate in vigore (1° luglio 2018), si inseriscono in una articolata successione di disposizioni normative e regolamentari nonché in una fitta serie di standard di settore dedicati al governo societario (e al sistema di gestione dei rischi e dei controlli interni), idealmente ponendosi (a temporanea) chiosa di un percorso avviato con l'emissione della precedente versione delle Linee Guida intervenuta ormai oltre 6 anni fa (era il 26 settembre 2011), sulla scia dei conclamati fallimenti della *goverance bancaria* registrati tra il 2007 e il 2010 in quasi tutte le latitudini[1].

In tale contesto le nuove Linee Guida EBA – in continuità con le sempre più pervasive disposizioni europee e ai sempre più insistiti interventi di *moral suasion* da parte di BCE[2] - pongono particolare enfasi sui doveri e sulle responsabilità dell'organo amministrativo nella sua funzione di supervisione nel controllo dei rischi, dando - nel contempo - particolare rilievo alla gestione strategica dei rischi tramite il sempre più centrale ruolo assunto dal Comitato Rischi e dal responsabile della funzione di Risk Management (argomenti su cui si appunterà il focus di approfondimento qui offerto - *cfr. infra*).

Tali linee guida mirano ad armonizzare ulteriormente le modalità, i processi e i meccanismi di governance interna delle istituzioni bancarie in tutta l'Unione Europea, in linea con le nuove esigenze introdotte dalla direttiva sui requisiti patrimoniali (CRD IV) e tenendo conto anche del principio di proporzionalità.

Complessivamente le linee guida traguardano un paradigma che potremmo definire di "governance aumentata", il quale ricomprende, *inter alia*:

[1] … e che comunque, da lì a poco, avrebbero raggiunto le latitudini ancora inesplorate dalle crisi bancarie (tra cui la nostra).

[2] Si confronti – quale epitome tra i plurimi interventi di BCE sulla governance – quello di Danièle Nouy (Presidente del Supervisory Board di BCE) "*Good governance for good decisions" tenuto il 22 marzo 2018 a Francoforte sul Meno.*

- le usuali disposizioni in materia di governo societario, essenzialmente riconducibili al ruolo e alla composizione degli Organi Aziendali e dei Comitati endo-consiliari;
- un'estensione del dominio della governance "oltre i confini" della singola entità giuridica e che determina a valere sugli Organi Aziendali della Capogruppo particolari responsabilità relative alla conoscenza e alla gestione della complessiva struttura societaria in cui si articola e ramifica il Gruppo Bancario di riferimento (il cd. "Know Your Structure");
- il totem della Risk Culture, abbinato nelle Linee Guida ai principi etici e di comportamento, ai conflitti di interesse e al Whistleblowing;
- il "Sistema dei Controlli Interni" rappresentato nella canonica conformazione piramidale dei controlli di primo, secondo (Risk Management e Compliance) e terzo livello (Internal Audit), ma che ricomprende altresì un'ampia digressione riservata ai processi di approvazione dei nuovi prodotti e di entrata in nuovi mercati[3].

Focus: la gestione strategica dei rischi e il ruolo del Board, del Comitato Rischi e del Risk Management

In tanta copia di argomenti, la scelta del presente intervento è ricaduta su quello che riteniamo il tema di maggiore rilievo, complessità e – sia detto – preoccupazione per gli Organi Aziendali: ovvero la gestione strategica, il monitoraggio e la supervisione dei rischi aziendali.

La trattazione qui proposta segue un percorso piuttosto semplice, ma serrato e concreto, idealmente articolato in tre tappe cruciali, i.e.:

- il ruolo, le responsabilità, le aspettative (del *regulator*) e le aspirazioni / ritrosie del Board in tema di gestione strategica dei rischi;
- il rinnovato ruolo del "Comitato Rischi";

[3] Tema che va oltre le finalità che il presente intervento vuole traguardare, ma che certamente sta assumendo sempre più una valenza strategica per le banche. A tal proposito, sia consentito fare rinvio a:
(i) alle disposizioni MIFID2 sulla Product Governance;
(ii) alle "*EBA - Guidelines on product oversight and governance arrangements for retail banking products* emesse il 22 marzo 2016";
(iii) alla modifica alle Disposizioni "Trasparenza delle operazioni e dei servizi bancari e finanziari. Correttezza delle relazioni tra intermediari e clienti" (Provvedimento della Banca d'Italia del 29 luglio 2009 e successive modificazioni, la cui entrata in vigore è prevista il 1° gennaio 2019);
(iv) agli *Orientamenti EIOPA preparatori sulle disposizioni in materia di governo e controllo del prodotto da parte delle imprese di assicurazione e dei distributori di prodotti assicurativi* che integrano le disposizioni della Direttiva 2014/97 (cd IDD) del 20 gennaio 2016, la cui entrata in vigore è prevista per il 1° ottobre 2018, e che per la parte distributiva dovranno essere applicate anche dalle banche.

