POSITION PAPER N° 24

Governance e strategia per la gestione dei rischi nelle imprese non finanziarie

AIFIRM
Associazione Italiana Financial Industry Risk Managers

Novembre 2020

AIFIRM RINGRAZIA

IL COMITATO GUIDA

COORDINAMENTO SCIENTIFICO

- **Cesare Conti** (Università Bocconi e Board Member)
- **Paola Schwizer** (Università di Parma)

COORDINAMENTO AIFIRM

- **Floricel Rugiero** (Enel S.p.A)

COORDINAMENTO TECNICO E PROJECT MANAGEMENT

- **Riccardo Bua Odetti** (PwC)
- **Giacomo Guerrini** (PwC)

IL GRUPPO DI LAVORO

- **Cristiano Bartalena** (Poste Italiane)
- **Filippo Bettini** (Pirelli)
- **Stefano Capodagli** (AIFIRM)
- **Lorenzo Cella** (Pirelli)
- **Angelo Cortese** (CDP/CDP Equity)
- **Luigi de Luca** (AIFIRM)
- **Andrea Dupont** (Banca Carige)
- **Andrea Giacchero** (AIFIRM)
- **Fabio Giovannini** (TIM)
- **Jennifer Hoffman** (Columbia University)
- **Stefano Orsini** (Luxottica)
- **Gabriele Palandri** (TIM)
- **Paolo Palliola** (Crédit Agricole Italia S.p.A.)
- **Ornella Perfetti** (Eni S.p.A.)
- **Roberto Rentocchini** (Eni S.p.A.)
- **Alessia Ruggeri** (TIM)
- **Carlo Zaganelli** (Leonardo S.p.A)

Si ringraziano i partecipanti alla Commissione che hanno contribuito a livello personale senza alcun tipo di adesione o avallo da parte delle Società o Enti verso i contenuti del presente position paper.

ISBN: 979-12-80245-03-8
DOI: 10.47473/2016ppa00024

SOMMARIO

ABSTRACT

The "Corporate Risk Governance & Control" Commission, composed of risk managers, working for the top leading companies and financial institutions, many of which are publicly listed, as well as academics and board members, worked together to produce a position paper that aspires to provide principles and best practices regarding strategic risk management and risk governance.

In particular, the document provides a framework, applicable to non financial companies based on their specific profiles, that integrates the general requirements established by the standard setters (i.e. the Code of Corporate Governance for publicly listed companies, the COSO Framework 2017, ISO 31000:2018 and banking and financial sector regulations) while taking into consideration elements of differentiation, uniqueness and different organizational and managerial approaches to affront risk

The document is composed of two main sections: "Risk Governance" and "Risk & Strategy". In the first section, roles and responsibilities regarding risk management are addressed, starting from the importance to diffuse a risk culture consistent with mission, vision and company values to outlining the benefits of adequate organizational principals and governance. Once clarifying the difference between the first, second and third level of defense, the section concludes with a detailed analysis dedicated to the role of the Chief Risk Officer, in which the requirements of professionalism and independence are underlined as well as the key role played in the consolidation of a holistic view of the risk profile within the organization. In the second section of the position paper, ample space is dedicated to the Risk Appetite Framework, a fundamental tool to connect the business strategy and punctual risk quantification. The objective is to offer guidelines to define the risk appetite within a company. The final section of the paper proposes some suggestions for risk classification considering a portfolio view, as well as ulterior reflections regarding risk quantification, highlighting also some of the principle approaches to targeted evaluations and the drafting of a strategic plan pondered around risk.

Obiettivo della Commissione "Corporate Risk Governance & Control", composta da *risk manager* operanti in aziende *corporate* e realtà finanziarie italiane di primaria rilevanza, prevalentemente quotate, accademici e consiglieri di amministrazione, è stato lo sviluppo di un *position paper* che aspira a delineare principi e *best practice* in tema di gestione strategica e *governance* dei rischi.

In particolare è stato sviluppato un *framework*, applicabile alle aziende non finanziarie in base ai rispettivi profili di specificità, che integra i requisiti generali stabiliti dagli *standard setter* di settore (i.e. Codice di Corporate Governance per le società quotate, COSO Framework 2017, ISO 31000:2018 e normative per il settore bancario e finanziario), considerando i potenziali elementi di differenziazione, le specificità e i differenti approcci organizzativi e gestionali dei rischi a cui le stesse possono essere esposte.

Il risultato è un documento articolato in due macro-sezioni. Nella prima, "Risk Governance e Risk & Strategy", si affrontano i temi legati a ruoli e responsabilità in tema di gestione e controllo del rischio, muovendo dall'importanza della diffusione di una cultura del rischio coerente con *mission*, *vision* e valori di fondo dell'azienda, e delineando i benefici di adeguati presidi organizzativi e di *governance*. Dopo aver chiarito la differenza tra i controlli di primo, secondo e terzo livello, la sezione si conclude con un approfondimento dedicato alla figura del *Chief Risk Officer*, di cui si evidenziano i requisiti di professionalità e indipendenza e il ruolo centrale per il consolidamento della visione complessiva del profilo di rischio dell'azienda. Nella seconda parte del *paper*, ampio spazio è dedicato al *Risk Appetite Framework*, strumento fondamentale per il raccordo tra la strategia aziendale e la quantificazione puntuale dei rischi ad essa sottesi. L'obiettivo è quello di fornire linee guida per la definizione della propensione al rischio dell'azienda. Una sezione operativa finale propone alcuni spunti per la classificazione dei rischi in una logica di portafoglio, nonché ulteriori riflessioni circa il grado di misurabilità degli stessi, passando in rassegna alcuni dei principali approcci di valutazione mirati alla stesura di un piano strategico aziendale ponderato per il rischio.

INTRODUZIONE

Il *paper* si propone di rappresentare le linee guida per la gestione ed il controllo dei rischi nelle imprese non finanziarie, soprattutto (ma non solo) quotate, anche mutuando dalle prassi già consolidate degli intermediari finanziari.

In particolare, nella prima parte sono individuati i *driver* per un'efficace *governance* dei rischi, non solo con riferimento ai requisiti regolatori per le società quotate. Un'efficace *risk governance* è infatti fondata sull'attivazione di idonei presidi organizzativi, sull'applicazione di modelli di riporto tempestivo agli Organi di controllo e gestione, sulla chiara identificazione di *mission*, ruoli e responsabilità per salvaguardare il raggiungimento degli obiettivi di *performance* e la loro sostenibilità nel tempo. In tale contesto, la definizione degli obiettivi di *performance* non può prescindere dall'analisi dei rischi connessi alla stessa attività di impresa e all'attuazione delle strategie; pertanto, come si rappresenterà nella seconda parte del *paper*, saranno identificate le fasi logiche di un processo valutativo (o di quantificazione) dei rischi di piano (industriale) che si fonda sull'individuazione dei fattori abilitanti dello stesso, della quantificazione - ove possibile - dei rischi connessi alla strategia definita e dell'impatto potenziale sui risultati di *business* rappresentati nel Piano strategico.

In **La cultura del Rischio: *mission*, *vision* e *core values*** sono definiti la *Risk Culture* e individuati alcuni strumenti utili alla sua diffusione dai livelli apicali di gestione e controllo (*Board*, Consiglio di Amministrazione, Comitato Controllo e Rischi) alle aree di *business*. La presenza di una diffusa cultura del rischio in azienda, dal vertice alle strutture di *business*, è infatti una condizione necessaria, anche se non sufficiente, ad abilitare i processi di gestione e controllo del rischio e a garantirne un ruolo non solo di *compliance* ma di efficace supporto alla salvaguardia del *business*.

Successivamente si delinea il **ruolo del *Board* e del Comitato controllo e rischi,** non solo in termini di "compiti" formali attributi dalla normativa di riferimento, ma anche traendo ispirazione dal modello di gestione dei rischi tipico del mondo delle istituzioni finanziarie spinto da un approccio rigoroso e sistematico, rappresentando gli elementi informativi necessari a una maggiore consapevolezza nell'assunzione delle decisioni strategiche.

A seguire è definito il **ruolo di eventuali *Risk Committees* manageriali** che, seppur non richiesti dalla regolamentazione in materia, in diverse realtà costituiscono il canale di trasmissione tra le scelte degli Organi deputati alle decisioni strategiche e le unità di *business*, per il tramite delle Funzioni o Unità di Gestione e Controllo dei rischi, e con ruolo di diffusione della *Risk culture* secondo un approccio integrato.

Anche laddove ci siano meccanismi di coordinamento fluidi, una struttura di *governance* dei rischi efficace deve essere fondata su tre pilastri ben distinti: **Il controllo di primo, secondo e terzo livello nelle *corporate*.** Nel paragrafo dedicato sono pertanto individuati i requisiti affinché siano stabilite tre linee di difesa indipendenti, ma complementari e non antitetiche o ridondanti. Il controllo di primo livello, effettuato da unità organizzative allocate nelle aree di *business*, è diretto ad assicurare il corretto svolgimento delle operazioni, inclusa la realizzazione delle azioni operative per l'efficace mitigazione dei rischi. Il controllo di secondo livello - o controllo sulla gestione dei rischi – deve essere affidato a unità diverse da quelle operative, con la responsabilità della validazione dei rischi identificati, della definizione di politiche e metodologie volte a misurarli e controllarli, assicurando il rispetto delle norme interne ed esterne e dei regolamenti. I controlli di terzo livello - internal audit - sono finalizzati alla valutazione e verifica periodica della completezza, adeguatezza, funzionalità e affidabilità dei processi aziendali e del sistema dei controlli interni. L'attività è condotta da strutture diverse da quelle operative e di controllo di secondo livello.

Alla luce dei principi di *Risk Governance* d'impresa, sempre più spesso il responsabile della funzione (o unità) di *risk management*, dove esistente, prende la denominazione di ***Chief Risk Officer***, o più brevemente CRO. Il CRO, non gestisce i rischi aziendali, ma governa il processo di analisi e gestione dei rischi che ricade sotto la responsabilità dei *risk owner*, favorisce il dialogo, guida i colleghi a livello metodologico, integra le informazioni provenienti dalle diverse funzioni in modo da consolidare una visione complessiva del profilo di rischio dell'impresa a supporto della definizione delle strategie. Il paragrafo focalizza quindi il ruolo del CRO evidenziandone la propria funzione a supporto della

complessiva *governance* d'impresa, i modelli di riporto possibili per la funzione rappresentando i pro e i contro di ogni impostazione, distinguendo, infine, le differenti prerogative e responsabilità della funzione (o unità) di *Compliance**.***

Dopo aver delineato i requisiti principali della *Risk Governance* di *best practice*, nella seconda Parte sono identificate le linee guida affinché la valutazione dei rischi e le attività di controllo di secondo livello possano adeguatamente supportare il processo decisionale della strategia di impresa.

Lo strumento per l'attuazione di quanto sopra, è rappresentato dal "***Risk appetite framework***" **– "RAF"** (sistema degli obiettivi di rischio), requisito regolatorio introdotto già dal 2013 per gli intermediari vigilati, che rappresenta la visione "top-down" del vertice aziendale, coerente con la strategia di lungo periodo, del rischio (natura e *quantum*) che si intende assumere, ottimizzandolo sulla frontiera efficiente rischio-rendimento, e di quello che si intende evitare. Nel paragrafo dedicato, partendo dall'assunto che non esiste un approccio standard alla definizione della propensione al rischio e che spetta – tendenzialmente, almeno nelle istituzioni finanziarie - al CdA approvarla e al *management* applicarla e darne adeguata comunicazione ai vari livelli dell'azienda, sono descritte linee guida per la definizione di un modello di *Risk Appetite* che da un lato richiede - e nel contempo produce - il rafforzamento di una cultura del rischio all'interno della società attraverso un approccio strutturato, dall'altro incorpora gli obiettivi del Vertice, in termini di *business* e di rischio, e le aspettative dei principali *stakeholder*. In tale ambito saranno forniti cenni anche ai concetti di *Risk Appetite Statement*, *Risk Tolerance* e *Risk Capacity*.

Il processo decisionale di definizione ed approvazione della strategia, tradizionalmente separato dall'*assessment* e monitoraggio dei rischi, secondo la best practices dovrebbe, ove possibile, essere rafforzato con una puntuale identificazione e quantificazione (o almeno valutazione) dei rischi ad essa sottesi. In un contesto di volatilità dei mercati, di manifestazione di nuovi rischi emergenti fino ad oggi non misurati (almeno non sistematicamente), di accresciuta incertezza del contesto interno ed esterno all'impresa, la fase di definizione dei driver di piano nonché della definizione *ex ante* di soglie o limiti di rischio da allocare ai *risk owner*, risulta fondamentale. Nel paragrafo **Decisioni strategiche e loro declinazione nell'organizzazione aziendale** sono pertanto delineate le linee guida metodologiche per la definizione di *risk factors* che, alla base della declinazione del piano strategico, consentono (o minano) il raggiungimento dei *target* economici e finanziari nello stesso dichiarati. Dopodiché viene definito un possibile processo di allocazione di limiti di rischio (*ex ante*) ai diversi fattori di rischio, il relativo monitoraggio, gli *step* per un'efficace gestione degli sconfinamenti di soglie o limiti (con il coinvolgimento anche dei Comitati manageriali o degli Organi formali). Il processo di allocazione di limiti di rischio e di monitoraggio degli stessi – per una sana e prudente, ed anche efficace, gestione – deve necessariamente prevedere *step* definiti formalmente in documentazione organizzativa interna (linee guida, disposizioni, *policies,* procedure, coerentemente con gli standard organizzativi della corporate), affinché se ne garantisca l'attuazione e si assicuri il coinvolgimento degli Organi deputati alla definizione della strategia con la consapevolezza anche dei rischi connessi.

Successivamente, si propongono alcuni spunti per una possibile **Classificazione dei rischi** che dovrebbe supportare, con una logica di portafoglio, la valutazione del profilo di rischio dell'organizzazione nel suo complesso, favorendo l'identificazione delle principali tipologie di rischio e considerando l'eventuale loro interrelazione; non esistendo un approccio *one fits all*, sarà necessario modellare la proposta di classificazione a seconda del settore industriale, della tipologia di *business* e della grandezza e complessità dell'organizzazione.

Una volta individuati e classificati i rischi, ulteriori riflessioni possono essere fatte in relazione al loro grado di misurabilità - **Rischi valutabili quantitativamente versus qualitativamente**. Una analisi di tipo quantitativo presuppone l'esistenza di dati storici (e robusti) per la modellizzazione e la definizione di scenari probabilistici attesi che, soprattutto nel caso dei rischi emergenti – non sempre è disponibile. Le "*what if analysis*"| *"scenario analysis"* (anziché l'implementazione di modelli probabilistici – stocastici) possono comunque trovare applicazione per fornire valutazioni sulla probabile realizzazione dei *target* finanziari ed economici dichiarati; nondimeno la quantificazione dei rischi consente di misurare l'impatto economico e/o finanziario sugli obiettivi di Piano strategico (Capitale, EBIT, EBITDA, etc.). Prevedere quindi una fase di ***Risk assessment*** **con simulazioni di rischio atteso e impatti sul Piano** consente di definire *target* di Piano differenziati in relazione ai diversi scenari di rischio e di dichiarare obiettivi effettivamente raggiungibili, prevedendo tempestivamente le necessarie azioni di

mitigazione, in caso di manifestazione, garantendo la sostenibilità nel tempo dei *target* dichiarati e dell'impresa nel suo complesso.

1 RISK GOVERNANCE

1.1 La cultura del rischio: mission, vision e core values

Il rischio è parte integrante del *business* di qualunque impresa. Esso è generato dalla variabilità di fattori interni ed esterni, la cui comprensione è necessaria per un efficace ed efficiente esercizio delle attività di impresa. Buone pratiche di *risk management* e, più in generale, processi di governo del rischio ben definiti contribuiscono a una gestione aziendale sana e prudente. A tal fine, il *management*, responsabile della gestione e del controllo del rischio, ha anche il ruolo di garantire una comunicazione fluida e aperta in tema di rischi a tutti i livelli aziendali, sia verso gli organi societari sia verso le aree di *business*, ed esternamente nei confronti degli *stakeholder* rilevanti. Tali flussi informativi sono da considerarsi parte integrante del processo di gestione, monitoraggio, misurazione e controllo dei rischi.

La cultura del rischio è parte della cultura organizzativa di ogni realtà aziendale, ma assume particolare rilevanza perché determina il modo in cui una determinata impresa valuta e gestisce i rischi che possono compromettere il raggiungimento degli obiettivi strategici. Se la cultura organizzativa, intesa nel senso più ampio, come insieme di valori condivisi e convinzioni di fondo che influenzano il comportamento e l'atteggiamento degli individui nel proprio ambiente professionale, assume grande importanza ai fini del processo di creazione del valore all'interno di un'impresa, ancor più una cultura che favorisce un'efficace gestione del rischio può incoraggiare la comunicazione, la condivisione delle conoscenze e delle migliori pratiche, il miglioramento continuo dei processi e un forte impegno nei confronti di comportamenti aziendali etici e responsabili in tema di assunzione di rischi. In generale, una cultura sana e coerente con la formula imprenditoriale scelta da un'azienda può contribuire in modo significativo a migliorare le prestazioni aziendali. Ciò richiede tuttavia che le persone interpretino tale cultura, comportandosi in conformità con i valori dell'azienda e declinando, nei propri comportamenti, la sua stessa identità.

I valori costituiscono il fondamento della cultura di un'azienda. Per valori d'impresa (*values o core values*) si intendono genericamente i principi cardine che ispirano e condizionano il modo di agire dell'azienda e dei suoi dipendenti, nel rispetto della *vision* e della *mission* dichiarate; si tratta cioè di un sistema di idee, modi di agire e attributi considerati "importanti" e quindi tali da informare l'azione dell'impresa. Molte realtà aziendali li diffondono anche attraverso la *Dichiarazione dei Valori* (o *Value Statement*), un documento formale che esprime il sistema di valori propri della società, quali ad esempio la qualità, la responsabilità, l'equità, l'etica, la collaborazione, l'efficienza, etc.

Mission e *vision* sono elementi fondamentali per identificare e rappresentare l'identità di un'azienda. Servono a comunicare l'obiettivo che essa intende raggiungere e i traguardi prefissati. La *mission* descrive l'obiettivo aziendale, da intendersi anche come la motivazione che ha portato alla costituzione dell'azienda; la *vision* esprime una situazione tendenziale e rappresenta l'ideale al quale l'impresa mira. Missione, visione e valori fondamentali definiscono quindi ciò che un'azienda si impegna ad essere e come intende condurre gli affari, e comunicano a tutti gli *stakeholder* lo scopo dell'impresa. Per la maggior parte delle realtà, missione, visione e valori fondamentali rimangono stabili nel tempo e, attraverso l'impostazione della strategia, vengono tipicamente riaffermati. Tuttavia, essi possono anche evolvere al mutare delle condizioni di contesto e delle aspettative dei diversi *stakeholder*.

Il framework del COSO (Committee of Sponsoring Organizations of the Treadway Commission) pubblicato nel 2017, trattando del ruolo che la gestione del rischio assume nella scelta della strategia e del rapporto tra queste due dimensioni, specifica che la prima può aiutare un'impresa a comprendere meglio come *mission*, *vision* e *core values* costituiscano l'espressione iniziale di quali tipologie e livelli di rischio siano accettabili per realizzare una determinata strategia.

Questi aspetti devono sempre essere tenuti in considerazione, quando si analizza una strategia. La strategia deve supportare la missione e la visione dell'impresa. Una strategia disallineata aumenta la possibilità che l'organizzazione non riesca a realizzare la propria *mission* e *vision*, o possa compromettere i propri *core values*, anche se la strategia stessa viene attuata con successo.

Tutto ciò rappresenta l'alveo in cui confluisce e si alimenta la *risk culture*: le organizzazioni aziendali che riflettono nei propri comportamenti sia principi di integrità sia, più generale, valori etici e una gestione consapevole del rischio, sono quelle che hanno una cultura del rischio sana e forte, la cui

pervasività ed effettività può determinare il destino dell'impresa. Definire e promuovere un'efficace cultura del rischio rappresentano dunque responsabilità importanti del *top management* e del *board*. Le imprese dotate di una cultura del rischio efficace sono quelle in cui è diffusa a tutti i livelli la consapevolezza dei rischi associati alla strategia e all'ambiente in cui si opera, e in cui i rischi assunti sono sempre coerenti con la propensione al rischio deliberata dal vertice aziendale.

In letteratura sono disponibili varie definizioni di *risk culture*. Il rapporto dell'Institute International of Finance 2009 "Riforma nel settore dei servizi finanziari: rafforzare le pratiche per un sistema più stabile", ad esempio, definisce la cultura del rischio come "le norme di comportamento per individui e gruppi all'interno di un'organizzazione che determinano la capacità collettiva di identificare e comprendere, discutere apertamente e agire sul rischio attuale e futuro delle organizzazioni". Sembra tuttavia più in linea con il nostro approccio la definizione proposta da una ricerca condotta nel 2014 dalla Risk Management Association e Protiviti, secondo la quale la cultura del rischio è "l'insieme di comportamenti, discussioni, decisioni e atteggiamenti incoraggiati e accettabili nei confronti dell'assunzione e della gestione del rischio all'interno di un'istituzione". La *risk culture* è quindi il fattore che lega tutti gli elementi del sistema di gestione del rischio, poiché riflette i valori, gli obiettivi, le pratiche e i meccanismi condivisi che incorporano il rischio nei processi decisionali di un'organizzazione e la gestione del rischio nei suoi processi operativi.

Il Financial Stability Board, nel suo documento del 2014 "*Guidance on Supervisory Interaction with Financial Institutions on Risk Culture - A Framework for Assessing Risk Culture"*, ribadisce che una solida cultura del rischio dovrebbe sottolineare in tutta l'azienda l'importanza di garantire che:

I. un adeguato equilibrio rischio-rendimento coerente con la propensione al rischio dell'ente sia raggiunto quando si assumono rischi;

II. un sistema efficace di controlli commisurato alle dimensioni e alla complessità dell'entità sia messo in atto correttamente;

III. la qualità dei modelli di rischio, l'accuratezza dei dati, la capacità degli strumenti disponibili per misurare accuratamente i rischi e le motivazioni per l'assunzione di rischi possano essere messe in discussione;

IV. tutte le violazioni dei limiti, le deviazioni dalle politiche stabilite e gli incidenti operativi siano attentamente seguiti da azioni disciplinari proporzionate, quando necessario.

Il citato documento del Financial Stability Board riporta inoltre gli indicatori per valutare la solidità della cultura del rischio. Riconoscendo che la valutazione della cultura del rischio è complessa ma confermando che, data la sua importanza, è un aspetto a cui bisogna prestare attenzione, il FSB elenca diversi indicatori che possono essere rappresentativi di una solida cultura del rischio, specificando che essi dovrebbero essere considerati collettivamente, rafforzandosi a vicenda; esaminando ciascun indicatore isolatamente si potrebbe rischiare di ignorare la natura multiforme della cultura del rischio.

I macro-indicatori proposti dal FSB sono i seguenti quattro:

- **Tone from the top**: Il *Board* ed il *Senior Management* definiscono i valori chiave aziendali e le attese in termini di cultura del rischio e, per primi, sono chiamati a riflettere tali valori nei loro comportamenti. Valori chiave sono l'aspettativa che il personale operi con integrità e riferisca tempestivamente problematiche di non-*compliance* osservate all'interno ed all'esterno dell'organizzazione. Il governo dell'organizzazione promuove, monitora e valuta la cultura del rischio; considera l'impatto della cultura sulla sicurezza ed integrità; interviene dove necessario apportando cambiamenti.

- **Responsabilità** *(accountability):* Il personale rilevante a tutti i livelli dell'organizzazione comprende i valori chiave dell'azienda ed il suo approccio al rischio, è in grado di esercitare il ruolo assegnato ed è consapevole di essere responsabile (*accountable*) delle proprie azioni in relazione al comportamento da tenere in casi di *risk taking*. L'accettazione da parte dello staff degli obiettivi in termini di rischio e dei connessi valori è essenziale.

- **Comunicazione e challenge** efficaci*:* Una adeguata cultura del rischio promuove un ambiente di aperta comunicazione ed efficace confronto in cui i processi decisionali incoraggiano l'espressione delle diverse opinioni; permette la verifica delle prassi correnti; stimola una attitudine positiva e critica nel personale; promuove un ambiente di coinvolgimento positivo e costruttivo.
- **Incentivi***:* La gestione delle prestazioni e dei talenti incoraggia e rafforza il mantenimento del comportamento desiderato di *risk management* dell'istituzione. Incentivi finanziari e non supportano i valori chiave e la cultura del rischio a tutti i livelli dell'organizzazione.

Lo stesso documento del Financial Stability Board riporta anche alcune indicazioni più specifiche in merito alle modalità con cui allineare *risk culture* e strategia. In particolare, nell'ambito degli indicatori della categoria "*Tone from the Top*", si sottolinea l'importanza dei seguenti fattori:

- occorre prevedere processi e meccanismi adeguati a garantire che la propensione al rischio, la strategia di gestione del rischio e la strategia aziendale siano effettivamente allineate e integrate nei processi decisionali e nelle operazioni a tutti i livelli dell'ente;
- il consiglio di amministrazione e il *senior management* devono avere punti di vista chiari sulle linee di *business* che pongono le principali sfide nella gestione del rischio, come linee di *business* con risultati inattesi o inspiegabili o linee di *business* con rischi non finanziari che potrebbero non prestarsi a una quantificazione immediata e semplice;
- il consiglio di amministrazione e l'alta dirigenza devono monitorare sistematicamente il modo con cui la direzione affronta prontamente ed efficacemente le questioni sollevate dal consiglio di amministrazione, dalle autorità di vigilanza e da tutte le funzioni aziendali di controllo.

Il framework del COSO, tra le cinque componenti interrelate che definiscono un sistema di *Enterprise Risk Management* solido, efficace e coerente, individua come primo aspetto ed elemento portante la "Risk Governance & Culture". In particolare, la *governance*, intesa come approccio complessivo dell'organizzazione al rischio, definisce l'impostazione dell'organizzazione stessa e garantisce, attraverso la definizione di strutture, responsabilità e sistemi di supervisione, l'equilibrio di tutti gli interessi coinvolti nel sistema azienda e nei confronti dei portatori d'interesse (secondo un sistema di pesi – gestione – e contrappesi – controllo). D'altronde una piena percezione e valutazione della combinazione rischio/rendimento, e il suo corretto bilanciamento, garantiscono la consapevolezza dei rischi assunti e potenzialmente assumibili in base alla strategia delineata. La cultura del rischio, come finora intesa, rappresenta la base della sostenibilità degli obiettivi di impresa, oltre che del mantenimento di valori etici, integrità, trasparenza e *accountability*; la cultura del rischio va quindi interpretata come qualcosa di intrinseco all'impresa, che fa parte del suo DNA e rappresenta il principale strumento per tutelarlo.

La diffusione della cultura del rischio all'interno dell'impresa assume grande importanza per garantire la consapevolezza dei rischi assunti e generati dall'operatività da parte dei *risk owners* (responsabili di aree in cui sorgono, risiedono i rischi e sono messe in pratica le relative azioni di mitigazione), *risk managers* (responsabili di funzioni o attività di controllo *ex ante* ed *ex post* del rischio) e organi aziendali. I primi, se consapevoli dei rischi possono intraprendere eventuali azioni di mitigazione o supportare la gestione del rischio stesso. I *risk managers* sono per loro natura i principali detentori delle metodologie di misurazione e delle informazioni sui rischi che essi devono rappresentare al *top management* e agli organi aziendali secondo requisiti di tempestività, completezza e precisione.

La diffusione della *risk culture* è pertanto un motore fondamentale per l'assunzione consapevole dei rischi e per la loro gestione, nonché per il processo di definizione delle scelte strategiche. E tale assunto è anche alla base degli *standard* internazionali in tema di *risk management*.

La *risk culture* dell'impresa deve essere quindi valutata, monitorata, gestita e diffusa.

La misurazione e la valutazione della cultura del rischio possono essere svolte sulla base di metodologie qualitative e/o quantitative, a seconda degli indicatori prescelti e della disponibilità e comparabilità dei dati e delle informazioni. Un esempio articolato di sistema di indicatori, coerente con l'impostazione

dell'FSB, è presentato nel *paper* "La cultura del rischio", pubblicato nel 2016 dall'Associazione Italiana Internal Auditors.

Quanto agli strumenti di gestione e diffusione, si rileva innanzitutto l'importanza della condivisione e della tempestiva circolarizzazione delle informazioni in tema di rischi all'interno dell'organizzazione. Il sistema di reporting è un elemento necessario e strumentale alla diffusione della cultura del rischio dell'impresa a tutti i livelli aziendali: operativo di dettaglio per le aree di *business* e manageriale sinottico per il *top management* e gli organi aziendali. Esso rappresenta sia il presupposto per l'assunzione di decisioni consapevoli da parte del *board* e del *management*, sia uno strumento utile alla disclosure sui rischi. Un ulteriore strumento di diffusione della cultura del rischio è l'informativa sui rischi attraverso canali non necessariamente strutturati o codificati (mail, riunioni, *workshop*, etc.).

Sono auspicabili anche altri canali informativi di tipo "soft", *una tantum* o predefiniti, quali ad esempio *newsletter*, sessioni di *training*, *academies*, incontri periodici per la condivisione di aspetti specifici monotematici (i.e. su *modeling*, *governance*, classi di rischio specifiche) soprattutto tra soggetti interni all'impresa, prevedendo eventualmente anche la partecipazione attiva di soggetti esterni (accademici, specialisti e *professionals* di *peers*, etc.).

La diffusione della cultura del rischio, tuttavia, non deve per forza presentare caratteristiche di metodicità o aspetti di natura organizzativa; di fatto può configurarsi più come una filosofia gestionale, che consente di parlare di rischio in azienda esattamente come si parla di *business*. E di fronte a un qualsiasi *business* e ai rischi ad esso connessi, si presenta sempre una necessaria valutazione di opportunità, che può portare a considerare la rischiosità come una dimensione non esclusivamente negativa.

Un'impresa che presenta una cultura di rischio forte e ben radicata mette naturalmente a disposizione del personale strumenti, informazioni e dati, al fine di minimizzare il rischio o di assumerlo in maniera ottimale (ovvero in relazione al rendimento/perdite potenziali o ai costi di investimento per minimizzarlo). Di seguito vengono elencate alcune azioni di natura pragmatica per poter creare o rafforzare la cultura del rischio in ogni impresa:

- effettuare formazione che spieghi che cos'è il rischio di *business* e qual è la sua importanza (utilizzando, ad esempio, dei *case study* sul rischio reputazionale che presentino una mancata gestione del rischio o come d'altra parte una scarsa propensione al rischio possa portare anche al fallimento di un'impresa);
- creare la funzione di *Risk Management*, ponendola in una posizione apicale in azienda, attribuendo alla funzione una forte *sponsorship* da parte degli *stakeholder*;
- implementare un processo di gestione dei rischi diffuso con ruoli definiti per le unità interessate ai vari livelli di impresa (*legal entity*, Paese, commessa/progetto, linea di *business*);
- riconoscere e premiare un'efficace gestione del rischio, intesa anche come comportamento proattivo verso questa dimensione;
- riconoscere e stigmatizzare la cattiva gestione del rischio;
- sensibilizzare il *board* sui rischi di impresa, attraverso *induction* o strumenti similari,
- creare e diffondere un *Risk Appetite Statement* che indichi non solo la propensione ma anche la tolleranza al rischio, identificando gli strumenti di misurare e monitoraggio.

Un ultimo aspetto riguarda gli strumenti di cambiamento o di miglioramento della *risk culture* di un'impresa. Una volta completata una valutazione iniziale della cultura del rischio presente in azienda, infatti, il top *management* dovrebbe prendere in considerazione l'eventuale necessità di apportare modifiche organizzative e adottare misure per attuare tali modifiche secondo gli eventuali indirizzi del *board*. Per creare la cultura del rischio desiderata, la direzione dovrebbe cercare di:

- rendere conveniente l'incorporazione della cultura del rischio desiderata nei comportamenti organizzativi. Le responsabilità e i comportamenti desiderati per la gestione del rischio

dovrebbero essere rafforzati attraverso *policies*, sistemi di limiti, procedure di escalation, sistemi di incentivazione;

- rappresentare direttamente, mediante l'esempio, la cultura del rischio come una priorità: gli esecutivi dovrebbero supportare la cultura del rischio desiderata mostrando personalmente i comportamenti desiderati attraverso azioni e decisioni, nonché comunicando periodicamente il valore fornito dalla cultura del rischio all'organizzazione;
- adottare un approccio integrato: se isolate, comunicazioni periodiche, campagne di sensibilizzazione e strategie di formazione rischiano di restare "sulla carta". Se inserite in un programma completo che allinea aspettative, prestazioni, ruoli e strutture retributive con un'adeguata assunzione dei rischi, esse rafforzano gli aspetti critici della cultura del rischio desiderata;
- valutare periodicamente i progressi e monitorare il comportamento dei dipendenti per nuove tendenze, attitudini o percezioni che richiedono attenzione. A questo fine, possono essere usate misure quantitative e qualitative di una cultura del rischio efficace utilizzando indicatori come:
    - Livello di sponsorizzazione da parte del *management* esecutivo
    - Livello di padronanza nella gestione del rischio da parte delle *business lines*
    - Efficacia del comitato rischi e dei processi di *governance*
    - Qualità delle discussioni nel *board* su questioni di rischio
    - Utilizzo della dichiarazione di *risk appetite* e *risk tolerance* nel processo decisionale
    - Allineamento e integrazione del rischio nella pianificazione strategica
- prestare attenzione ai segni di cambiamento. I sondaggi tra i dipendenti e i *focus group* sono esempi di strumenti che possono fornire spunti ai fini della valutazione della cultura del rischio. Occorre altresì considerare gli effetti dei cambiamenti nella strategia e nell'organizzazione nonché il verificarsi di eventi esterni, compresi gli sviluppi normativi, per valutare se essi richiedano nuovi interventi volti a rafforzare o far evolvere la cultura del rischio.

In sintesi, la cultura del rischio rappresenta una fondamentale leva di gestione per qualunque impresa e un elemento determinante del sistema di ERM: occorre sempre ricordare che senza rischio non c'è rendimento e senza redditività non c'è impresa. La *risk culture* diventa dunque un fattore capace di orientare i comportamenti dell'organizzazione secondo una logica ben precisa, e finalizzata a far funzionare realmente il sistema di gestione dei rischi, a supporto delle strategie e quindi del conseguimento e di un valore sostenibile e duraturo nel tempo.

1.2 Il ruolo del Board e del Comitato Controllo Rischi

1.2.1 I riferimenti suggeriti dal codice di autodisciplina per le società quotate

Il processo di gestione dei rischi aziendali può essere analizzato da diversi punti di vista, tanto all'interno quanto all'esterno dell'impresa. Ciascun punto di vista si caratterizza per finalità, metodi e persino linguaggi differenti.

Dentro l'impresa, un punto di vista che assume particolare rilievo è quello del *board* e, in particolare, del comitato controllo interno e gestione dei rischi (CIeGR). Peraltro, pure in seno al *board* e al CIeGR vi possono essere punti di vista che sottendono obiettivi fisiologicamente diversi, ad esempio tra consiglieri esecutivi vs non esecutivi, indipendenti vs non indipendenti, espressione degli azionisti di minoranza vs di maggioranza.

Per orientare e indirizzare il comportamento del *board* e del CIeGR è consuetudine fare riferimento alle best practice esistenti. Nel contesto italiano, la principale best practice è identificabile nel codice di autodisciplina per le società quotate, redatto e via via aggiornato dal Comitato per la Corporate Governance costituito per iniziativa della Borsa Italiana. L'ultima versione è aggiornata a gennaio 2020 ed entrerà in vigore a far tempo dal 2021.

In tale ambito è possibile ravvisare anche alcune indicazioni che riguardano specificatamente la *governance* della gestione dei rischi. Più precisamente, l'ultima versione del codice di autodisciplina identifica gli organi che dovrebbero indirizzare e governare il processo di gestione dei rischi e attribuisce loro alcuni compiti.

Tali organi sono identificati nel CdA, nell'Amministratore incaricato del sistema di CIeGR (che coincide con il CEO) e, infine, nel Comitato CIeGR. In generale, questi dovrebbero: a) definire il livello di rischio compatibile con gli obiettivi strategici; b) individuare le linee di indirizzo del sistema di CIeGR; c) verificare che i rischi siano identificati, misurati, gestiti e monitorati; d) descrivere il sistema di CIeGR ed esprimere una valutazione circa la sua adeguatezza.

Più in particolare:

a) il CdA, con il supporto del Comitato CIeGR, dovrebbe:

- definire la natura e il livello di rischio compatibile con gli obiettivi strategici dell'emittente, nell'ottica del successo sostenibile della società;
- definire le linee di indirizzo del sistema di CIeGR in coerenza con le strategie della società e valutare, con cadenza almeno annuale, l'adeguatezza del medesimo sistema rispetto alle caratteristiche dell'impresa e al profilo di rischio assunto;
- descrivere, nella relazione sul governo societario, le principali caratteristiche del sistema di CIeGR e le modalità di coordinamento tra i soggetti in esso coinvolti, indicando i modelli e le best practice nazionali e internazionali di riferimento;
- esprimere la propria valutazione complessiva sull' adeguatezza del sistema stesso.

b) Il CEO, nella sua funzione di Amministratore incaricato del sistema di CIeGR, dovrebbe:

- curare l'identificazione dei principali rischi aziendali e sottoporli periodicamente all'attenzione del *board*;
- dare esecuzione alle linee di indirizzo definite dall'organo di amministrazione, curando la progettazione, realizzazione e gestione del sistema di CIeGR e verificandone l'adeguatezza e l'efficacia;

- riferire tempestivamente al Comitato CIeGR in merito a eventuali problematiche e criticità emerse nello svolgimento della propria attività.

c) Il Comitato CIeGR dovrebbe:

- possedere nel suo complesso un'adeguata competenza nel settore di attività in cui opera la società e prevedere che almeno un suo componente possieda un'adeguata competenza in materia contabile e finanziaria o di gestione dei rischi;
- esprimere pareri su specifici aspetti inerenti alla identificazione dei principali rischi e supportare le valutazioni del *board* relative alla gestione dei rischi derivanti da fatti pregiudizievoli;
- riferire al CdA, almeno in occasione dell'approvazione della relazione finanziaria annuale e semestrale, sull'attività svolta e sull'adeguatezza del sistema di CIeGR;

Il codice di autodisciplina, dunque, identifica gli organi competenti e attribuisce loro talune responsabilità. Al tempo stesso, il codice lascia aperti diversi interrogativi. Non è, ad esempio, esplicitato il metodo mediante il quale gli organi preposti dovrebbero operare, così come non è chiaro su quali basi il sistema di CIeGR dovrebbe essere ritenuto "adeguato".

Gli stessi estensori del codice di autodisciplina sembrano consapevoli di tali limiti, laddove invitano il lettore a trarre spunto dalle best practice esistenti in ambito nazionale e internazionale. Per tale motivo, di seguito viene proposta una breve sintesi di alcune possibili best practice che possono integrare e completare le indicazioni fornite dal codice. Si tratta, in particolare, dell'ultima versione del COSO Report (2017), dei princìpi internazionali stabiliti dal G20/OCSE e, infine, dall'esperienza che può essere tratta dai *board* delle banche.

1.2.2 Alcuni riferimenti e riflessioni ritraibili dal COSO Report 2017

Il titolo del COSO Report 2017 è "Enterprise Risk Management (ERM) integrating with strategy and performance". Tale titolo è di per sé indicativo del messaggio che il documento intende veicolare e promuovere, ovvero una progressiva integrazione tra ERM, strategia e *performance*.

Come riportato nel paragrafo 1.1, il documento è articolato in cinque punti in cui sono enunciati venti princìpi. Il primo dei cinque punti, denominato "governance & culture" e articolato in cinque princìpi, è quello che riguarda più direttamente il *board*[1]. Per tale motivo merita un breve approfondimento.

In generale, tale punto sottolinea che il ruolo del *board* consiste nell'indirizzare e controllare il processo di gestione dei rischi implementato dal *management*. In tale ambito il *board* dovrebbe identificare una struttura operativa adeguata che, mediante *management* competente, implementa decisioni coerenti con la mission, i *core values*, il *risk appetite*, gli obiettivi strategici e la creazione di valore.