- il principale fattore abilitante: la Risk Management Function (RMF) e il suo responsabile.

Il Board

I cicli SREP intervenuti negli ultimi 4 anni nell'era del *Single Supervisory Mechanism*, l'inanellarsi delle diverse *Thematic Review (*ad esempio quella relativa *a Risk Governance & RAF*), per non dire delle pressoché ininterrotte e diuturne attività di "*on site inspection*" a valere sugli specifici profili di rischio condotte dagli onnipresenti "Team di Supervisione Congiunta" (Joint Supervisory Team, *vulgo* "JST"), restituiscono un messaggio forte e chiaro: la Risk Governance è il primo e costitutivo elemento oggetto di pervasivo scrutinio e assidua valutazione da parte del Supervisor e a cui guardano – di riflesso – gli analisti e, più in generale, la comunità finanziaria nonché, con crescente interesse, gli organi di stampa, i media e, di conseguenza, la parte più avveduta dell'opinione pubblica (o sicuramente quella più attenta alle dinamiche finanziarie ed economiche del nostro paese).

Lo spirito delle Linee Guida da questo punto di vista risulta assecondare tale trend, rimarcando la chiara e irrefutabile responsabilità degli amministratori nell'esercizio delle proprie funzioni di supervisione strategica a valere sulle strategie di governo, gestione, supervisione e monitoraggio dei rischi aziendali.

Siffatta responsabilità si configura come stella polare nel complessivo universo dell'Internal Governance, ma non rappresenta invero per gli "addetti ai lavori" una novità assoluta e dirompente nell'economia della governance bancaria. Purtuttavia le richieste derivanti dalle Linee Guida EBA pongono nuovi e interessanti prospettive di analisi all'interno delle quali è facile collocare opportunità di intervento volte a rafforzare il framework e i meccanismi di governo strategico e operativo dei rischi aziendali.

Da una prospettiva più pragmatica la vera sfida sollecitata dalle Linee Guida è quelle di definire soluzioni organizzative ed operative adeguate e che possano fornire una sorta di "assurance" al Board tramite il ponderato rafforzamento e nel contempo (e a seconda dei casi) l'intelligente razionalizzazione della filiera in cui si articola la Risk Governance e che pervade l'intera banca, ovvero: dalle funzioni di business e operative ("risk taker"), alle Funzioni Aziendali di Controllo di 2° e 3° livello ("risk controller"), passando per i Comitati Tecnici/Manageriali, fino al coinvolgimento dei Comitati endo-consiliari e del Board stesso ("risk oversighter").

Come preannunciato nella premessa del presente focus, la disamina del *Risk Governance framework* qui proposta si ispira – secondo una logica consolidata in letteratura e, peraltro, auspicata dal Regulator / Supervisor in tutte le sue diverse funzioni (regolatoria, ispettiva e "afflittiva") – ad un approccio top-down, dall'alto verso basso e che, quindi, non può che partire dal ruolo e dalle responsabilità del Board in tema di governo strategico dei rischi.

Anzitutto il Board è chiamato ad una efficace ed efficiente, ma soprattutto consapevole, definizione delle strategie aziendali secondo logiche di rischio/rendimento e che, nel contempo, salvaguardino elementi quali stabilità e sostenibilità dell'istituto nella consueta prospettiva della "sana e prudente gestione".

Per realizzare tale compito il *Board* opera attraverso l'organo con funzione di supervisione strategica (OFSS) che è chiamato, *inter alia*, a (i) declinare l'articolazione organizzativa della Risk Governane (e.g. integrando il mandato dei comitati endo-consiliari, auspicando la costituzione di comitati gestionali, etc.); (ii) definire i "meccanismi di funzionamento" (es. e.g. articolando le modalità di interlocuzione tra Organi e Funzioni di Controllo e tra Funzioni di Business e Funzioni di Controllo).