A tal fine, come anticipato, vengono identificati i seguenti cinque princìpi che rimarcano l'importanza della conoscenza e della diffusione della cultura del rischio:

1. **Exercises Board Risk Oversight.** Il *board* è chiamato a ricoprire, nel rispetto del requisito di indipendenza, un ruolo di supervisione dell'attività del *management*, per supportarlo nel raggiungere gli obiettivi strategici coerentemente con l'obiettivo della generazione di valore nel medio e lungo termine;
2. **Establishes Operating Structures**. Il *board* deve verificare che sia chiaramente definita la struttura operativa, ovvero lo strumento attraverso cui l'organizzazione può realizzare i suoi obiettivi. Devono pertanto essere ben definite le attività, le responsabilità, le risorse, i sistemi e le procedure per raggiungere gli obiettivi;

[1] Gli altri quattro punti, che ricomprendono i residui quindici princìpi, sono così intitolati: strategy & objective setting; performance; review & revision; e, infine, information, communication & reporting.

3. **Defines Desired Culture**. Il *board* deve promuovere la definizione e la diffusione della cultura dell'*enterprise risk management*, che può essere più o meno avversa al rischio. Tale cultura influenza le tecniche di identificazione del rischio, nonché i tipi di rischio che sono sopportati o trasferiti a terzi e, infine, le modalità di gestione dei rischi stessi;
4. **Demonstrates commitment to core values**. Il *board* deve verificare la presenza di un adeguato commitment rispetto ai valori e alla mission condivisi dal *management* e dai dipendenti;
5. **Attracts, Develops, and Retains Capable Individual**. Il *board* è chiamato a verificare la presenza delle competenze necessarie a implementare la strategia e a raggiungere gli obiettivi, in modo che il capitale umano diventi e rimanga un vantaggio competitivo.

Nella prospettiva del *board*, l'aspetto più rivoluzionario del COSOReport 2017 riguarda l'integrazione tra *risk appetite*, strategia, *governance* e *performance*.

In tale ambito, l'identificazione del *risk appetite* riveste un ruolo centrale in quanto è il punto di partenza da cui derivano conseguenze significative per selezionare le strategie così come per indirizzare la *governance* e la misurazione della *performance* aziendale.

Nel framework del COSOReport 2017, infatti, il *risk appetite* nasce prima delle strategie e, in particolare, è il setaccio con cui le strategie debbono essere selezionate.

Al tempo stesso, l'identificazione preliminare del *risk appetite* indirizza la *governance* perché induce a verificare come il rischio viene ripartito tra gli *stakeholder* che in varia misura lo sopportano (clienti, fornitori, dipendenti, investitori, ecc.).

Infine, identificare preliminarmente il *risk appetite* impatta la misurazione della *performance* perché obbliga a verificare *ex ante* l'attitudine dell'azienda a remunerare adeguatamente il rischio sopportato da ciascuno *stakeholder*. Remunerare adeguatamente gli *stakeholder* è il presupposto per preservare/creare valore economico sostenibile nel tempo, nel rispetto dei valori ambientali/sociali adottati spontaneamente dall'azienda e/o imposti dagli stessi *stakeholder*.

In ultima analisi, il COSOReport 2017 costituisce un utile complemento del codice di autodisciplina in quanto induce il *board* e il comitato CIeGR a farsi promotori di un progressivo miglioramento culturale e, in particolare, a verificare:

a) se le indicazioni necessariamente generali del codice di autodisciplina sono tradotte in decisioni concrete che siano ispirate al COSOReport 2017 ma anche adeguate rispetto alla *governance* e alle caratteristiche dimensionali e settoriali dell'azienda;
b) se e come l'azienda ha identificato il suo *risk appetite* e come esso viene declinato ai vari livelli dell'organizzazione, ovvero come viene utilizzato nella selezione delle decisioni strategiche e operative;
c) come il rischio è ripartito tra gli *stakeholder* e se esso è remunerato adeguatamente. In effetti, questa verifica non può che essere effettuata dal *board* e deve essere ispirata al requisito della indipendenza;
d) se la mappatura dei rischi è organizzata in modo da assegnare una priorità alle varie tipologie di rischi in relazione alla loro attitudine a influire sul *risk appetite* e sulla realizzabilità degli obiettivi strategici, economici, reputazionali e di sostenibilità;
e) se la cultura del rischio è coerente con la *mission*, i valori e l'obiettivo della creazione di valore sostenibile nel tempo;
f) se l'azienda promuove o meno un progressivo *upgrading* della cultura aziendale e delle figure professionali che possono supportare il CEO nell'allineamento alla *best practice*. Nell'ambito del COSO Report 2017 è ormai infatti evidente che le tradizionali competenze di *internal auditing* e

di *risk management* meritano di essere integrate con la conoscenza del *business*, della *governance*, della strategia e della finanza;

g) se e come la cultura del rischio viene recepita negli schemi di remunerazione del *management*.

1.2.3 I principi internazionali stabiliti dal G20/OCSE

Il consiglio di amministrazione è l'organo centrale del sistema di *corporate governance* ed è stato investito nel tempo di funzioni e doveri crescenti in materia di governo e controllo dei rischi.

Tale organo è il primo, e ultimo, responsabile del disegno e del corretto funzionamento del sistema di controllo interno e gestione dei rischi. Per altro verso, proprio questo sistema rappresenta il principale strumento a disposizione del *board* per l'efficace svolgimento della funzione di supervisione strategica e per la qualificazione e il monitoraggio della corretta esecuzione delle strategie, nell'interesse di lungo periodo dell'impresa e di tutti i suoi *stakeholder*.

I principi internazionali, stabiliti dall'OCSE in accordo con il G20 (OECD, 2015[2]), stabiliscono che il sistema di *corporate governance* deve assicurare la conduzione strategica dell'impresa, l'efficace controllo da parte del *board* sull'andamento della gestione e *l'accountability* del consiglio nei confronti della società e dei relativi azionisti. A tal fine, gli amministratori, agendo in buona fede e in modo diligente e informato, prendono decisioni che rispettano principi etici e tengono in debita considerazione gli interessi degli *stakeholder* rilevanti per l'impresa.

Le condizioni necessarie affinché l'organo sia in grado di svolgere tale ruolo in modo efficace riguardano innanzitutto i relativi profili di composizione, organizzazione e funzionamento. In particolare, i principi G20/OCSE ritengono fondamentale che gli amministratori siano in grado di esprimere valutazioni e deliberazioni in modo indipendente e obiettivo rispetto alle proposte e alle azioni del *management*, prevenendo conflitti di interesse che possano andare a detrimento dell'impresa nel suo complesso. Ciò presuppone, in termini di composizione del *board*, che:

- vi sia un numero sufficiente di amministratori esterni al nucleo degli azionisti di controllo e del *management* (c.d. "*outsider*"), meglio se indipendenti, ossia privi di relazioni personali o professionali con la società e i relativi azionisti ed esponenti, che potrebbero comprometterne l'obiettività di giudizio;
- i ruoli di presidente e amministratore delegato siano separati;
- il presidente sia assistito da un segretario del consiglio.

In particolare, la condizione di indipendenza, che non può ovviamente prescindere da una adeguata professionalità, contribuisce alla qualità delle decisioni prese dal *board*. Gli indipendenti portano un punto di vista autonomo e terzo nella valutazione delle *performance* del consiglio e del *management*. Essi sono, inoltre, nelle condizioni di svolgere un ruolo fondamentale nelle questioni in cui interessi del *management*, dell'impresa e dei suoi azionisti possono divergere, come le remunerazioni degli esecutivi, i piani di successione, le operazioni straordinarie e i controlli interni. La determinazione dei requisiti che qualificano l'indipendenza è stabilita, per alcune società (quotate, banche e intermediari finanziari), da codici o normative, mentre per altre può essere inclusa negli statuti. Spetta comunque al consiglio valutarne il possesso da parte dei singoli amministratori, al momento dell'assunzione dell'incarico e poi su base periodica.

In termini di organizzazione, i princìpi suggeriscono la costituzione di comitati endoconsiliari, con funzioni propositive, consultive e istruttorie, per la trattazione di temi potenzialmente oggetto di conflitti di interesse fra *stakeholder* (remunerazioni, nomine, controllo, *risk management*, sostenibilità).

In tale ambito, il comitato, o i comitati, incaricati del presidio di controlli e rischi, supportano il consiglio nell'istruttoria relativa a questi temi, tramite una interlocuzione diretta e approfondita con il *management* e le funzioni aziendali di controllo.

---

[2] OECD (2015), G20/OECD Principles of Corporate Governance, OECD Publishing, Paris. http://dx.doi.org/10.1787/9789264236882-en

Quanto al funzionamento dell'organo, i princìpi G20/OCSE sottolineano l'importanza di favorire l'accesso del *board* a una informativa accurata, rilevante e tempestiva sull'andamento della gestione e sui temi oggetto di trattazione e delibera nelle sedute. Non è solo importante che il consiglio disponga di una adeguata quantità di informazioni, ma anche che questa sia trasparente, completa e rilevante, ossia presentata in modo tale da consentire una preparazione efficace e una chiara individuazione degli aspetti critici, meritevoli di discussione. Così, ad esempio, in tema di rischi, è fondamentale che il consiglio sia messo a conoscenza delle ipotesi di scenario sottostanti ai modelli di valutazione, della qualità dei dati utilizzati per la loro costruzione, del significato strategico e gestionale delle misure e dei relativi valori. Il *board* deve assicurarsi che siano identificati tutti i rischi connessi con il *business* e che le strategie di mitigazione siano tali da consentire alla società di perseguire i propri obiettivi, mantenendo il profilo di rischio a un livello coerente con la propensione al rischio (*risk appetite*) desiderata.

La valutazione dei rischi, così come altri temi di competenza del consiglio, può richiedere competenze specifiche, che devono essere garantite in seno al *board* anche con opportuni interventi di induction e di formazione continua.

In ultima analisi, i principi internazionali stabiliti dal G20/OCSE propongono indicazioni allineate a quelle del codice di autodisciplina, con particolare riferimento al prerequisito della indipendenza dei consiglieri e all'opportunità di costituire appositi comitati endoconsiliari, quali ad esempio il CIeGR. Un aspetto enfatizzato dai princìpi internazionali, che meriterebbe di essere valutato con attenzione nelle imprese non finanziarie, riguarda la qualità delle informazioni, con particolare riguardo agli scenari sottostanti i modelli di identificazione e valutazione dei rischi connessi al *business*.

1.2.4 L'esperienza dei board bancari: lessons to learn

I principi sopra esposti hanno ispirato e trovano ora una dettagliata rappresentazione nella normativa bancaria in tema di governo societario (Direttiva CRD IV, Linee Guida dell'Autorità Bancaria Europea, Circolare Banca d'Italia 285/13, Titolo IV, Capitoli 1 e 3). Fatte salve le particolari finalità di tali norme, che riflettono l'interesse pubblico nei confronti dell'attività delle banche e l'importanza di assicurare la sana e prudente gestione delle stesse a tutela della stabilità dell'intero sistema economico-finanziario, il grado di dettaglio della disciplina bancaria contribuisce a chiarire e fornire spunti ulteriori sulle modalità di declinazione e di interpretazione dei principi più generali nelle singole realtà aziendali.

La revisione normativa introdotta dopo la crisi finanziaria, inoltre, ha accentuato l'attenzione sul governo dei rischi alla luce delle carenze rilevate e considerate fra le cause della crisi stessa, e fornisce quindi importanti indicazioni ai fini di un corretto presidio dei processi di *risk management*, sia in chiave strategica e gestionale, sia nell'ottica della prevenzione di situazioni di dissesto. L'azione, sempre più pervasiva e costante nel tempo, dei supervisori (Banca Centrale Europea per le banche rilevanti e Banca d'Italia per le altre) contribuisce a rappresentare in modo concreto le attese nei confronti degli organi aziendali in merito alle modalità con cui gli stessi dovrebbero applicare la normativa di riferimento.

Quali indicazioni dunque dovrebbero utilmente trarre le imprese non finanziarie dall'esperienza bancaria?

In primo luogo, alcune regole generali e imprescindibili per una buona *governance* dei rischi. Esse riguardano: la chiara distinzione dei ruoli e delle responsabilità (ispirata al principio del "*check and balance*"), inclusa la determinazione analitica, precisa e chiara delle deleghe, anche nell'indicazione dei limiti quantitativi o di valore e delle eventuali modalità di esercizio; l'appropriato bilanciamento dei poteri; l'equilibrata e diversificata composizione degli organi, inclusa la presenza di un numero adeguato di amministratori indipendenti; l'efficacia dei controlli; il presidio di tutti i rischi aziendali; l'adeguatezza dei flussi informativi.

In particolare, è stabilito nella normativa che gli organi aziendali devono assicurare il governo di tutti i rischi a cui la banca si espone, individuandone per tempo le fonti, le possibili dinamiche, i necessari presidi. Ciò significa che gli amministratori devono:

- avere una competenza tale da comprendere i modelli di misurazione e gestione dei rischi, i relativi profili regolamentari e applicativi;

- avere piena consapevolezza del sistema di *governance* e dell'organizzazione della società e del gruppo di riferimento (c.d. principio del "know your structure"), al fine di saper individuare le fonti specifiche di rischio nei singoli processi e nelle diverse attività svolte;
- impegnarsi attivamente nella preparazione e nello svolgimento delle attività consiliari, favorendo un confronto costruttivo ("*challenge*") con il *management*, tramite un dibattito vivace che consente la messa a fattor comune delle esperienze, anche maturate dai singoli al di fuori del contesto specifico, ai fini della presa di buone decisioni.

Al fine di garantire l'efficace svolgimento dei lavori del *board*, il Presidente, che nelle banche ha il divieto di assumere funzioni esecutive, deve garantire l'equilibrio di poteri rispetto all'amministratore delegato e agli altri amministratori esecutivi. Il Presidente promuove l'effettivo funzionamento del sistema di governo societario anche determinando l'agenda delle riunioni in modo tale da garantire che vi sia tempo sufficiente per la trattazione dei temi strategici.

Egli favorisce, in modo neutrale, la cultura del dibattito durante le sedute, stimolando la dialettica tra componenti esecutivi e non esecutivi e sollecitando la partecipazione attiva dei componenti non esecutivi; inoltre, promuove occasioni di scambio e confronto fra gli amministratori anche al di fuori delle stesse, ad esempio organizzando incontri *off-site*, per approfondire e confrontarsi sulle questioni strategiche, riunioni monotematiche su argomenti rilevanti, sessioni di *induction*, formative e informative, che consentano l'allineamento progressivo e il necessario aggiornamento delle competenze. Il Presidente inoltre coordina un processo di autovalutazione annuale del *board* e degli eventuali comitati consiliari, dal quale trae stimoli per il continuo miglioramento dell'efficacia del sistema di *governance*.

Non vi è dubbio che nella regolamentazione bancaria l'attenzione sia posta soprattutto sulla funzione di supervisione e controllo in capo al consiglio di amministrazione, volta a garantire il regolare svolgimento della gestione e a prevenire assunzione di rischio eccessivo rispetto alle capacità di governo dell'azienda. A tal fine, è considerato fondamentale che le funzioni aziendali di controllo (*internal auditing*, *risk management*, *compliance*, antiriciclaggio, dirigente preposto, etc.) abbiano una relazione diretta con gli organi e non mediata dall'amministratore delegato o dall'eventuale comitato esecutivo.

L'attività di nomina e revoca dei responsabili delle funzioni di internal auditing, di *compliance* e di *risk management* rientra tra le funzioni non delegabili dal consiglio. Inoltre, il *board* deve approvare i piani di attività pluriennali e annuale, monitorarne la regolare implementazione e ottenere una reportistica tempestiva in merito agli esiti delle verifiche svolte e alle rispettive azioni di rimedio. Il consiglio deve inoltre esprimere, su base semestrale o annuale, una propria valutazione in merito alla completezza, l'adeguatezza, la funzionalità e l'affidabilità del sistema dei controlli interni e di gestione dei rischi.

In tema di rischi, il consiglio di amministrazione ha la responsabilità di definire e approvare il quadro di riferimento per la determinazione della propensione al rischio (*Risk Appetite Framework* - "RAF") che caratterizza i piani strategici, le politiche di governo dei rischi, i processi di gestione dei rischi. Questi devono coprire tutti i rischi legati al *business* bancario, dai rischi di credito, di mercato, operativo, ai rischi di liquidità, di tasso di interesse, e rischi meno facilmente misurabili come quello reputazionale, strategico, legato ai processi IT (incluso il rischio *cyber*), di *compliance*, di condotta, e altri già in parte individuati nei testi normativi. Inoltre, ciascuna nuova linea strategica, incluso il lancio di nuovi prodotti, l'ingresso in nuovi mercati, cambiamenti organizzativi e operazioni straordinarie, deve essere valutata rispetto ai profili di rischio, anche nuovi, che la caratterizzano, alla capacità dei controlli interni di presidiare tali rischi, e alla relativa compatibilità con la propensione al rischio deliberata dal consiglio.

La circolazione di informazioni tra gli organi sociali e all'interno degli stessi rappresenta una condizione imprescindibile affinché siano effettivamente realizzati gli obiettivi di efficienza della gestione dei rischi ed efficacia dei controlli. Le banche devono porre specifica cura nello strutturare forme di comunicazione e di scambio di informazioni complete, tempestive e accurate tra gli organi, in relazione alle competenze di ciascuno di essi, nonché all'interno di ciascun organo; presidi organizzativi sono approntati per evitare il rischio di divulgazione impropria di notizie riservate. La predisposizione di flussi informativi adeguati e in tempi coerenti con la rilevanza e la complessità delle decisioni da assumere è necessaria anche per la piena valorizzazione dei diversi livelli di responsabilità all'interno dell'organizzazione aziendale. Tali esigenze sono coerenti con le previsioni civilistiche in tema di: competenza esclusiva degli amministratori per la gestione aziendale; dovere di "agire in modo informato"; informativa periodica al

consiglio da parte degli organi delegati; diritto degli amministratori di avere dagli organi delegati informazioni sulla gestione della società.

Il principio di tracciabilità dei processi decisionali, che permea la normativa bancaria, richiede che flussi informativi, procedure, metodi di lavoro, tempistiche delle riunioni siano adeguatamente formalizzati in regolamenti e procedure e che l'operato del consiglio, incluso il dibattito che porta alle delibere finali, sia chiaramente ricostruibile dai verbali delle sedute.

Assumono quindi particolare rilievo l'individuazione e la formalizzazione di prassi operative (procedure di convocazione, periodicità delle riunioni, partecipazione) che assicurino effettività e tempestività all'azione degli organi e dei loro comitati.

Nelle banche di maggiori dimensioni o complessità operativa, è necessario che siano costituiti tre comitati endoconsiliari, specializzati in tema di "nomine", "rischi" e "remunerazioni". Ciascun comitato è composto, di regola, da 3-5 membri, tutti non esecutivi e in maggioranza indipendenti; ove sia presente un consigliere eletto dalle minoranze, esso fa parte di almeno un comitato. I comitati devono distinguersi tra loro per almeno un componente. I lavori di ciascun comitato sono coordinati da un presidente scelto tra i componenti indipendenti.

In particolare, il comitato rischi, competente in tema di rischi e controlli, deve prestare particolare attenzione a tutte quelle attività strumentali e necessarie affinché il *board* possa determinare in modo corretto il RAF, le politiche di governo dei rischi e l'assetto adeguato del sistema organizzativo e di controllo interno. A tale scopo, ad esempio, il comitato, al fine di formulare proposte o pareri e rendicontare al *board*:

- condivide e propone in approvazione al *board* i piani di attività delle funzioni aziendali di controllo e ne monitora lo stato di avanzamento;
- esamina la reportistica predisposta dalle funzioni aziendali di controllo;
- analizza e monitora le criticità rilevate a seguito degli interventi effettuati e valuta l'adeguatezza, l'efficacia e il funzionamento delle azioni di rimedio;
- esamina la proposta di RAF connessa con il piano strategico e i piani annuali e monitora, almeno su base trimestrale, il profilo di rischio rispetto agli obiettivi di *risk appetite*;
- esamina il processo di determinazione dell'adeguatezza del capitale rispetto ai rischi assunti, e della situazione di liquidità;
- analizza e valuta i modelli di misurazione dei singoli rischi e la qualità delle informazioni e dei dati sottostanti, nonché i risultati delle attività di validazione interna e di revisione;
- analizza in dettaglio e valuta le politiche di svalutazione dei crediti e delle altre voci rilevanti ai fini di impairment;
- sulla base delle informazioni acquisite anche direttamente dai revisori contabili, acquisisce e analizza la valutazione del Dirigente Preposto alla redazione dei documenti contabili societari sul corretto utilizzo dei principi contabili e sulla loro applicazione nella predisposizione del progetto di bilancio e nell'informativa periodica;
- analizza le politiche e i processi di valutazione delle attività aziendali, inclusa la verifica che i prezzi e le condizioni delle operazioni con la clientela siano coerenti con il modello di *business* e le strategie in materia di rischi;
- valuta le prestazioni annuali delle funzioni aziendali di controllo e dei relativi responsabili;
- accerta che gli incentivi sottesi al sistema di remunerazione e incentivazione della banca siano coerenti con il RAF.

Dato l'elevato tecnicismo che caratterizza la misurazione e la gestione dei rischi in ambito bancario, la presenza del comitato è di fondamentale importanza affinché i singoli temi siano indirizzati e approfonditi in modo adeguato e gli amministratori possano interloquire con i manager competenti per

ottenere i chiarimenti necessari, imparare a comprendere le specificità dei singoli modelli, interpretare i risultati delle misurazioni al fine di coglierne la rilevanza e le ricadute strategiche e gestionali. Al contempo, il comitato deve stimolare le funzioni aziendali di controllo a valutare tutti i rischi, anche emergenti, connessi con i piani strategici e gli orientamenti di lungo periodo deliberati dal *board*, cercando in tal modo di rendere il *risk management* e i controlli più funzionali alla qualificazione delle decisioni strategiche e al presidio dell'equilibrato sviluppo del *business*.

Se il comitato opera in modo efficace, le valutazioni condotte dallo stesso saranno riportate al consiglio in una forma sintetica e utile ai fini del processo decisionale e la cultura dei rischi sviluppata dai membri del comitato contribuirà ad affinare le competenze e la sensibilità degli altri consiglieri. Ciò è fondamentale affinché l'attività di *risk management* e controllo interno, largamente fondata su criteri regolamentari, non sia percepita come puramente formale o tecnica, e quindi in prevalenza orientata a rispondere alle attese della vigilanza e a evitare sanzioni, ma sia valorizzata a fini strategici e di sana e prudente gestione aziendale.

Le norme bancarie si applicano in base a un principio di proporzionalità, relativo alle dimensioni, alla complessità operativa e al *risk appetite* delle singole imprese, in modo da assicurare la coerenza del sistema di gestione dei rischi e di controllo interno con le specificità del *business*, l'articolazione organizzativa e le strategie aziendali. Spetta però in prevalenza alle singole banche il compito di valutare il proprio fabbisogno in tema di presidio dei rischi e di "convincere" i supervisori dell'adeguatezza delle proprie scelte. Per questa ragione, è fondamentale che il *board* sia consapevole del complessivo profilo di rischio connesso con le proprie decisioni strategiche e con il modello di *business* adottato, delle relative capacità di governo e della coerenza della cultura dei rischi presente in azienda.

Le caratteristiche peculiari dell'attività bancaria, la funzione sociale delle banche, le possibili ricadute di un dissesto per l'economia, la complessità legata alla gestione dei rischi rendono il compito dell'amministratore di una banca diverso, e per certi versi più delicato e "visibile", di quello di un amministratore di una società non finanziaria. Il confronto diretto fra singoli amministratori ed esponenti del supervisore mette spesso "alla prova" i primi, in un dialogo che rappresenta un momento di verifica della relativa comprensione della realtà in cui opera. D'altra parte, i membri del *board* (e dell'organo di controllo) di una banca sono soggetti a requisiti di professionalità, onorabilità, indipendenza e time commitment, più stringenti di quelli delle altre imprese e devono superare il c.d. "fit and proper test", sul quale il giudizio finale spetta all'Autorità di Vigilanza.

Di conseguenza, l'accountability dell'amministratore bancario è massima. E lo sono, di conseguenza, anche le sue responsabilità. Tutto ciò rende molto difficile e rischioso per i singoli assumere il ruolo senza una adeguata consapevolezza delle attese nei propri confronti e dell'impatto che un atteggiamento passivo o un limitato impegno possono produrre sulla reputazione individuale.

Per trarre profitto dall'esperienza della *governance* dei rischi nelle banche è utile rimarcare i principi concretamente applicati dalle banche che sono già stati recepiti dalle corporate più evolute:

- il Presidente assolve un ruolo di promotore nella trattazione in seno al *board* di temi strategici e di temi legati alla misurazione e gestione dei rischi, in collaborazione con l'amministratore incaricato del sistema di CIeGR ovvero con il CEO;
- l'istituzione di una funzione di *risk management*. L'attribuzione di responsabilità di *risk management* deve essere chiaramente identificata e distinta da quella del I e del III livello di controllo, al fine di assicurare segregation of duties nelle diverse responsabilità e la necessaria dialettica con l'amministratore incaricato del sistema di CIeGR nell'ambito del Comitato;
- assicurare la promozione da parte del *board* di un quadro di riferimento per la determinazione della propensione al rischio (*Risk Appetite Framework* o RAF) con riguardo a tutti i rischi legati al *business* che hanno rilievo strategico. Conseguentemente, il *board* delle imprese non finanziarie dovrebbe valutare i profili di rischio connessi a nuove linee strategiche, al lancio di nuovi prodotti e alle operazioni di natura straordinaria, come ad esempio le acquisizioni e le fusioni, ecc.;

- possibilità di un confronto con standard setters e autorità istituzionali sulle migliori pratiche da adottare in tema di *governance* e gestione dei rischi al fine di garantirne l'efficacia e la consistenza con i diversi modelli di *governance*, operativi, di *business* e organizzativi delle corporate, al fine di acquisire anche uno stimolo esogeno che caratterizza per definizione le banche attraverso una rigorosa e puntuale regolamentazione di riferimento;
- il "fit and proper test" per i membri del Comitato CIeGR è assicurato grazie a un'attenta analisi delle competenze anche specialistiche.

Nelle imprese non finanziarie in cui il processo di *risk management* è tipicamente in uno stadio meno avanzato, l'organo che in prima battuta dovrebbe sopperire alle funzioni che nelle banche sono svolte dal presidente e dal supervisore esterno è identificabile nel Comitato CIeGR. È pertanto su tale organo che finiscono per accentrarsi le maggiori responsabilità. Proprio per questo motivo, nelle imprese non finanziarie assume particolare rilievo la composizione di tale organo, che dovrebbe rispondere a requisiti molto rigorosi al fine di avviare e perseguire un percorso virtuoso nella *governance* e nella gestione dei rischi aziendali.

Il punto di partenza per avviare e indirizzare il suddetto percorso virtuoso nelle imprese non finanziarie è pertanto identificabile nella composizione del Comitato CIeGR. In effetti, non è casuale che la raccomandazione 35 dell'ultima versione del Codice di autodisciplina preveda, seppure in linea generale, che almeno un componente del comitato debba possedere conoscenza ed esperienza in materia contabile e finanziaria o di gestione dei rischi.

Una volta acquisite la competenza e la sensibilità necessarie, le priorità del comitato CIeGR dovrebbero risiedere nello svolgere le funzioni che nelle banche sono riservate al presidente del *board* e all'organo di vigilanza, laddove possibile anche supportando e promuovendo una leadership del presidente su tali aspetti. Tali funzioni dovrebbero consistere soprattutto:

- nel portare all'attenzione del *board* la tematica del rischio, con particolare riguardo alla discussione e alla identificazione del *risk appetite*;
- nell'analizzare che le decisioni assunte dal *board* seguano un approccio di *risk management* e contemplino il monitoraggio dei rischi;
- nell'assicurare che in seno all'azienda esistano le competenze idonee a misurare, gestire e comunicare l'impatto esercitato dai rischi aziendali sulla *performance* e sul valore dell'azienda;
- nell'allineamento del processo di governo e gestione dei rischi alle migliori best practice, pur tenendo in debito conto del principio della proporzionalità e delle specificità proprie di ogni contesto aziendale;
- nello svolgere in seno al *board* e nei riguardi del *management* una funzione di challenge, ovvero di continua discussione critica di tutti i punti precedenti.

È evidente che difficilmente tutte le suddette funzioni possono essere svolte in autonomia da parte del comitato CIeGR. In effetti, a tale comitato dovrebbe essere richiesto di assumere un ruolo di stimolo, indirizzo e coordinamento, con particolare riferimento all'integrazione tra le *best practice* acquisibili all'esterno prevedendo eventualmente di colmare gap esistenti con il supporto di consulenti specializzati e/o all'assunzione di specifiche figure professionali e l'imprescindibile bagaglio interno di competenze/conoscenze che caratterizza ogni contesto aziendale.

1.3 Il ruolo di eventuali Risk Committee manageriali

Nell'ambito dei presidi collegiali di *Risk management* è possibile distinguere i Comitati endoconsiliari, istituiti con modalità di funzionamento definite dall'Organo di Amministrazione[3], dai Comitati manageriali, istituiti da disposizioni di *corporate governance* o organizzative.

Con riferimento ai Comitati endoconsiliari, il Consiglio di Amministrazione, svolgendo un ruolo di indirizzo e di valutazione dell'adeguatezza del sistema, individua al suo interno:

I. uno o più amministratori, incaricati dell'istituzione e del mantenimento di un efficace sistema di controllo interno e di gestione dei rischi;

II. un comitato controllo e rischi, con il compito di supportare, con un'adeguata attività istruttoria, le valutazioni e le decisioni del Consiglio di Amministrazione relative al sistema di controllo interno e di gestione dei rischi, nonché quelle relative all'approvazione delle relazioni finanziarie periodiche.

Menzionando quanto riportato nel Codice di Corporate Governance, "l'organo di amministrazione definisce i compiti del comitato e ne determina la composizione, privilegiando la competenza e l'esperienza dei relativi componenti ed evitando, nelle società grandi, una eccessiva concentrazione di incarichi in tale ambito. Ciascun comitato è coordinato da un presidente che informa l'organo di amministrazione delle attività svolte alla prima riunione utile. Il presidente del comitato può invitare a singole riunioni il presidente dell'organo di amministrazione, il *Chief Executive Officer*, gli altri amministratori e, informandone il *Chief Executive Officer*, gli esponenti delle funzioni aziendali competenti per materia".

In sostanza il comitato controllo e rischi assiste e supporta il Cda nelle sue valutazioni e decisioni in tema di controllo e gestione dei rischi.

Tale orientamento è definito anche da precedenti Standard setters (International Organization for Standardization - ISO con gli ISO 31000 e 31004, rispettivamente del 2009 e del 2010, e il Financial Stability Board, nel documento "Thematic Review on Risk Governance" del 2013), che promuovono i seguenti criteri nell'istituzione e nelle competenze di Comitati rischi endoconsiliari:

a) autonomia del comitato, con distinzione dal comitato di audit laddove esistente;

b) presidenza attribuita ad un amministratore indipendente, evitando sovrapposizioni con il presidente del consiglio di amministrazione o di qualsiasi altro comitato;

c) inclusione di membri indipendenti;

d) inclusione di membri con esperienza in materia di gestione dei rischi;

e) analisi delle strategie di rischio su base sia aggregata sia per tipologia di rischio;

f) esame e approvazione delle politiche sui rischi dell'impresa almeno una volta all'anno;

g) vigilanza sull'attuazione delle politiche di rischio approvate.

Oltre a quanto sopra rappresentato, al fine di garantire nel continuo l'attuazione delle politiche di rischio, il monitoraggio e il controllo dei rischi assunti, nonché la tempestiva adozione di azioni di mitigazione dei rischi da parte delle unità di controllo di I livello, le Società si dotano di presidi organizzativi, di natura collegiale: i cosiddetti Comitati rischi manageriali.

In sostanza i Comitati rischi manageriali costituiscono in pratica il braccio operativo in tema di presidio dei rischi aziendali, assicurando l'integrazione delle analisi sul rischio a supporto delle decisioni di

[3] Codice di Corporate Governance, Gennaio 2020, raccomandazioni 16 e 17

business e strategiche, in virtù della partecipazione allo stesso sia della Funzione di *Risk management* (o CRO) sia degli owner delle decisioni di *business* e strategiche.

Il numero, la composizione, il ruolo, le responsabilità, i meccanismi di funzionamento e le deleghe attribuite ai Comitati rischi manageriali dipendono dal complessivo modello operativo, organizzativo e di *business* della Società e sono definiti formalmente in disposizioni di *governance* (i.e. sistema di controllo interno e gestione dei rischi) o organizzativa (i.e. Circolari/Comunicazioni organizzative, Policies). È possibile, ad esempio, prevedere un Comitato manageriale unico, in caso di modelli di *governance* fortemente accentrati in cui le subsidiaries hanno limitata autonomia formale e decisionale (i.e. unità produttive) ovvero un sistema di Comitati manageriali anche locali in caso di partecipate con elevato grado di autonomia societaria (i.e. partecipate quotate). È possibile attribuire al/ai Comitato/i la responsabilità di adozione di un sistema di limiti operativi di rischio, se le deleghe attribuite dagli Organi formali, per esempio il Comitato endoconsiliare, lo suggeriscono al fine anche di assicurare un tempestivo rientro in caso di superamento di soglie di rischio definite, nell'ambito del più generale *Risk Appetite Framework* formalmente approvato.

Nonostante ci siano peculiarità specifiche, in linea generale le principali finalità di tali Organi collegiali possono essere le seguenti:

- assicurare l'attuazione delle scelte strategiche in tema di rischio, costituendo un "trait d'union" tra le strutture di controllo di primo (process e risk owner) e secondo livello (Risk management o CRO o funzione/unità analoga);
- garantire una tempestiva rappresentazione dei rischi (anche attraverso l'adozione di un sistema di limiti o soglie di rischio) alle strutture di business, non solo attraverso il sistema di reporting assicurato dal CRO o funzione analoga, ma anche attraverso l'attivazione di un processo dialettico in seno ad un organo collegiale manageriale;
- consentire che il management - indipendentemente dalla linea di business - acquisisca informazioni sui complessivi rischi aziendali e non solo relativamente al perimetro di riferimento;
- assicurare un confronto nel continuo sui rischi aziendali tra i risk owner (tipicamente unità di business) e i risk manager (tipicamente secondo livello di controllo), con riferimento a trend, esposizioni, key risk indicators ed eventuali azioni di mitigazione.

Al fine di assolvere alle finalità sopra individuate, le modalità di funzionamento dei Comitati rischi manageriali sono sintetizzabili come segue:

- convocazione regolare (in presenza o con modalità telematica) o "ad evento/necessità", per assicurare un presidio nel continuo;
- presidenza attribuita al *Chief Executive Officer* e membri individuati dai primi livelli di riporto del CEO, per assicurare la diffusione dell'informativa sui rischi e il coordinamento tra primo e secondo livello di controllo;
- strumenti informativi definiti e formalizzati, nel contenuto (i.e. classi di rischio e relativi indicatori) e nella forma (i.e. reportistica e strumenti di comunicazione, quali mail, repositories, etc.);
- attribuzione di ruoli e responsabilità definite all'unità di *Risk* indipendente (*Risk management* o Control di II livello) nell'ambito del Comitato, a supporto dell'efficace funzionamento dello stesso.

Nell'ambito di tale quadro generale, è ipotizzabile prevedere per i Comitati rischi manageriali un ruolo consultivo nei confronti del *Chief Executive Officer*/Presidente del Comitato CIeGR in relazione agli indirizzi nella gestione dei principali rischi; tale ruolo può essere esteso fino a contemplare responsabilità nell'ambito di un sistema di deleghe che dovrà essere formalmente definito, che possono includere:

- analisi periodica di esposizione ai rischi (*Risk Profile*) e *Key Risk Indicators*;

- recepimento di *Risk Policy* e *Risk methodologies*;
- approvazione dei limiti operativi e delle soglie di tolleranza;
- autorizzazione per il superamento dei limiti superiori alle soglie a livello di azienda e/o di gruppo ovvero individuazione delle possibili azioni di mitigazione dei rischi, della relativa tempistica di adozione e di eventuali vincoli alla loro assunzione;
- definizione di strategie di risposta al rischio, individuazione delle azioni da intraprendere a seguito di operazioni straordinarie o significative, o in situazioni di particolare complessità o criticità, o in caso di operazioni che coinvolgono nuovi mercati, nuovi prodotti e nuovi strumenti di mitigazione del rischio

1.4 Il Controllo di primo, secondo e terzo livello nelle corporate

Partendo dall'assunto che tutte le tipologie di rischio aziendale devono essere presidiate, nell'atto di implementare un sistema dei controlli interni che assicuri un' efficace gestione dei rischi occorre considerare la complessità e la dimensione aziendale, nonché la natura dell'attività svolta.

Premesso che tutte le strutture aziendali - e non solo le funzioni aziendali di controllo propriamente dette - sono coinvolte nella gestione dei rischi, è possibile distinguere le seguenti tipologie di controllo:

1. **Controlli di primo livello (o controlli di linea),** effettuati dalle strutture operative (di *business* e di supporto) al fine di assicurare il corretto svolgimento delle operazioni. Le strutture operative sono le prime responsabili del processo di gestione dei rischi, attraverso (i) il monitoraggio dei rischi nel rispetto di eventuali limiti operativi assegnati e (ii) l'identificazione e la valutazione dei rischi derivanti dall'operatività aziendale;
2. **Controlli di secondo livello (o controlli sui rischi e sulla conformità),** effettuati da strutture dedicate e distinte da quelle operative al fine di assicurare (i) l'indirizzo e la corretta implementazione del processo di *risk management*, (ii) il monitoraggio e controllo dei rischi, anche attraverso l'applicazione di limiti operativi e (iii) la conformità dell'operatività aziendale alla normativa interna ed esterna;
3. **Controlli di terzo livello (o revisione interna),** effettuati da una struttura dedicata ed indipendente rispetto alle strutture di primo e secondo livello, al fine di valutare - su base periodica - la completezza, l'adeguatezza, la funzionalità (in termini di efficienza ed efficacia) e l'affidabilità del sistema dei controlli interni e del sistema informativo.

Le funzioni aziendali appartenenti a diversi livelli di controllo sono tra loro necessariamente indipendenti[4], al fine di prevenire potenziali situazioni di conflitto d'interesse. In tale contesto, tenuto conto che le funzioni di *compliance* e di *risk management* sono periodicamente sottoposte a verifica da parte dell'Internal Audit, quest'ultima non può svolgere tali funzioni. Si noti, inoltre, che le funzioni di *compliance* e di *risk management*, pur essendo entrambe strutture di controllo di secondo livello, sono in linea generale e in alcune realtà più complesse tra loro indipendenti.

La costituzione di specifici Comitati manageriali, come precedentemente descritti, non può prescindere dalla necessità di inquadrare la loro attività in modo coerente nel sistema dei controlli interni. L'operato di tali Comitati, costituiti all'interno degli organi aziendali, deve essere considerato come un'importante opportunità di approfondimento su determinate tematiche da parte dell'azienda.

I presupposti per l'implementazione di un sistema di controlli interno, che risulti funzionale, completo ed efficace, sono:

- la cultura del controllo, che deve ricoprire una posizione di rilievo nella scala dei valori aziendali;
- l'esistenza di una organizzazione aziendale adeguata ad assicurare la sana e prudente gestione;
- la formalizzazione dei processi decisionali e delle funzioni affidate al personale, al fine di identificare chiaramente ruoli e responsabilità e prevenire possibili conflitti di interesse.

L'integrazione del processo di gestione dei rischi tra le diverse funzioni aziendali di controllo può essere agevolata da: (i) adozione di una tassonomia condivisa sui rischi a tutti i livelli dell'organizzazione; (ii) reportistica dei rischi integrata; (iii) adozione di metodi e strumenti di rilevazione e valutazione coerenti

[4] Con indipendenza si intende la distinzione nell'ambito del riporto gerarchico e/o funzionale, ovvero l'esistenza di un sistema di deleghe chiaramente definito che individui ambiti e perimetro di attività – nel rispetto delle *segregation of duties* - di ciascun livello di controllo, così come individuato.

in termini, ad esempio, di modello dei processi interni o di cartografia dei rischi; (iv) previsione di momenti di coordinamento formalizzati, finalizzati alla pianificazione delle rispettive attività; (v) scambio periodico di flussi informativi relativi alle risultanze emerse nel corso delle attività svolte; (vi) condivisione delle azioni di mitigazione individuate.