Se ci si sofferma sui compiti e sulle responsabilità del Board (compiti puntualmente delineati nelle Linee Guida EBA) emerge in modo evidente che (limitandosi al solo ambito di *risk management*) il Board debba essere primariamente in possesso di profonde competenze di tipo tecnico-specialistico che possano consentire al Board stesso – sia pur nella sua più ampia compagine - di assumere consapevolmente le complesse deliberazioni di sua propria competenza in materia di definizione della strategia di rischio e sua supervisione.

Non è il caso qui di indugiare sulle tematiche di "fit & proper" e "suitability" dei membri del Board oggetto anch'esse di recente revisione da parte della BCE (i.e. *Guide to fit and proper assessments* – maggio 2018) nonchè di EBA ed ESMA (i.e. *Joint ESMA and EBA Guidelines on the assessment of the suitability of members of the management body* entrate in vigore il 30 giugno 2018); disposizioni il cui recepimento e declinazione è in corso da parte del MEF.

Il Comitato Rischi

In via generale, la complessità del contesto esterno nonché la trasversalità delle tematiche che sono sottoposte alla continua valutazione e successiva consapevole approvazione da parte dell'OFSS, anche alla luce delle Linee Guida qui in commento, implicano un ruolo sempre più operativo dei Comitati endo-consiliari.

In particolare, in materia di governo dei rischi e Risk Strategy il Comitato Rischi è chiamato ad assumere un ruolo vitale che trova *in primis* attuazione nei meccanismi di reporting del Comitato verso gli Organi Aziendali e nelle modalità di interrelazione con le Funzioni di Business (CFO, CLO, CCO) e le Funzioni Aziendali di Controllo (CRO).

In tale scenario il Comitato Rischi risulta sempre più "attratto" (nel continuo) all'interno dei tipici framework di gestione e governo dei rischi. Qui concretamente ci si riferisce al coinvolgimento nella definizione e costante monitoraggio del Risk Appetite Framework, all'ICAAP / ILAAP e quindi anche processi di pianificazione strategica: coinvolgimento da situarsi temporalmente prima della presentazione e discussione in seno al Board.

L'attrazione e il coinvolgimento in tali framework si attua prevedendo sessioni di approfondimento e discussione nelle riunioni del Comitato Rischi.

In tale contesto appare del tutto cogente la necessità di procedere rapidamente ad un rafforzamento degli strumenti informativi e reporting predisposti dalle funzioni tecniche specialistiche (tipicamente CRO e CFO) a disposizione del Comitato Rischi per l'esercizio delle proprie funzioni: una reportistica di rischio che consenta una immediata scalabilità e una razionale correlazione tra le informazioni critiche "da Executive Summary", con le viste di dettaglio sui singoli profili di rischiosità.

E ancora, sempre secondo le Linee Guida, il ruolo del Comitato Rischi diventa sempre più incisivo in riferimento a:

- alle valutazioni derivanti dagli scostamenti del *Risk Profile* rispetto alla *Risk Strategy* definita (ciò non solo per i *breach* di *Risk Tolerance* e *Capacity*, ma anche in caso di scostamento dal *Risk Appetite*);

- all'attività di advising a favore dell'OFSS a presidio dei cambiamenti del contesto esterno, del *Business Model* e dell'emissione di nuovi prodotti e dell'ingresso in nuovi mercati (si pensi a quanto rapidamente riportato in una nota più sopra, riguardo alla cd. "*Product Oversight Goverance"* relativa ai nuovi prodotti finanziari, bancari e assicurativi).

In merito a questo ruolo di advisor, particolare attenzione deve essere posta riguardo al presidio delle dinamiche attese (*forward-looking*) derivanti da analisi di scenario, valutate anche in condizioni avverse (*Stress Test Scenario*), ciò al fine di consentire una valutazione compiuta della capacità di reazione della banca ai cambiamenti interni ed esterni.

In altre parole il ruolo attribuito dalle Linee Guida al Comitato Rischi sembra indulgere verso un'applicazione molto operativa: al *Risk Committee* viene richiesto di entrare in modo maggiormente pervasivo nei processi di definizione e declinazione della *Risk Strategy*, naturalmente senza assumere un ruolo propositivo, ma con l'intento di porre in esser quel sano *challenge* sulle funzioni gestorie (CEO e/o Comitato con deleghe esecutive) deputate a conseguire gli obiettivi strategici in linea con gli indirizzi del Board.