Sotto il profilo organizzativo, le funzioni aziendali di controllo sono tra loro separate. Nella normativa interna sono formalizzati i rispettivi ruoli e responsabilità, le modalità operative, i flussi informativi, nonché la programmazione dell'attività di controllo. Tutti questi elementi dovrebbero essere formalizzati in un documento approvato dal *board* e diffuso a tutte le strutture interessate.

Sebbene le funzioni aziendali di controllo siano tra loro indipendenti e posseggano differenti ambiti di responsabilità, devono operare con la massima collaborazione sia tra loro sia con le altre funzioni aziendali, così da rendere coerenti le proprie metodologie valutative con le strategie e l'operatività dell'azienda. In particolare, al fine di garantire una corretta comunicazione tra tutte le funzioni aziendali di controllo è necessario definire puntualmente ruoli e responsabilità, flussi informativi - sia tra le stesse funzioni che verso gli organi aziendali - contenenti le risultanze delle attività svolte da ciascuna funzione che possano risultare utili allo svolgimento delle attività da parte delle altre funzioni aziendali di controllo e, nel caso in cui gli ambiti di controllo presentino aree di potenziale overlapping o permettano di sviluppare sinergie, le modalità di coordinamento e di collaborazione. Ad ogni modo, le modalità di interazione non devono, in nessun modo, alterare - formalmente o nella sostanza - le responsabilità attribuite a ciascun organo aziendale nell'ambito del complessivo sistema dei controlli interni.

La presenza di tutti gli strumenti necessari all'espletamento delle attività, in termini di risorse umane ed economiche, competenze, accesso ai dati aziendali e a quelli esterni necessari per svolgere in modo appropriato i propri compiti contribuisce a preservare l'indipendenza delle funzioni aziendali di controllo. Con particolare riferimento alle risorse umane, è importante garantire un dimensionamento quali-quantitativo adeguato in relazione alle attività svolte. Le risorse devono disporre delle competenze tecnico-professionali necessarie e devono seguire un processo di aggiornamento e formazione continua. I responsabili delle funzioni aziendali di controllo (i) sono dotati di adeguati requisiti di professionalità e sono collocati in posizione gerarchico/funzionale adeguata, (ii) devono essere indipendenti rispetto alle aree operative (non avendone la responsabilità e non essendo gerarchicamente sottoposti ai responsabili delle stesse) e (iii) devono comunicare direttamente - senza alcuna intermediazione - con gli organi aziendali.

Alla luce di quanto sopra, i compiti delle funzioni aziendali di controllo di II livello (*Risk management* e *Compliance*) e III livello (Internal Audit) sono di seguito individuati.

(A) Funzione di Risk Management

I principali compiti della funzione di *Risk management* riguardano:

- il supporto alla definizione del *risk appetite framework*, della politica di *risk governance* e l'identificazione dei limiti operativi per le tipologie di rischio a cui è esposta l'azienda, da sottoporre per approvazione agli Organi competenti;
- la verifica dell'adeguatezza del processo di *risk management* e dei limiti operativi in coerenza con il *risk appetite framework* (e ad integrazione dello stesso);
- l'identificazione e la selezione, con il possibile supporto dei *risk owner* e di ulteriori unità di gestione e controllo dei rischi, ove esistenti, di metodologie per la valutazione dei rischi;
- la verifica, in coordinamento con le funzioni aziendali interessate, della coerenza dei sistemi di misurazione e gestione dei rischi con i processi e le metodologie di valutazione delle attività aziendali;
- la definizione e l'implementazione di *risk indicator* volti al monitoraggio dei rischi, nonché alla rilevazione di eventuali anomalie o inefficienze dei sistemi di misurazione e gestione eventualmente attuata dalle unità di primo livello;

- la valutazione dei rischi connessi all'introduzione di nuovi prodotti e/o servizi, di nuovi progetti o investimenti, di ingresso in nuovi mercati e/o di individuazione di nuovi segmenti di clientela, etc.;
- la verifica dell'adeguatezza delle azioni di mitigazione a fronte di gap rilevati nel processo di gestione dei rischi e il monitoraggio - nel continuo - dell'efficacia di queste ultime.

(B) Funzione di Compliance

I principali compiti della funzione di *Compliance* riguardano:

- il supporto alle strutture aziendali nella definizione delle metodologie di valutazione dei rischi di non conformità;
- l'individuazione di misure di prevenzione del rischio di non conformità, verificandone la corretta applicazione da parte delle strutture *owner* dell'implementazione;
- il monitoraggio, nel continuo, delle normative applicabili all'azienda;
- la valutazione dell'impatto sui processi aziendali delle normative tempo per tempo applicabili;
- la proposta di modifiche organizzative e procedurali finalizzate ad assicurare un adeguato presidio dei rischi di non conformità identificati e la verifica della loro efficacia;
- la predisposizione di flussi informativi diretti agli organi aziendali e alle funzioni interessate (e.g. *Risk management*, Internal Audit).

(C) Funzione di Internal Audit

I principali compiti della funzione di Internal Audit riguardano:

- l'esecuzione di attività di verifica volte alla valutazione della completezza, adeguatezza, funzionalità e affidabilità dei processi aziendali (inclusi quelli relativi alla gestione dei rischi) e del sistema dei controlli interni;
- la valutazione dell'efficacia del *risk appetite framework* in termini di conformità dell'operatività aziendale a tale *framework*;
- lo svolgimento di attività ispettive - la cui frequenza può essere casuale o predeterminata a seconda di quanto il processo interno oggetto di analisi sia giudicato rischioso - volte a verificare la corretta esecuzione delle attività aziendali, a tutti i livelli dell'organizzazione. L'attività ispettiva è volta a verificare anche il rispetto dei meccanismi di delega, nonché l'adeguatezza e la sicurezza del sistema informativo;
- l'identificazione di opportune azioni correttive a fronte delle anomalie rilevate durante le attività di verifica/ispettive, monitorando nel continuo l'implementazione delle stesse da parte dei rispettivi *owner*;
- la verifica dell'adeguatezza complessiva del Piano di continuità operativa dell'azienda;
- la facoltà di svolgere di attività ispettive sui fornitori ritenuti critici per l'operatività aziendale presso le rispettive sedi.

1.5 La figura del Chief Risk Officer: necessità o opportunità?

In un'impresa con una *governance* di controllo a tre livelli, la funzione di secondo livello (come quella del *Chief Risk Officer*) deve essere indipendente dalle funzioni di *business*, per poter esercitare la propria attività con caratteristiche di terzietà e al fine di poter attuare un *challenge* sulle funzioni di *business* che gestiscono i rischi, per poter portare valore nel percorso decisionale, con un obiettivo di supporto al *business* e non di mera adeguatezza ai dettami degli *standard setters*.

La necessità di assicurare al contempo una stretta e diretta relazione con il *business* e un sempre maggiore coinvolgimento nella definizione del piano strategico e industriale, può indurre le aziende alla definizione di una funzione indipendente dalle unità di *business*, operative e tecniche, ma garante di un approccio unico, omogeneo e sistematico nella gestione dei rischi sia in termini di processo che di approcci metodologici, modelli e strumenti applicativi.

A prescindere dalla dimensione della società, è chiaro come la gestione del rischio sia diventata quindi un fattore strategico critico per il successo delle organizzazioni e una funzione di *risk management* autonoma, che miri a portare valore aggiunto nel processo decisionale tramite la valutazione del rischio, non può che rivestire un ruolo al vertice dell'organizzazione aziendale.

Partendo da questi elementi risulta pertanto opportuno prevedere una figura di *Chief Risk Officer* (CRO) alla guida della funzione di *Risk management*, posizionata a livello apicale per consentire una visione integrata della rischiosità dell'impresa assicurandone il controllo, la valutazione, nonché l'efficacia e la completezza nel considerare e presidiare tutti i rischi effettivamente rilevanti.

1.5.1 Mission del Chief Risk Officer

Le *mission* del *Chief Risk Officer*, nell'ambito della complessiva *risk governance*, possono essere declinate in tre ambiti principali.

In primis il *Chief Risk Officer* agisce a supporto del CEO, del *top management* e degli organi aziendali di governo (Comitato Controllo e Rischi e *Board*) nelle fasi di definizione della strategia assicurando la vista sui rischi aziendali principali e i relativi impatti sui *target* strategici, integrando la definizione della strategia con la proposta di soglie adeguate di propensione al rischio (*Risk Appetite*), identificando eventuali rischi impliciti nella pianificazione, assicurando pertanto la consapevolezza e la diffusione della cultura dei rischio nell'ambito del processo strategico.

In secondo luogo, il *Chief Risk Officer*, alla guida di una funzione sempre più integrata nel *business* e nei processi decisionali, facilita la gestione dei rischi all'interno di tutti i processi aziendali, favorendo l'approccio *risk based thinking*. Il *Risk Manager* partecipa quindi attivamente alle decisioni del *business*, che sono pertanto assunte nella consapevolezza del rischio. Esempi ne sono la partecipazione ai processi di investimento, allo sviluppo ed aggiornamento di prodotti e servizi, alla gestione dei progetti, a partire dalla preparazione dell'offerta e per tutta a la fase di esecuzione, incluso il post-vendita. Il CRO assicura, in coerenza con gli standard e le *best practices* nazionali ed internazionali, un supporto al *business* anche attraverso la definizione, l'aggiornamento e lo sviluppo delle metodologie, delle metriche e degli strumenti per la corretta misurazione e gestione dei rischi.

Last but not least il *Chief Risk Officer* – attraverso la propria attività – assicura agli organi di governo dell'impresa e agli *stakeholder*s una visione sui rischi che ne consenta da parte degli stessi un governo e una percezione consapevoli e integrati nell'ambito della complessiva *corporate governance*, attraverso la comunicazione periodica, completa e tempestiva agli organi aziendali sui rischi e sui relativi *trend*, anche attraverso la partecipazione ai comitati endo-consiliari (e.g. Comitato Controllo e Rischi, Steering committee) e manageriali (e.g. Comitato Rischi Finanziari, Comitato Rischi di Gruppo) eventualmente dedicati alle tematiche di rischio.

Avendo delineato le tre mission fondamentali di un *Chief Risk Officer*, appare evidente come - per il rispetto di un generale principio di segregazione dei ruoli – a tale figura non possano essere attribuite

responsabilità sulla gestione operativa; tale ruolo spetta, infatti, alle unità operative o di *business* (*risk owners*).

In aggiunta a quanto sopra, nell'ambito dei controlli di II livello e in particolare in contesti fortemente regolamentati, il *Chief Risk Officer* fornisce supporto e strumenti metodologici idonei all'identificazione e alla gestione di specifiche tematiche di rischio di *compliance*, riferibili ad esempio al mantenimento di un adeguato sistema anticorruzione aziendale. Nelle realtà caratterizzate da minore complessità operativa e organizzativa, per non appesantire eccessivamente la struttura di *governance* dell'impresa, può rivestire la responsabilità di garantire la piena conformità dell'organizzazione alle normative applicabili. Ciò non si ritiene auspicabile nelle realtà maggiorente strutturate, in considerazione della peculiarità dei temi di *risk* rispetto ai temi di mera *compliance*.

1.5.2 Posizionamento organizzativo del Chief Risk Officer

Sebbene il posizionamento non sia necessariamente standardizzabile, alcuni fondamentali principi costituiscono fattori di successo per un suo efficace funzionamento:

- autonomia e indipendenza di giudizio rispetto agli altri *Top / Chief managers*;
- supervisione strategica ed olistica delle aree di *business* e dei rischi connessi, senza detenere l'*ownership* dei singoli rischi;
- accesso alle informazioni rilevanti e a flussi informativi periodici (in taluni casi anche di dettaglio su singole transazioni o operazioni significative, nonché su dati massivi potenzialmente di impatto su *target* finanziari ed economici);
- partecipazione attiva (e non mediata) agli Organi aziendali (Comitati endo-consiliari, Comitato Controllo e Rischi e/o *Board*) e ai Comitati manageriali laddove esistenti (es. Comitato Rischi) per una rappresentazione efficace, tempestiva e completa sui principali rischi aziendali.

Secondo tali principi generali, nel panorama delle Corporate italiane sono per lo più osservabili differenti i modelli organizzativi che vedono il CRO posizionato a riporto del CEO, del CFO o anche all'interno delle strutture di *business*.

In relazione all'esperienza bancaria maturata nel tempo, come best practices vengono segnalati i seguenti modelli organizzativi:

1. **Riporto del Risk Management al Chief Executive Officer**: tale approccio garantisce autonomia e indipendenza di giudizio rispetto agli altri *Top / Chief managers* e la supervisione strategica ed olistica dei rischi; è necessario in tal caso assicurare tempestivi e diretti flussi informativi tra le unità operative e il CRO, anche di dettaglio e con viste specifiche per le analisi di rischio, al fine di assicurare non solo una mera rappresentazione dei rischi ma un loro governo concreto. La definizione di idonei meccanismi di coordinamento tra l'area del CRO e i diversi presidi aziendali risulta particolarmente rilevante per le società che i) gestiscono vari *business*, ii) hanno una forte diversificazione geografica, iii) hanno una consolidata tradizione organizzativa che prevede strutture di *risk management* a silos (tipicamente funzioni che si occupano di *risk management* finanziario oppure di gestione assicurativa dei rischi).
2. **Riporto del Chief Risk Officer al Consiglio di Amministrazione**, sia per via diretta sia attraverso la partecipazione ad un Comitato endo-consiliare. In questo secondo caso è preferibile prevedere un Comitato Rischi separato dal Comitato di Controllo Interno, per garantire un adeguato focus sugli aspetti specifici di rischio. Tale approccio presenta in primo luogo i vantaggi dell'autonomia decisionale e di indipendenza dagli altri *Top/Chief manager*, inclusa la funzione *Finance*, l'allineamento strategico con i vertici aziendali e un riporto tempestivo della supervisione dei rischi agli Organi aziendali. Il canale diretto con il

Comitato Controllo e Rischi agevola infatti il rilascio, da parte di quest'ultimo, del parere preventivo al Consiglio sulla gestione dei rischi coerentemente con gli obiettivi strategici individuati. In tal caso, tuttavia, risulta opportuno prevedere meccanismi di coordinamento tra strutture di business, strutture deputate al supporto delle decisioni strategiche e CRO al fine di consentire tempestività di analisi e di rappresentazione al Board anche fondandosi su evidenze di business.

Concludendo, la domanda da porsi oltre alla collocazione della funzione del CRO, è se questa abbia il giusto livello di *sponsorship* dal *Board*/CEO/Comitato Rischi/ Collegio Sindacale e le adeguate risorse (competenze e numero) per poter identificare, valutare, mitigare e monitorare tutti rischi (strategici, finanziari, operational e di *compliance*) ai vari livelli (i.e. *business*, Paese e commessa).

1.5.3 Requisiti del Chief Risk Officer

In coerenza con quanto prima delineato, è possibile identificare alcuni punti chiave - esemplificativi - del profilo professionale di un *Chief Risk Officer* e/o ad ogni modo delle figure professionali riconducibili a tale area o unità organizzative analoghe:

- capacità analitiche per la comprensione dei *business* a supporto di una tempestiva identificazione dei rischi connessi, nonché per l'individuazione di eventuali azioni di mitigazione;
- competenze tecnico – quantitative per la rappresentazione - sia alle aree di *business* sia al *Top Management* sia agli Organi aziendali - dei risultati di valutazione o quantificazione dei rischi;
- capacità di sintesi dei fenomeni aziendali per la rappresentazione sinottica agli Organi aziendali dei rischi e dei relativi impatti sui *target* economico e finanziari e sugli obiettivi strategici;
- proattività al fine di poter cogliere le evoluzioni del contesto e poter intervenire in maniera tempestiva eventualmente adattando/modificando le azioni in essere;
- competenze di interpretazione degli scenari esterni all'impresa per la tempestiva identificazione di eventuali minacce esterne al *business* e al raggiungimento degli obiettivi;
- conoscenze del contesto in cui l'impresa opera (settoriale, di *governance*, macroeconomico, etc.) per poter agire proattivamente limitandone eventuali impatti negativi.

Quanto sopra appare congruente con i requisiti definiti per gli intermediari vigilati[5] in cui la figura del *Chief Risk Officer* ha raggiunto ormai un certo livello di "maturità". A tal riguardo, infatti, la Banca d'Italia disciplina[6] requisiti specifici per le Funzioni Aziendali di Controllo (FAC) – in cui rientra il CRO - che dovranno in particolare:

- disporre dell'autorità e delle risorse necessarie per lo svolgimento dei loro compiti;
- avere accesso ai dati aziendali e a quelli esterni necessari per svolgere in modo appropriato i propri compiti;
- essere dotate di adeguate risorse economiche, eventualmente attivabili in autonomia, eventualmente ricorrendo a consulenze professionali esterne;
- disporre di personale adeguato sia per numero che per competenze tecnico-professionali;

disporre di personale che non sia che coinvolto in attività che tali funzioni sono chiamate a controllare.Da quanto sopra riportato appare evidente come l'esistenza in azienda di un ruolo organizzativo focalizzato sul governo dei rischi di impresa - che ne assicuri una vista olistica e di

[5] cfr. Par 6 "Principi Generali", Sezione I, Capitolo 3, Titolo IV, Parte Prima della Circolare della Banca d'Italia n. 285 del 17/12/2013

[6] cfr. Par 1, Sezione III, Capitolo 3, Titolo IV, Parte Prima

portafoglio - possa costituire quanto meno un'opportunità – se non una necessità - per la sostenibilità dei risultati nel breve come nel medio – lungo termine.

Tale assunto è avvalorato da varie analisi e studi sull'efficacia ed efficienza della funzione di *Risk management* e sul processo di gestione dei rischi come strumento di valore per l'impresa: è stato rilevato che l'impresa è più redditizia se ha una funzione di *risk management* apicale con la sponsorship di un Comitato Rischi. Queste analisi sono state principalmente effettuate in Europa, in Germania, Italia e UK (Lechner and Gatzert, 2018; Florio and Leoni, 2017; Cineas/Mediobanca – Osservatorio sulla diffusione del *risk management* nelle medie aziende italiane - 2020).

Di fatto, la redditività dell'impresa è correlata alla presenza di una *governance* di *risk management* ed in generale ad una organizzazione con la capacità di legare la pianificazione strategica con la gestione dei rischi di impresa. In altre parole, il *risk management* dovrebbe essere una parte integrante del processo di generazione del valore, a sua volta inteso come somma tra la valorizzazione del modello di *business* corrente e quella delle future opzioni di sviluppo. Una gestione efficiente dei rischi mira a sfruttare le opportunità di *business* con l'obiettivo di favorire la crescita futura, proteggendo al contempo il valore creato. Il modello logico di riferimento per la gestione dei rischi è profondamente integrato nei meccanismi decisionali aziendali ed è di tipo tridimensionale, in quanto passa attraverso l'identificazione della natura del rischio (operativo, finanziario, strategico, di *compliance*), del livello di riferimento (per esempio *business*, Paese, commessa) e della fase evolutiva del progetto (per esempio sviluppo, realizzazione, gestione).

Appare altresì evidente come, a prescindere dall'allocazione organizzativa di tale figura, i requisiti di indipendenza dalle unità operative, di autonomia di giudizio e nella rappresentazione dei rischi e dei relativi impatti alle aree di *business*, al *Top management* e al *Board*, costituiscano un fattore abilitante all'effettiva utilità della figura del *Chief Risk Officer* (o funzione equivalente).

I principi sopra rappresentati intendono costituire spunti di riflessione per consentire che la figura del CRO eserciti da un punto di vista sostanziale le *mission* di supporto alle decisioni operative, alla definizione della strategia e all'integrazione della *risk governance* nella complessiva *corporate governance* di impresa e ne sia abilitato un ruolo decisionale, in tema di rischio, e non solo formale.

2 RISK & STRATEGY

2.1 Il Risk Appetite Framework (RAF)

2.1.1 Definizione, componenti e funzioni del RAF

La valutazione dei rischi, e dei relativi presidi di controllo, consente di qualificare in modo più corretto gli obiettivi strategici in termini di rischio/rendimento e fornisce una chiave di lettura indispensabile per valutare la capacità dell'azienda di realizzare le proprie strategie. Un approccio e/o processo particolarmente valido al fine di determinare la propensione al rischio desiderata, in termini di entità e tipologie di rischio che l'impresa è disposta ad assumere rispetto alla propria capacità massima di assunzione dei rischi, nel perseguire i propri obiettivi di *business*, è il *Risk Appetite Framework* (RAF).

Introdotto come strumento obbligatorio per le banche, a seguito di un documento di indirizzo pubblicato dal Financial Stability Board nel 2013 (*Principles for An Effective Risk Appetite Framework*), ed adottato anche dal Committee of Sponsoring Organisations of the Treadway Commission (*Understanding and Communicating Risk Appetite,* 2012) nell'ambito della definizione dell'*Enterprise Risk management* Framework, il RAF rappresenta oggi un approccio fondamentale a disposizione dei *board*, e di tutte le tipologie di impresa, per il governo e il controllo dei rischi della gestione e per la corretta allocazione delle risorse sulle singole aree di *business*.

Il *Risk Appetite Framework* rappresenta uno strumento fondamentale anche per garantire lo sviluppo sostenibile nel medio-lungo periodo, evitando che siano scelte opzioni di massimizzazione di profitti di breve, associate però ad un eccessivo livello di rischio rispetto alla capacità massima di assunzione dei rischi.

L'introduzione del RAF nelle società industriali, attive in settori molto differenti ed eterogenei, dovrà essere guidata da principi di flessibilità che tengano in adeguata considerazione le complessità legate alla presenza di rischi di natura diversa, valutati anche in modo qualitativo, difficilmente modellizzabili e spesso tra loro fortemente correlati.

L'adozione del RAF potrebbe essere indirizzata ad aumentare il grado di consapevolezza del profilo di rischio dell'azienda, anche attraverso l'adozione di *statement* non solo quantitativi ma anche qualitativi che, declinando opportunamente mission e valori dell'azienda, forniscano un indirizzo gestionale su livello e natura dei rischi accettabili e sulla loro compatibilità con gli obiettivi strategici di breve e medio/lungo termine.

Le considerazioni esposte di seguito forniscono dunque solo una linea guida per lo sviluppo e l'aggiornamento periodico di un *Risk Appetite Framework* coerente con gli obiettivi di *business* e le *best practice*, da declinare rispetto alle specificità delle singole realtà aziendali, in linea con la loro *risk culture*.

Secondo il FSB, il *Risk Appetite Framework* può essere definito come un approccio generale, integrato con la strategia, che include politiche, processi, controlli e sistemi, per la determinazione, la comunicazione e il monitoraggio della propensione al rischio (FSB, 2013, p. 2). Esso si compone dei seguenti elementi, descritti in dettaglio più avanti:

1. I limiti relativi alla propensione al rischio, declinati in termini di *risk capacity, risk appetite, risk tolerance e risk profile*.
2. I limiti di rischio assegnati alle diverse unità di *business*, che si qualificano come *risk-owner*.
3. Un *Risk Appetite Statement*.
4. Una descrizione dei ruoli e delle responsabilità in tema di costruzione, approvazione e monitoraggio del RAF.

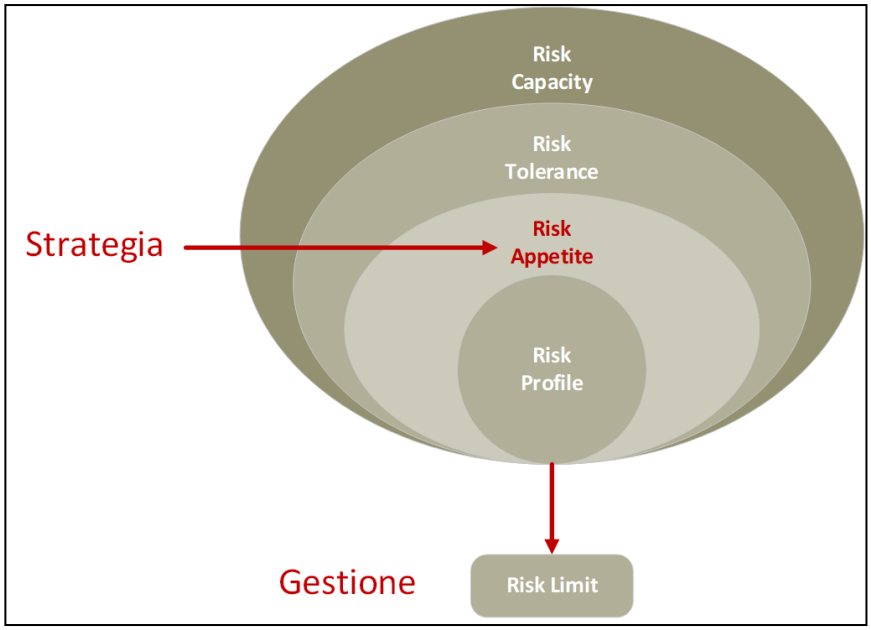

Figura 1 - Le soglie del RAF

La figura 1. mostra le principali componenti del RAF, che rappresentano altresì le soglie qualificanti la propensione al rischio dell'azienda. In particolare:

- La **risk capacity** (massimo rischio assumibile) può essere definita come il livello massimo di rischio – volatilità delle *performance* e livello di perdite – che una impresa è tecnicamente in grado di sopportare senza fallire. Tale valore potrebbe, per semplicità, essere rappresentato ad esempio dal patrimonio netto (e quindi dalla capacità di assorbire le perdite) e dalla liquidità (cash flow) disponibili, tenuto conto del piano e delle condizioni esterne attuali e prevedibili[7].
- Il **risk appetite** (propensione al rischio) rappresenta il livello di rischio (complessivo e per tipologia) che l'impresa intende o è disposta ad assumere per perseguire i propri obiettivi strategici. Il *risk appetite* è qualcosa in più di un KPI di *risk management*: è lo strumento core per allineare strategia, allocazione del capitale e delle risorse, e rischi. I rischi oggetto del RAF, e i livelli *target* dei singoli *Key Risk Indicators* (KRI), dipendono naturalmente dal modello di *business* dell'impresa e dalle strategie di volta in volta deliberate.
- La **risk tolerance** (soglia di tolleranza) è la deviazione massima dal risk appetite che l'azienda ritiene di essere in grado di sopportare senza compromettere il raggiungimento degli obiettivi strategici o addirittura senza incorrere nel rischio di fallimento per perdite, problemi operativi o danni reputazionali. Essa definisce il livello di incertezza (e di perdita) che l'organizzazione è pronta ad accettare, nel complesso e per singola *business unit* o tipologia di rischio. La soglia di tolleranza è fissata in modo da assicurare in ogni caso margini sufficienti per operare, anche in condizioni di scenario avverso, entro il massimo rischio assumibile: la *risk capacity* diventa quindi un vincolo per la *risk tolerance*. Quest'ultima può essere determinata sulla base di uno stress test delle variabili di piano (worst-case scenario) e/o di un management buffer rispetto al *risk appetite*, che contribuisce a qualificare la propensione al rischio. Sarà quindi stabilito un margine dalla *capacity* tanto maggiore quanto maggiori sono gli impatti determinati dalle ipotesi di scenario prese a riferimento e quanto più marcata è la volontà del *board* e del management di mantenere un elevato grado di

[7] Nel caso delle banche, tale soglia configura anche il livello di rischio compatibile con l'obiettivo di rispettare i requisiti regolamentari o gli altri vincoli imposti dall'autorità di vigilanza.

flessibilità rispetto alla possibilità di cogliere ulteriori opportunità di sviluppo futuro del *business* o di evitare situazioni di difficoltà gestionale (ossia quanto minore è la relativa propensione al rischio).

- Il **risk profile** è il livello di rischio assunto dall'impresa a una determinata data (*point in time*) e si qualifica in termini di un sistema integrato di KPI, KRI e/o di scostamenti economico-finanziari dai risultati di *business*. Esso rappresenta un insieme di valori da monitorare e da confrontare con le soglie precedenti, al fine di valutare il pieno raggiungimento degli obiettivi strategici e/o consentire di mettere in atto per tempo le necessarie misure correttive.
- I **risk limit** sono dati dalle soglie di rischio che, in coerenza con gli obiettivi aggregati di *risk appetite*, devono essere assegnati come obiettivo/vincolo alle singole unità *risk taking* (*business unit* e *legal entities*) per assicurare che esse prendano decisioni coerenti con la propensione al rischio deliberata. Tali limiti andranno definiti a cascata, in modo tale da poter essere scomposti in KRI specifici per le unità rilevanti.

Nell'esperienza bancaria, sulla base delle soglie precedenti, annualmente è definito un *Risk Appetite Statement (RAS)*, ossia una dichiarazione formale in linea generale contenente i seguenti elementi:

- l'orizzonte temporale di riferimento, indicando le connessioni con le strategie aziendali in termini di business, di adeguatezza patrimoniale e liquidità (nel caso delle banche), e di redditività.
- i rischi ai quali l'azienda intende esporsi (*risk preferences*) e il relativo grado di rilevanza (mappatura dei rischi);
- la rappresentazione delle politiche adottate per diversi ambiti di rischio. In particolare, tali politiche forniscono un insieme di linee guida e di azioni per gestire il rischio e ottimizzare il rapporto rischio-rendimento;
- la definizione delle soglie (*risk thresholds*);
- per i rischi difficilmente quantificabili, indicazioni di natura qualitativa;
- la declinazione in limiti operativi, definiti, in linea con il principio di proporzionalità, per tipologie di rischio, unità e/o linee di business, linee di prodotto e tipologie di clienti/portafoglio.

Il RAF, e di conseguenza il RAS, devono includere tutti i rischi rilevanti, considerati materiali, in un'ottica *forward-looking*, anche sulla base di una valutazione delle attese degli *stakeholder* dell'impresa. La prospettiva degli *stakeholder* può caratterizzare l'intero RAF e rappresentare un criterio di articolazione dei singoli KRI, come meglio specificato in seguito.

2.1.2 Il processo di determinazione del RAF

Le caratteristiche del processo di implementazione di un *framework* di *risk appetite* dipendono dalla dimensione e dalla complessità della azienda, dall'ambiente in cui opera e dal livello di maturità dei relativi processi di *risk management*. Le considerazioni esposte di seguito forniscono dunque solo una linea guida per lo sviluppo e l'aggiornamento periodico di un *Risk Appetite Framework* coerente con gli obiettivi di *business* e le *best practice*, da declinare rispetto alle specificità delle singole realtà aziendali.

In termini di **governance del processo**, il coordinamento operativo è affidato al *Chief Risk Officer (CRO)*. È buona norma tuttavia che siano coinvolte tutte le funzioni aziendali, in base alle rispettive competenze. Il RAF infatti deve essere uno strumento di direzione e controllo, ma anche di gestione. Se resta un atto formale, è difficile immaginare che esso sia efficace nell'indirizzare il processo decisionale dei *risk owner* e possa quindi garantire una assunzione di rischio consapevole.

In linea generale:

- Il **Consiglio di Amministrazione** definisce e approva il RAF complessivo dell'impresa o del Gruppo. Approva il *Risk Appetite Statement*, sull'orizzonte di piano e su base annuale (in coerenza con il *budget*). Monitora inoltre periodicamente (su base trimestrale o almeno semestrale) il rispetto delle soglie e delibera l'azione di eventuali misure correttive.
- Il **CEO**, in collaborazione con il **Chief Risk Officer (CRO),** propone e cura la determinazione di soglie e indicatori di rischio coerenti con le strategie e con gli indirizzi del *board*, e la relativa declinazione in limiti di rischio per le *business unit* e i *risk owner*, e, ove opportuno, per le singole *legal entities* del gruppo.
- Il **CRO** cura e coordina inoltre il processo di raccolta dei dati sui rischi assunti ai fini della definizione del *risk profile* e del monitoraggio del rispetto delle soglie RAF e dei limiti di rischio.
- I **responsabili delle business units e delle legal entities** collaborano nella individuazione delle misure (KPI e KRI) e delle soglie di rischio in funzione degli obiettivi strategici.
- La funzione di **internal auditing**, o una terza parte indipendente, verifica l'adeguatezza del processo e valuta l'efficacia e l'efficienza dei controlli interni e degli altri strumenti di mitigazione dei rischi, formulando proposte di miglioramento.

Quanto allo **sviluppo del processo**, è fondamentale che esso sia integrato, anche in termini di tempistica, con la pianificazione strategica. CRO e CFO devono quindi collaborare in modo intenso affinché le tipologie di rischio e le soglie RAF siano coerenti con i contenuti e le variabili *target* del piano.

Le singole fasi del processo di implementazione del RAF, impostato partendo da un'analisi delle aspettative degli *stakeholder*, possono essere rappresentate come in Figura 2.

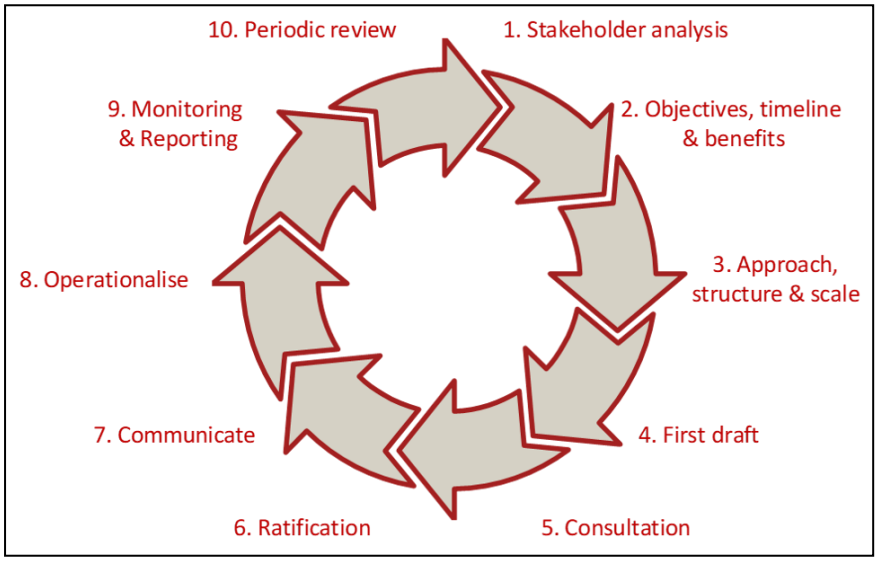

Figura 2 - Step by step cycle of risk appetite development

Esse comprendono le seguenti azioni:

1. Identificare gli *stakeholder* interni/esterni, i loro obiettivi e aspettative, e coinvolgerli nella definizione del *framework*.
2. Stabilire gli obiettivi di soddisfazione degli *stakeholder*, le relative *timeline* e i *target* attesi in termini di livello e controllo del rischio.
3. Definire la struttura di massima del *Risk Appetite Framework*, in termini di numero e tipologie di indicatori (KRI), e di articolazione dei singoli indicatori (es. indicatori di primo livello, declinati poi in indicatori di secondo livello).

4. Produrre il primo draft ed avviare una fase di condivisione interna (indicare uffici da coinvolgere).
5. Formalizzare e ratificare *il Risk Appetite Framework*.
6. Condividere il RAF con gli *stakeholder* fino all'approvazione formale da parte del CdA.
7. Implementare il RAF sul piano operativo tramite la definizione e la comunicazione di *risk limit*.
8. Implementare sistemi di monitoraggio e *reporting*.
9. Collegare gli indicatori RAF al processo decisionale di *business*.
10. Attuare una revisione periodica dell'intero *framework*.

Alcune aree di attenzione nello sviluppo delle singole fasi sono rappresentate in figura 3. Il riferimento alle aree di attività deve essere ovviamente declinato in funzione delle *business unit* rilevanti per la singola *corporate*.

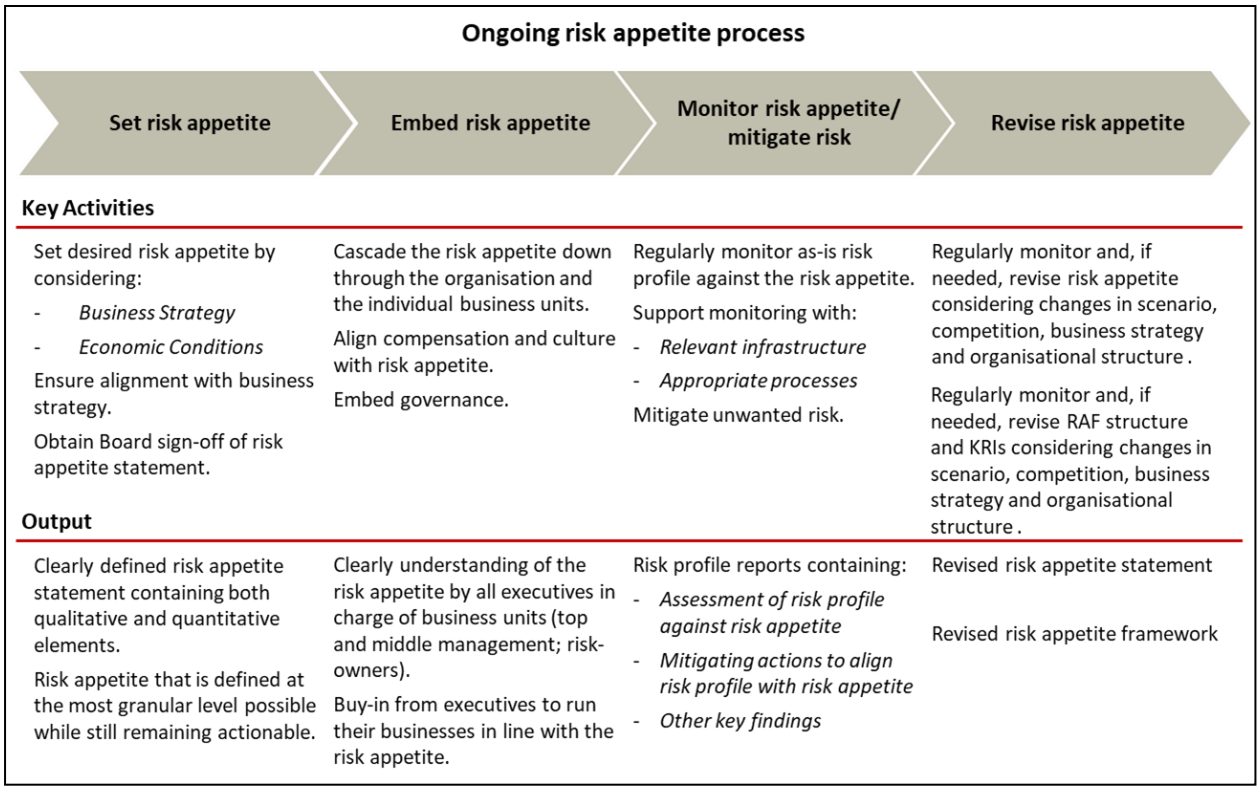

Figura 3 - Le aree di attenzione nel processo di implementazione del RAF

Dal punto di vista metodologico, inoltre, la definizione delle soglie RAF richiede un processo di analisi articolato nei seguenti *step*:

- identificazione degli *stakeholder* rilevanti e delle rispettive misure di utilità/impatto, alla luce degli obiettivi del piano strategico.
- individuazione degli ambiti di attività, dei processi e dei risultati della gestione impattati dal comportamento degli *stakeholder* o che possono avere un impatto sulle attese degli *stakeholder* nell'arco di piano.
- individuazione dei rischi connessi con gli ambiti sopra individuati.
- definizione degli indicatori di rischio nel caso di rischi misurabili e misurati.

- definizione, per ciascuna tipologia di rischio identificata e misurata, delle soglie *target* (almeno in termini di *risk appetite* e di *risk tolerance*), in coerenza con gli obiettivi del piano.
- definizione di eventuali "*management buffer*" rispetto alle soglie precedenti, per tener conto di eventuali rischi non misurati o non misurabili.
- definizione delle procedure e degli interventi gestionali da attivare nel caso in cui sia necessario ricondurre il livello di rischio entro l'obiettivo o i limiti prestabiliti.
- definizione delle procedure di *escalation* in caso di sconfinamento.
- definizione del processo di monitoraggio e dei relativi tempi.

L'efficacia del RAF quale strumento di *risk governance* è favorita dalla presenza di alcune condizioni abilitanti, quali:

- La presenza in azienda di una adeguata e diffusa cultura del rischio.
- Sistemi di misurazione dei rischi evoluti e affidabili.
- Il coinvolgimento ed un buon livello di comunicazione e collaborazione tra tutti i livelli organizzativi dell'azienda (CdA – *Top Management* – Livelli operativi).
- La volontà di integrare e qualificare le decisioni strategiche con valutazioni dei rischi, per determinare obiettivi di rischio-rendimento.