Tale ruolo opportunamente declinato operativamente rafforza senza dubbio il principio cardinale del "*check and balance"*, a tutela delle responsabilità in capo al Board, aspetto – quest'ultimo – particolarmente critico agli occhi del Supervisor, specialmente in quelle realtà aziendali dove "storicamente e culturalmente" le figure gestorie evocano (*rectius*: evocavano, sperabilmente) poteri pressoché infiniti ed incontrollabili, quasi "sovraordinati e superiori" a quelli del Board stesso.

In tale prospettiva un percorso di sano e concreto miglioramento del modello di funzionamento del Comitato Rischi potrebbe passare da una *review* critica delle

procedure e dei processi operativi sottesi ai *framework core* in ottica di Risk & Business Strategy, quali ad esempio il RAF, ICAAP, ILAAP, Processi di gestione dei rischi e Recovery Plan.

La richiamata revisione dovrebbe essere condotta al fine di identificare in sede di definizione delle *Risk Strategy* "momenti istituzionali" di confronto e di dialettica discussione, basati anche su *preliminary outcomes* forniti dalle funzioni di controllo e di business al *Risk Committee* in modo da avviare successivi approfondimenti, permettendo al Comitato stesso di esplicare concretamente la richiamata funzione di supporto ed *advice* verso il Board.

Per agevolare l'operato del Comitato Rischi e rendere efficienti i meccanismi di funzionamento, la preventiva pianificazione delle sedute nonché la preordinata identificazione dei contenuti da sottoporre al Comitato stesso in ottica di programmazione periodica delle attività si configura certamente come un utile, se non vitale, fattore abilitante (i.e. calendario programmatico dei lavori del Comitato Rischi).

Infine – atteso il ruolo attribuito al *Risk Committee* dalle Linee Guida EBA di supervisionare la corretta implementazione delle *Risk Strategy* – si ritiene auspicabile che il Comitato Rischi sia coinvolto ed informato in modo tempestivo anche in caso di sforamenti dei limiti operativi / limiti di *Risk Appetite*, malgrado questi siano contenuti entro livelli di *Risk Tolernace* e *Capacity*[4].

La funzione di "Risk Management" (e il suo Responsabile)

Sin qui si è detto dei ruoli, dei compiti e delle responsabilità degli Organi Aziendali (i.e. Board, OFSS e Comitato Rischi), ma un altrettanto ruolo vitale è assegnato dalle Linee Guida alla funzione di Risk Management (e al suo Responsabile).

In una battuta e attingendo alla lingua inglese – meglio attrezzata e più diretta della nostra su tali materie – potremmo dire che la transizione indirettamente invocata dalle Linee Guida è la seguente "*from a Risk Control Function … to a Risk Management Function"*.

Il "nuovo" paradigma della Risk Management Function (RMF) può essere colto guardando soprattutto ai meccanismi di funzionamento dei comitati gestionali/manageriali, e quindi, in particolare:

- al rafforzamento dei momenti di valutazione, discussione approvazione delle proposte afferenti le «single risk strategy» supportate da tempestive analisi *risk sensitive/oriented* messe a disposizione dalla Funzione di Risk Management alle funzioni di business;

[4] Naturalmente il superamento dei limiti di Risk Tolerance e Capacity già ad oggi comportano un coinvolgimento diretto degli Organi Aziendali (tipicamente Board con passaggio preventivo in Comitato Rischi).

- alla definizione di meccanismi partecipativi del Responsabile della RMF (ovvero di personale della RMF opportunamente delegato) per assicurare un presidio costante e diffuso nonché di supporto al *«decision making process»*;

- all'integrazione e al consolidamento degli strumenti di governance a disposizione del Responsabile della RMF per assicurare un effettivo ed efficace *challange* sulle decisioni prese dalle funzioni di Business (es. *risk opinion e veto power*).