A seguito della definizione e dell'approvazione del RAF è inoltre opportuno predisporre opportune *policy* in materia di assunzione e gestione dei rischi, volte a garantire che siano presenti efficaci meccanismi di mitigazione per i rischi "non evitabili" e altrettanti presidi e strategie di immunizzazione, minimizzazione e/o di trasferimento per quelli da mitigare perché non in linea con la strategia e il *risk appetite* desiderati.

2.1.3 Le soglie RAF: alcuni esempi

Gli indicatori su cui formulare le soglie RAF dipendono dalle tipologie di rischio connesse con i singoli *business model* e con i piani strategici. In linea generale, essi rappresentano misure, quantitative e qualitative, dei rischi rilevanti per l'azienda.

I relativi valori soglia andranno determinati sulla base dei piani strategici (per il *risk appetite*) e delle relative analisi di scenario e di sensitività e, in ogni caso, della propensione al rischio deliberata dal *board*.

I singoli indicatori RAF possono essere declinati per tipologia di *stakeholder*. Ad esempio, con riferimento agli azionisti, si possono utilizzare misure di rischio legate al *Total Shareholder Return* o alla crescita degli utili; per i clienti, indicatori legati alla *customer loyalty*, alla *customer satisfaction*, alla reputazione, al numero dei reclami, alle non conformità di prodotto rilevate da verifiche di audit; per i dipendenti, indicatori che esprimano il tasso di *turnover* volontario, e altri.

La Tabella 1 mostra un esempio di come si possano articolare soglie di *risk appetite* in termini di KRI e KPI, in funzione della strategia deliberata, per la categoria di *stakeholder* "dipendenti".

Tabella 1 - Un esempio di indicatori RAF per la categoria di *stakeholder* "dipendenti"

Strategia	**Risk appetite (KRI)**	**Target (KPI)**
Le nostre persone contribuiscono con soddisfazione e determinazione al successo della nostra azienda.	1. Probabilità di scostamento rispetto al livello *target* di soddisfazione del personale > 12% e relativo impatto economico	1. Soddisfazione del personale: 70%

La nostra strategia del personale si pone i seguenti obiettivi: • attrarre e trattenere le competenze e le capacità richieste per raggiungere i nostri obiettivi strategici • sviluppare e mantenere la nostra leadership di mercato • consolidare la nostra cultura organizzativa.	2. Deviazione standard del tasso di turnover volontario > X% e corrispondenti costi attesi 3. Volatilità del tasso di turnover dei dipendenti in un arco temporale (deviazione standard > X%) e costo atteso connesso per la minimizzazione 4. Costo atteso per la sostituzione di dirigenti con responsabilità strategiche senza un piano di successione approvato (probabilità di uscita per costo medio)	2. Tasso massimo di turnover volontario: 15% 3. Tasso massimo di turnover volontario di dipendenti con meno di un anno di servizio: 20% 4. Piano di successione disponibile per il 100% dei dirigenti con responsabilità strategiche

In ogni caso, gli indicatori di rischio devono essere legati alla tassonomia adottata (cfr. Appendice A) e riflettere le tipologie di rischio considerate rilevanti nell'orizzonte di piano.

Così, ad esempio, un'impresa potrebbe determinare un obiettivo RAF in termini di *earnings at risk* o di leva finanziaria massima, considerando la media dei peer e i propri piani di sviluppo. Oppure, si potrebbe assumere quale riferimento il *cash flow* operativo risultante dal *business plan* e declinare su tale base *risk appetite* (valore di piano) e *risk tolerance* (valore determinato tramite analisi di scenario o di *sensitivity*). Ancora, nell'ambito dei rischi finanziari, per il rischio di cambio, è possibile identificare come *risk appetite* un determinato tasso di cambio medio atteso sull'orizzonte di piano, e identificare valori di *risk tolerance* corrispondenti alla perdita massima accettata per effetto di un andamento sfavorevole del cambio in caso di scenario avverso.

La Figura 4 mostra un esempio di come gli indicatori RAF possono essere articolati e valutati in termini di *risk appetite* e *risk profile* per singola tipologia di rischio.

L'adozione di un modello ERM aiuta a identificare i rischi strategici e a declinarli in opportune misure e KPI.

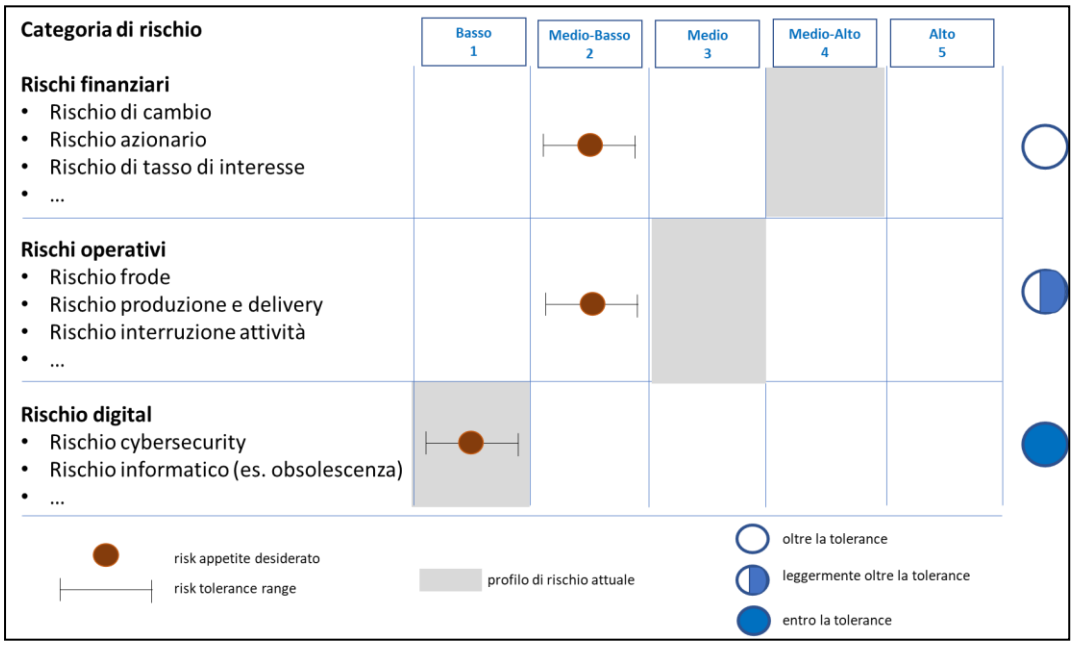

Figura 4 - Esempio di articolazione delle soglie RAF

2.2 Decisioni strategiche e loro declinazione nell'organizzazione aziendale

Si può definire *strategica* una decisione che si pone l'obiettivo di delineare il percorso ottimale per una efficiente allocazione delle risorse in ottica di massimizzazione del valore sostenibile per tutti gli *stakeholder*, coerente con la mission e nel rispetto dei *core values* aziendali. Nello svolgimento del percorso evolutivo e di sviluppo aziendale molteplici e differenti sono le decisioni strategiche e i momenti nei quali le stesse dovranno essere analizzate e in ultima analisi assunte o scartate; tuttavia ai fini del presente documento, non sembra prioritario intraprendere un'analisi delle molteplici tipologie di scelte strategiche che l'azienda potrebbe trovarsi ad affrontare nel corso della sua vita utile poiché largamente dipendenti da variabili specifiche di contesto, di settore e di *business* difficilmente sintetizzabili o generalizzabili. Sembra invece opportuno evidenziare come il processo decisionale strategico debba seguire una costante sequenza logica di sviluppo, che dovrebbe trovare evidenza nella documentazione predisposta a favore degli organi deputati alla assunzione della scelta stessa e in ultima analisi trovare una sintesi nell'ambito del periodico aggiornamento del *business plan* nonché dello sviluppo del *Risk Appetite Framework*.

In relazione a quest'ultimo aspetto occorre premettere che, mentre alcune aziende potrebbero decidere di sviluppare strategia e RAF parallelamente, e quindi integrando i due processi e andando a perfezionare i due aspetti progressivamente durante lo sviluppo delle decisioni strategiche, altre potrebbero decidere di dare priorità, anche temporale, all'uno o all'altro processo. A prescindere da quale sia l'approccio adottato è importante agire su entrambi gli aspetti in gioco in un'ottica di continuo allineamento al fine di ottenere un *Risk Appetite Framework* maggiormente dettagliato grazie all'individuazione di relative *risk tolerances* coerenti con la *risk capacity* e con il profilo di rischio-rendimento della strategia stessa. A questo riguardo, tale verifica può essere svolta mediante l'utilizzo dei *Key Performance Indicators* (KPIs) ovvero indicatori di *performance*, progettati e selezionati al fine di fornire una panoramica circa le prestazioni raggiunte dall'organizzazione nonché dalle sue principali funzioni e/o unità di *business* in un determinato intervallo temporale. Tuttavia, al fine di permettere la creazione di un sistema di controllo in grado di misurare adeguatamente la *performance* (*actual* o *forecast*) sarà opportuno considerare la stessa non solo in termini assoluti ma anche in funzione del rischio assunto; conseguentemente, è necessario affiancare agli indicatori di *performance* anche quelli di rischio (*Key Risk Indicators - KRIs*), tenendo comunque presente la finalità della misurazione che può essere svolta in logica *backward-looking*, piuttosto che *forward- looking,* per rispondere alle esigenze predittive o all'abilitazione delle suddette scelte strategiche. In altre parole, potremmo dire che la valutazione dei rischi, e dell'efficacia delle relative misure di prevenzione e gestione, qualifica gli obiettivi strategici e contribuisce a una più consapevole formulazione dei piani di sviluppo futuro.

I *Key Risk Indicators* sono generalmente indicatori di tipo predittivo, focalizzati sull'analisi delle cause che potrebbero generare il rischio, individuati con l'obiettivo di fornire una percezione dell'ammontare del profilo di rischio in essere ovvero cogliere in anticipo l'eventuale possibilità di un mancato raggiungimento dei *performance target* prefissati. L'efficacia predittiva di tali indicatori cresce quanto più il KRI è in grado di avvicinarsi alla radice della causa ("*root cause*") dell'evento rischioso ed è interpretato considerando le relative soglie (cfr. Par. 2.1), il superamento delle quali fornirà il segnale necessario a intraprendere in maniera proattiva e tempestiva le azioni di mitigazione necessarie[8]. I KRI, solitamente di tipo quantitativo (non è escluso tuttavia l'utilizzo di metriche tipo qualitativo) rientrano generalmente, ma non obbligatoriamente, nell'ambito dei sistemi di controllo di I livello e vengono quindi identificati, calcolati e monitorati dai *Risk Owner*, con l'eventuale supporto dei *Risk Specialist* (funzioni aziendali di controllo di secondo livello), ovvero dai soggetti che, in qualità di esperti, sono nella posizione migliore per conoscere l'esistenza di eventuali punti di stress all'interno delle singole unità di *business* o nei processi che rispettivamente gestiscono e supervisionano.

Ferma restando la diversa finalità specifica, nella pratica i KPIs e i KRIs dovrebbero sempre essere letti congiuntamente al fine di comprendere meglio le modalità di raggiungimento di un determinato obiettivo *target* o l'eventuale mancato raggiungimento delle *performance* desiderate.

[8] Beasley M.S., Branson B.C., Hancock B.V., Developing Key Risk Indicators to Strengthen Enterprise Risk Management, COSO, 2010.

Alcune delle seguenti ragioni potrebbero complicare il raggiungimento dei vantaggi desiderati:

- difficoltà nell'identificare i KRI per tutti i rischi individuati;
- scarso collegamento con le cause dei rischi;
- mancata automazione della fase di calcolo dei KRI;
- mancata sinergia tra i KRIs individuati e i KPIs esistenti;
- mancata individuazione delle relative soglie di tolleranza.

Ciò premesso, il percorso decisionale strategico inizierà con l'analisi del contesto di riferimento, inteso come l'insieme dei trend, delle relazioni e di qualsiasi altro fattore in grado di influenzare l'esecuzione della strategia aziendale e quindi il raggiungimento degli obiettivi di *business*, il quale dovrà essere correttamente osservato e compreso sia con riguardo a tutti gli *stakeholder*s esterni (tra i quali organi di vigilanza, investitori, clienti, fornitori, comunità etc.) sia nella sua componente interna ovvero con riferimento al modello organizzativo e operativo dell'azienda (dimensione/distribuzione, divisioni, unità operative, funzioni etc.).

Il *Risk management* si pone come l'elemento di raccordo tra il management e il *Board* per la valutazione critica delle strategie di evoluzione e sviluppo aziendale. In particolare, tra gli obiettivi della funzione dovrebbe esservi anche quello di assicurare che i principali rischi (*top risks*) cui la società è esposta siano adeguatamente identificati, compresi e gestiti dai *risk owner* (funzioni operative) e adeguatamente riportati ai membri degli organi di governo societario; il *risk management* dovrebbe poi valutare l'adeguatezza delle politiche di governo e mitigazione dei rischi, supportando una efficace implementazione della *risk strategy* in modo che gli obiettivi aziendali siano raggiunti nel rispetto del *Risk Appetite* pre-definito.

Ne deriva che il *Risk management* assume un ruolo chiave nel corso del processo decisionale-strategico, con responsabilità di coordinamento diretto e di collaborazione con le varie funzioni aziendali coinvolte nella gestione dei rischi.

In particolare, la funzione sarà chiamata a**:**

1. **contribuire all'analisi delle variabili** che influenzano la strategia nel medio e lungo termine;
2. **supportare la scelta della strategia** grazie allo svolgimento di attività di *risk assessment* e scenario analysis in grado di mostrare chiaramente i fattori in grado di incidere sul rapporto rischio-rendimento atteso;
3. **supportare la successiva attuazione dell'alternativa prescelta** facilitando la declinazione della stessa in specifici obiettivi di *business* e garantendo l'identificazione di momenti di verifica e controllo degli stessi all'interno dell'organizzazione;
4. **monitorarne l'esecuzione** grazie ad attività di *risk assessment* "*on a going concern*".

Iniziando dal primo aspetto, la funzione di *Risk management* dovrebbe supportare l'individuazione delle alternative strategiche percorribili nel lungo periodo. Essa inoltre contribuisce all'interpretazione e alla lettura dei mega trend, concentrandosi su quelli potenzialmente in grado di incidere sul *business* aziendale (e.g. variabili macroeconomiche, sociali e tecnologiche) e di influenzare l'evoluzione di lungo termine della domanda e dell'offerta di beni e servizi, soprattutto in termini di quantità, qualità, prezzi e localizzazione. In particolare, la lettura delle opportunità, connesse all'evoluzione del contesto esterno alla luce della mission e dei *core values* aziendali, guiderà l'organizzazione nella definizione delle direttrici di sviluppo e del rispettivo posizionamento di lungo termine, tenendo conto sia delle risorse (finanziarie e non) di cui l'azienda deve disporre per lo sviluppo dell'iniziativa strategica, sia dell'incertezza che caratterizza le assunzioni di scenario**,** avendo riguardo a quelle con maggiore impatto sui fattori chiave di successo. Nell'ambito di questa analisi potrebbero emergere e dovranno essere tenuti in debito conto sia aspetti di interesse globale (e.g. temi legati al cambiamento climatico oppure al processo di digitalizzazione) sia aspetti che assumono rilevanza specifica per le direttrici di sviluppo

ipotizzate dall'azienda (e.g. potenziale ingresso in specifiche aree geografiche, nuovi settori di *business*, etc.).

Con riferimento alla definizione dei piani strategici di medio termine, è utile svolgere un processo sostanzialmente analogo, ma su ambiti di analisi maggiormente focalizzati sulla specifica realtà aziendale; per il contesto esterno, le analisi potrebbero essere rivolte ai mercati di presenza e/o di prossimo sviluppo, e includere considerazioni sugli scenari dei mercati di approvvigionamento e vendita, sul mercato dei cambi, dei tassi o delle commodity, sul contesto competitivo, sui relativi sviluppi tecnologici, sulle evoluzioni normative e sullo specifico contesto locale e geopolitico. Per il contesto interno, che assume generalmente un maggior peso nelle scelte di medio termine anche in considerazione dei tempi, della complessità e fattibilità di rilevanti cambiamenti strutturali (o rilevanti discontinuità), potrebbero assumere un ruolo decisivo nonché abilitante della strategia, la disponibilità di risorse non solo finanziarie e tecniche ma anche e soprattutto umane.

Infine, ulteriori aspetti da non sottovalutare sono i temi reputazionali legati ai rapporti con gli *stakeholder*s rilevanti; il supporto degli *stakeholder*s chiave (sia interni che esterni) o, al contrario, la loro opposizione, può incidere su tempi, costi e modalità di realizzazione di una o più iniziative nonché talvolta sull'effettivo raggiungimento dei *target* stessi. A questo riguardo, le aspettative e la percezione degli *stakeholder*s devono essere puntualmente analizzate e monitorate per coglierne i disallineamenti, valutarne gli impatti e definire le eventuali azioni di risposta necessarie (ad esempio attraverso la predisposizione di opportune strategie di comunicazione o tavoli di discussione e/o condivisione). Tenendo conto di tutti gli aspetti sopracitati nonché delle minori capacità di adattamento che possono essere espresse nel breve e medio periodo, è importante quindi riuscire ad anticipare il più possibile i cambiamenti e, specialmente in contesti caratterizzati da elevata volatilità, assicurare la capacità di assorbire eventuali fasi negative del ciclo economico.

Una volta definite le strategie attuabili, il *Risk management* dovrà farsi promotore di una attività *di risk assessment* al fine di individuare i rischi e le opportunità legati a ciascuna alternativa strategica. Questo tipo di attività ha, in estrema sintesi, lo scopo di valutare le alternative in gioco, con due principali prospettive:

1. **Risk OF the Strategy,** ovvero il rischio che la strategia sia disallineata rispetto alla mission e ai *core values*;
2. **Risk TO the Strategy**, ovvero il rischio che la strategia, pur coerente con la *mission* e i *core values* aziendali, possa non essere attuata nei tempi e nei modi previsti per raggiungere i principali *target*.

Mentre la valutazione del *Risk OF the Strategy* è importante al fine di non andare a compromettere la visione degli *stakeholder* circa il valore e la reputazione dell'azienda, le valutazioni afferenti al *Risk To the Strategy* ovvero alle implicazioni di ciascuna alternativa saranno fondamentali per l'individuazione dei principali rischi e opportunità.

Questo aspetto viene valutato andando a considerare per ogni alternativa strategica i seguenti elementi:

I. il *trade off* rischio-rendimento, al fine di esprimere un giudizio sul profilo di rischio complessivo e sulla coerenza dell'alternativa strategica con il *risk appetite* e la *risk capacity*;

II. le assunzioni alla base dell'alternativa strategica e dei relativi piani nonché il loro grado di incertezza.

Soltanto grazie all'individuazione dei fattori di rischio primari e allo sviluppo di scenario analysis e/o *what if analysis* (alle quali è dedicato un approfondimento nel successivo par. 2.5), se non anche alla quantificazione di *Key Risk Indicators* basati su approcci probabilistici o stocastici (si veda successivo par. 2.4 per la definizione di KPIs e KRIs), gli organi di governo societario saranno messi in condizione di procedere, in modo consapevole, ad effettuare la scelta tra le varie opzioni strategiche.

Il terzo aspetto è rappresentato dalla necessità di tradurre operativamente in obiettivi di *business* la strategia prescelta, declinando gli stessi in sub-obiettivi specifici per le funzioni coinvolte nella realizzazione dell'iniziativa strategica. Gli obiettivi possono essere declinati a cascata lungo la struttura organizzativa, generalmente con un approccio *top-down* e con un grado di dettaglio crescente (dalle divisioni o funzioni alle singole unità di *business*), oppure selezionati e assegnati *ad hoc* (ad esempio

per specifici prodotti o servizi). Inoltre, siano essi di tipo quantitativo o qualitativo, strettamente finanziari (ad esempio obiettivi legati alle disponibilità liquide) o non finanziari (ad esempio legati a tematiche *Environmental Social and Governance* – ESG), gli obiettivi dovranno essere chiari e misurabili in termini di scostamenti rispetto ai risultati attesi, perseguibili e allineati alla strategia prescelta quindi ai valori e alla mission aziendale.