Soffermandoci sul rapporto tra Responsabile della RMF e le funzioni di business, possibili interventi atti a rafforzare i suddetti meccanismi possono riguardare il ruolo del Responsabile della Funzione RMF all'interno dei comitati gestionali/manageriali (es. Comitato Direttivo, Comitato Finanza, ALM, etc.). Questi ultimi tipicamente rappresentano il "luogo istituzionale" dove sono:

- discusse e tracciate le proposte relative alla *business and risk strategy* in tutte le loro articolazioni e declinazioni (i.e. Capital Plan, Funding Plan, politiche creditizie/Commerciali etc.) e che successivamente sono portate all'attenzione del *Board* per il tramite dell'organo gestorio;

- presentate e discusse le dinamiche andamentali (aderenza alle linee strategiche), i *risk limits breachs* e identificate le più opportune azioni di mitigazione e rimedio.

È cosa risaputa che già oggi il Responsabile della RMF è usualmente presente in tali sedi istituzionali secondo eterogenei meccanismi di coinvolgimento. Tanto premesso, nella prospettiva delle Linee Guida, si tratta di prevedere interventi capaci di preservare in maniera più robusta i principi di *"check & balance"* e indipendenza, più volte invocati all'interno delle Linee Guida.

In particolare, tali interventi potrebbero concretizzarsi attraverso una review critica dei modelli di funzionamento dei comitati gestionali/manageriali prevedendo una *mission* chiara degli stessi, orientata a definire le strategie di rischio/rendimento basata su informazioni *risk sensitive* messe tempestivamente a disposizione da parte dalla funzione di Risk Management. All'interno dei comitati dovrà essere previsto il coinvolgimento del Responsabile della RMF come membro "senza diritto di voto", ma con la possibilità - a valere sulle proposte delle Business Function - di prevedere la redazione di una *Risk Opinion* da allegare alla proposta stessa a supporto della successiva valutazione degli Organo Aziendali.

Tali previsioni (i.e. partecipazione senza diritto di voto e possibilità – ovvero obbligo – di redigere la *Risk Opinion*) applicate sia in sede di set up delle strategie e sia in caso di definizione delle azioni di rimedio a seguito dei *risk limit breachs*, comportano la definizione di meccanismi di escalation e, auspicabilmente, una revisione dei poteri e delle deleghe operative, sulla falsa riga di quanto già accaduto con l'introduzione delle disposizione sulle "Operazioni di Maggior Rilievo" e, soprattutto, con l'intento di disciplinare compiutamente il percorso di approvazione/autorizzazione in caso di *Risk*

Opinion negativa (ovvero nei casi estremi di applicazione del "veto power" da parte del Responsabile della Funzione Risk Management).

Il richiamato percorso di revisione dei modelli di funzionamento dei comitati gestionali, in ossequio alle logiche dianzi descritte, potrebbe presentare delle "aree di sovrapposizione" rispetto a quanto, già oggi, viene svolto in alcune banche all'interno del "Comitato Rischi Manageriale". Nel modello qui auspicato tale Comitato dovrebbe evolvere verso una funzione squisitamente tecnico specialistica orientata al presidio delle metriche /modelli di risk management e alla diffusione presso l'organizzazione (in particolare verso il Top Management nonchè nei confronti delle funzioni di business) della *Risk Culture* attraverso mirate sessioni di discussione circa la valutazione del profilo e della dinamica dei rischi.

Conclusioni

Una lettura *prima facie* delle Linee Guida EBA in materia di Internal Governance potrebbe far ritenere che – in *special modo per il mercato italiano, ove gran parte dei principi in materia di governo societario e dei rischi erano già stati oggetto di disciplina da parte del Regolatore domestico (Cfr. Circolare Bankit 263 e poi 285 nelle varie novelle)* – quanto previsto dalle Linee Guida sia già adeguatamente regolamento e quindi (in teoria) applicato dalle nostre banche.

Nondimeno se si riuscisse a cimentarsi nel non semplice compito di porsi nei pensieri del Regolatore Europeo e nelle vesti del Supervisore ispettivo (come qui si è faticosamente cercato di fare), sarebbe possibile trarre dalle Linee Guida EBA ispirazione e impulso per definire calibrati interventi sul complessivo assetto di *Risk Governace* e sulle sue declinazioni operative.

Si tratta di interventi improntati a scelte virtuose e di facile implementazione guidate da un duplice spirito: uno "più nobile" di continuo miglioramento della governance dei rischi e l'altro "più prosaico" finalizzato a rispondere con sempre maggiore tempestività, rigore e forza alle sempre più varie sollecitazioni rivenienti dall'esercizio del *Supervisory Review and Evaluation Process*, con particolare riferimento alla componente di *Internal Governance e Risk Management.*