Una volta assegnati gli obiettivi, ogni dipartimento/divisione/*business unit* sarà responsabile di individuare i principali rischi sottesi; a questo riguardo si potranno osservare: la presenza di più rischi impattanti uno specifico obiettivo; diversi obiettivi sottoposti al medesimo rischio; la possibile presenza di interdipendenze tra rischi e obiettivi di dipartimenti/divisioni/*business unit* differenti. Un esercizio utile, ai fini di una visione integrata nella logica di portafoglio ("*Portfolio View*"), potrebbe essere quello di raggruppare gli obiettivi in categorie coerenti ad esempio con gli aspetti strategici definiti ovvero seguendo la struttura organizzativa e le aree di *business* aziendali. La costruzione di una mappa dei rischi faciliterà la loro successiva riaggregazione così da apprezzare il rischio complessivo a livello aziendale, verificare l'effettivo rispetto del *Risk Appetite Framework* nonché determinare quali siano gli obiettivi che hanno il più alto rischio di non essere raggiunti con il relativo potenziale effetto sulla *performance* complessiva dell'azienda.

Infine, è fondamentale il monitoraggio *"on a going concern*", necessario al fine di verificare in tempo reale l'effettivo raggiungimento dei *performance target* e quindi dei rispettivi obiettivi di *business* all'interno dei limiti di rischio prefissati. Tale monitoraggio può essere effettuato mediante l'utilizzo di *dashboard* che vadano ad includere i principali KPIs e KRIs di riferimento per la divisione/dipartimento/*business unit* e la creazione di una adeguato processo di reporting interno nonché prevedendo meccanismi di *escalation*. Tale monitoraggio dovrà essere svolto periodicamente almeno con cadenza trimestrale e/o on demand.

Anche il processo di predisposizione dell'aggiornamento del piano strategico vedrà coinvolta la funzione *Risk management* che supporterà il resto del *top management* nella selezione delle opzioni per il nuovo piano, valutandone l'adeguatezza in termini di profilo di rischio ed innescando in questo modo un circolo virtuoso di approvazione che si concluderà con la nuova proposta per il *Board*. È conseguentemente buona norma che al nuovo piano si accompagni anche l'aggiornamento del RAF, che al piano dovrà sempre mantenersi collegato e che, contestualmente alla sua approvazione, dovrà recepire gli eventuali adeguamenti.

Si sottolinea in ultimo come, in una organizzazione ottimale, il processo di aggiornamento del piano e delle metriche di rischio a questo collegate, dovrebbe svolgersi in via anticipata rispetto all'esercizio e al periodo a cui il medesimo si riferisce.

In conclusione, la funzione di *Risk management* può, grazie alla propria *expertise* e all'approccio proattivo che la contraddistingue, agire lungo il processo decisionale strategico facendo emergere i rischi latenti e/o legati ad anticipazioni di *macro-trend*, creando così consapevolezza e cultura del rischio nel momento dell'effettuazione della scelta strategica; inoltre, tramite gli strumenti a disposizione ovvero mediante un *risk assessment* strategico, essa può facilitare le adeguate valutazioni in termini di profilo di rischio assunto, supportando l'identificazione dei principali rischi sottesi agli obiettivi di *business* e producendo una corretta ed efficace informativa ai vertici aziendali. Infine, grazie a un monitoraggio costante dell'andamento dei rischi identificati, la funzione può stimolare la verifica del raggiungimento dei *target* di *performance* prefissati, promuovendo, se necessario, eventuali strategie di mitigazione.

2.3 Classificazione dei Rischi

L'esposizione ai rischi di una Corporate è fortemente influenzata da una molteplicità di fattori, in particolare è correlata al modello di *business*, organizzativo, operativo, distributivo, alla complessità dimensionale, al grado di innovazione dei prodotti e servizi, all'attività finanziaria, ai vincoli regolatori cui è soggetta e ad ulteriori elementi peculiari e caratteristici della stessa.

Il rischio, inteso come la possibilità di accadimento di eventi che possono impattare il raggiungimento della strategia e degli obiettivi di *business*, può essere ulteriormente scomposto nelle relative determinanti, secondo una classificazione che tenga conto dei seguenti criteri:

1. non esistendo una mappa dei rischi "*one fits all*" universalmente valida, è auspicabile che ogni impresa identifichi e declini le classi di rischio - e le relative definizioni - in coerenza con gli elementi sopra identificati;
2. i rischi devono essere connessi ai fattori di origine interna o esterna che possono impattare sul piano strategico e comprometterne l'esecuzione;
3. nella declinazione dei rischi è opportuno evitare ridondanze di classificazione (che potrebbero indurre ad un "double counting" dei rischi e dei relativi impatti in termini di losses o mancati profitti nella fase di valutazione o misurazione), pur assicurandone la completezza;
4. la classificazione dovrebbe supportare, con una logica di portafoglio, la valutazione del profilo di rischio dell'organizzazione nella sua interezza, favorendo l'identificazione delle principali tipologie di rischio, considerando l'eventuale interrelazione tra le diverse categorie di rischio (ad esempio, i rischi operativi legati alla produzione e delivery possono far emergere rischi di credito) nonché un chiaro collegamento del possibile impatto di queste sui principali *target* strategici (COSO ERM 2017, Principio 14, "Develops Portfolio View" pag. 84- 85).

Per semplicità si può partire dalle classificazioni tipiche dei principali modelli di ERM, individuando, in prima battuta, le seguenti macrocategorie di rischio:

- **Rischi strategici**, derivanti dalla evoluzione dei fattori sottostanti le principali assunzioni utilizzate per lo sviluppo del piano strategico. In tale ambito possono essere ricompresi i rischi generati dall'evoluzione del contesto macroeconomico e competitivo nonché da altre tematiche geopolitiche o di natura globale e/o sistemica;
- **Rischi finanziari**, derivanti dalla variabilità dei parametri finanziari (tasso di interesse, cambio e *commodity*) e dai prezzi di mercato degli strumenti finanziari e degli *asset* sottostanti;
- **Rischi operativi**, derivanti dall'inadeguatezza o dalla disfunzione di procedure, risorse umane e sistemi interni, oppure da altri eventi esogeni, come pure quelli che posso portare ad una interruzione dei processi produttivi o di distribuzione;
- **Rischi Digital, ICT, *Cyber***, derivanti dalla evoluzione digitale del *business* e del contesto competitivo, dall'adozione delle relative tecnologie e infrastrutture, dalla necessità di garantire adeguati presidi su *Cybersecurity*, *third-party risk*, *data privacy* etc.;
- **Rischi di *compliance* e *Legal***, derivanti dalle normative esterne e interne applicabili all'attività di impresa, incluse le normative a carattere volontario (es. standard ISO), nonché da cambiamenti dell'impianto regolatorio;

- **Rischi ESG**, derivanti da tematiche ambientali, sociali e di *governance*: il continuo incremento del livello di trasparenza e di *accountability* richiesto dal mercato pone alle aziende la sfida di una sempre maggiore integrazione dei temi ESG nei propri processi decisionali strategici; è spesso conseguenza di questo aspetto un allungamento della prospettiva di piano che tenga conto delle capacità di *value creation* non solo per gli *shareholder* ma anche per tutti gli *stakeholder* aziendali;
- **Rischi Reputazionali**, derivanti dalla percezione dell'immagine dell'impresa da parte dei suoi principali *stakeholders* quali clienti, controparti, azionisti, investitori o autorità di vigilanza etc. Spesso i rischi reputazionali possono essere considerati come derivanti da rischi appartenenti alle altre categorie di rischio sopra menzionate e spesso possono sorgere in contesti esterni al perimetro aziendale (e.g. *social network*).

Una diversa classificazione dei rischi può alternativamente considerare non la natura del rischio stesso bensì il suo impatto, distinguendo così tra rischi Strategici (ovvero con un impatto sugli obiettivi di Piano) e rischi Operativi (con un impatto sui processi e sulla *performance* aziendale).

La peculiarità del modello di governance, organizzativo, di business ed operativo rende opportuno che la classificazione dei rischi per le imprese non finanziarie, pur seguendo regole generali, non sia standardizzata.

Ad esempio, rispetto agli intermediari vigilati, in cui la fattispecie "*compliance*" (e le rispettive sanzioni) sono spesso ricondotte ad eventi di rischi operativi, nel caso delle imprese non finanziarie tale classe di rischio può avere una valenza autonoma qualora specifiche linee di business siano soggette a regolamentazione *ad hoc* per la quale sia i presidi organizzativi sia gli impatti e le probabilità di rischio siano valutabili indipendentemente dagli altri, garantendone un governo specifico.

Analogamente per molte imprese non finanziarie i rischi ESG possono essere strettamente riconducibili a rischi strategici (si pensi a titolo esemplificativo ad imprese operanti nel settore dell'energia, utilities, imprese che offrono servizi e prodotti direttamente riconducibili a fattori ESG), laddove per gli intermediari vigilati questi sono invece spesso considerati nell'ambito di rischi "core", come il rischio di mercato e di credito.

Ad ogni modo, una tassonomia più articolata, ispirata agli Accordi di Basilea per gli intermediari vigilati, ma comunque potenzialmente applicabile anche al mondo delle corporate, è fornita in Appendice come ulteriore spunto di riflessione.

2.4 Rischi misurabili quantitativamente versus qualitativamente

Nel mondo del *risk management* un tema spesso affrontato è inerente alla misurabilità dei rischi. In genere ci si riferisce ai rischi misurabili quando è possibile – con un buon livello di confidenza – elaborare misure quantitative di probabilità ed impatto associate a fattori di rischio chiaramente individuabili. Per rischi non misurabili si intendono invece le categorie di rischio per le quali non sono applicabili modelli per la determinazione di probabilità ed impatto in termini numerici, ad esempio attraverso l'utilizzo di *Key Risk Indicator*[9]. Tali rischi, vengono solitamente valutati sulla base di scale qualitative (e.g. alto, medio, basso) e mediante *expert judgement*.

Quanto sopra, soprattutto nel caso di approcci evoluti di governo del rischio, potrebbe essere supportato da considerazioni, proprie di ciascuna corporate, su ***disponibilità***, ***applicabilità*** e ***significatività*** di modelli quantitativi per la misurazione dei rischi che l'impresa ha riconosciuto come rilevanti in relazione al proprio *business model* e alle caratteristiche organizzative e operative.

Con disponibilità si fa riferimento all'esistenza di modelli o metodologie matematici, statistici o probabilistici atti a rappresentare probabilità e impatto dei rischi (differentemente da *Key Performance Indicator*); con applicabilità si intende la possibilità effettiva, a fronte dell'esistenza dei modelli o delle metodologie suddette, di elaborare - a partire da dati di input e attraverso la calibrazione di idonei parametri di modello - misure quantitative attraverso la metodologia o il modello definiti; con significatività ci si riferisce all'aderenza dei risultati dell'applicazione di modelli o metodologie alla realtà, comprovata da test statistici o analisi di *backtesting*.

Riferendosi alla **disponibilità** di modelli di quantificazione si può in linea generale e teorica assumere che per le principali categorie di rischio - ad esempio quelle definite nel paragrafo precedente relativo alla tassonomia dei rischi - modelli quantitativi almeno deterministici, se non stocastico-probabilistici, siano chiaramente identificabili. A titolo esemplificativo si fa riferimento all'esistenza di distribuzioni di probabilità in grado di modellizzare il comportamento del fenomeno di interesse (prezzo di una commodity, variazioni della domanda di un prodotto, perdite per cause legali, etc.), in relazione alla popolazione di riferimento, ovvero alla totalità dei casi di cui lo sperimentatore osserva un dato campione.

Questo criterio generale – ovvero la possibilità di modellizzare in modo attendibile qualsiasi fenomeno – non è declinabile nei concetti di **applicabilità** e **significatività** dei modelli per la quantificazione dei rischi.

Infatti, l'applicabilità di un modello stocastico o probabilistico dipende dalla disponibilità di dati di input e di modellizzazione delle assunzioni attraverso la calibrazione di parametri:

- numerosità delle osservazioni sui fattori di rischio (es. quanti dati di perdita per un dato evento di rischio; quante osservazioni di prezzi per asset sottostanti al rischio, etc.);
- frequenza delle osservazioni disponibili (es. disponibilità di dati annuali / mensili / giornalieri);
- profondità della serie storica disponibile (es. 1 anno, 2 anni …);
- stima dei parametri di modello (es. media, varianza).

Si è fatto prima cenno al concetto di popolazione di riferimento. Nel caso degli eventi rari (tipici di rischi catastrofali) la popolazione di riferimento (ovvero la numerosità, la frequenza e la lunghezza storica delle osservazioni disponibili) spesso costituisce un limite per l'applicazione di modelli matematici, stocastici o probabilistici (o anche semplicemente deterministici) seppur teoricamente esistenti. Semplificando, il modello esisterebbe ma i dati per alimentarlo non sono sufficienti.

[9] I *Key Risk Indicator* si fondano su stime di probabilità e impatto degli eventi in ottica prospettica (probabilità che la perdita sia superiore ad una soglia su un orizzonte temporale e ad un certo livello di confidenza); i *Key Performance Indicator* indicano la manifestazione storica di specifici eventi (quante volte il prezzo è salito di più del 10% rispetto alle stime) che possono avere effetti sulla probabilità di manifestazione degli eventi di rischio o sui relativi impatti.

Ad esempio, spesso le serie storiche dei fattori di rischio o delle perdite possono non essere significative perché non sufficientemente lunghe o perché riferite a periodi in cui il *business* dell'azienda era molto diverso rispetto all'attuale e possono, quindi, portare a risultati non congruenti. Anche i *benchmark* di mercato (e.g. dati consortili) spesso non sono rappresentativi del *business* e quindi del rischio di una specifica azienda.

In tali circostanze si può far ricorso - in tutto o integrando le evidenze quantitative - a valutazioni soggettive (judgemental) del rischio. Il limite è la soggettività della stima degli indicatori di probabilità e impatto (strettamente dipendenti dalla avversione/propensione al rischio del valutatore, oltre che alla conoscenza individuale del fenomeno).

Per ovviare o mitigare la soggettività di valutazione è opportuno individuare informazioni quantitative interne o esterne per supportare la ragionevolezza della stima *judgemental* ovvero per integrare componenti quantitative nella stima. In tale circostanza il *risk management* opera coinvolgendo in via diretta le funzioni di *business*, incentivando l'avvio di un processo di raccolta delle informazioni relative alle possibili evoluzioni dei fattori di rischio e degli impatti economici, finanziari e/o patrimoniali. Il ruolo delle unità di *business* diventa fondamentale anche per valutare la significatività dei risultati ottenuti e la loro coerenza con le assunzioni sottostanti.

A stime esclusivamente *judgemental* si può ricorrere quando il modello è disponibile, la popolazione di riferimento è adeguata ma la veloce ed imprevedibile evoluzione del contesto di riferimento (e quindi dei "comportamenti" della popolazione di riferimento) rendono il modello poco significativo in termini di aderenza alla realtà. Altresì un modello è poco significativo per l'impresa se modellizza ed elabora misure di rischio a basso impatto per la stessa; in casi cioè in cui probabilità ed impatto della manifestazione del rischio non vanno a modificare (se non in modo marginale) i risultati economici, finanziari e patrimoniali, anche nel caso di realizzazione di eventi estremi. Ci si riferisce in tal caso al concetto di **significatività** del modello precedentemente enunciato.

Per rendere maggiormente operativo quanto sopra espresso, seppure un modello probabilistico fosse disponibile in linea teorica, nella sua applicazione potrebbero riscontrarsie problematiche come il reperimento dei dati di input, spesso in carico ai *risk owner*, che dovranno pertanto dotarsi di architetture applicative (procedure, estrattori dei dati dai sistemi sorgente, *data flow* alimentanti il sistema di *risk management*). D'altro canto un modello probabilistico ben alimentato ed elaborato, in condizioni di mercati emergenti, scenari altamente volatili, prezzi negativi potrebbe risultare non "significativo" e pertanto, a fronte di una quantificazione teoricamente e tecnicamente ineccepibile, i risultati del modello non potrebbero idoneamente supportare le scelte operative e strategiche.

Nella determinazione quindi dei rischi da considerare misurabili o meno, nella specifica realtà aziendale, anche al fine di alimentare il *Risk Appetite Framework*, è opportuno verificare da un punto di vista quantitativo se l'evento di rischio considerato sia statisticamente modellizzabile, quali siano i dati di input interni ed esterni per l'alimentazione del modello e per la sua calibrazione. Non di meno sarà necessario verificare se l'implementazione di un'architettura per il calcolo (inclusiva degli estrattori da *source system* per l'alimentazione dei *risk engine* da implementare per l'elaborazione di probabilità e impatti) e di processi per il periodico monitoraggio del rischio possa produrre risultati significativamente validi e stabili nel tempo.

A seguito della definizione di una tassonomia dei rischi di impresa, è quindi fondamentale definire e formalizzare (anche nell'ambito del *Risk Appetite Framework*) gli approcci per la misurazione o valutazione dei rischi individuati al fine di supportare adeguatamente i processi decisionali strategici e di *business* e, conseguentemente, minimizzare ovvero ottimizzare i rischi di impresa, consentendo il posizionamento sulla frontiera efficiente tra rischio e rendimento.

Una valutazione di tipo quantitativo è normalmente auspicabile perché consente di dare una rappresentazione più rigorosa e meno soggettiva del profilo di rischio e dei possibili impatti.

Tuttavia, seppure un modello fosse disponibile ed applicabile, nel caso di bassa significatività, i costi di sviluppo ed implementazione potrebbero non compensare il beneficio atteso dalla quantificazione degli impatti relativi. In tal caso, nel RAF la corrispondente classe di rischio potrà essere individuata come categoria oggetto di controllo, gli eventi saranno mitigati con un sistema di controllo (monitorato attraverso l'applicazione di KPI), ovvero opportuni presidi organizzativi, ma non necessariamente sarà auspicabile l'attivazione di modelli quantitativi (deterministici o stocastici) per la quantificazione di KRI

o degli impatti economici, finanziari o patrimoniali (Earnings, EBIT, Net Income, etc.). Al contrario per rischi significativi (potenzialmente ad alto impatto sui risultati economici, finanziari o sulla capitalizzazione di impresa), in caso di disponibilità di modelli ma di carenza di disponibilità di dati, sarà opportuno in ogni caso attivare metodologie *judgemental* per ottenere almeno una stima del rischio e dei relativi impatti economico, finanziari o patrimoniali.

È quindi fondamentale che, consapevolmente, l'impresa individui i rischi per i quali è opportuno attivare modelli di determinazione di KRI di natura quantitativa se disponibili, applicabili e significativi, ovvero deterministici o *judgemental* in assenza dei presupposti sopra individuati. La formalizzazione delle scelte fatte - anche in forma tabellare semplificata come segue - e l'aggiornamento periodico dei contenuti potrà costituire una parte integrante del RAF.

		MODELLO				
Rischio	**Fattore**	**Disponibilità**	**Applicabilità**	**Significatività**	**Calcolo KRI**	**Impatto economico finanziario**
Rischio A	Domanda	Approccio deterministico (what if)	Approccio judgemental	Contesto volatile	NO	EBIT
Rischio B	Regolatorio	Distribuzione binomiale	Assenza osservazioni	Soggettività	NO	Losses/Profit
Rischio C	Prezzo commodity	Distribuzione normale	Disponibilità dati	Si (test statistici)	PaR	P&L
Rischio D	Currency	Distribuzione normale	Disponibilità dati	Si (test statistici)	VaR	P&L
Rischio E	Sanzioni legali	Distribuzione binomiale	*Da attivare loss data collection*		*To be*	Losses
…	…	…	…	…	…	…

Figura 5 - Esempio di rappresentazione dei driver di misurazione dei rischi

Ciò consentirà la definizione di un *framework* che garantisca la necessaria coerenza tra le scelte metodologiche effettuate, il governo dei rischi aziendali e la visione sinottica per il *Board* e il *Top Management* delle scelte operative effettuate.

2.5 Risk Assessement: simulazioni di rischio atteso e impatti sul piano

Nel corso del processo di sviluppo e/o aggiornamento del piano strategico, il *top management* aziendale coadiuvato dal CRO, una volta individuati i principali rischi e il loro grado di misurabilità e variabilità, dovrebbe sviluppare una serie di scenari simulati che, partendo dal *base case*, permettano di verificare gli impatti dei rischi sul piano, l'efficiente allocazione delle risorse, la realizzabilità degli obiettivi e il rispetto dei limiti di *risk appetite*. In particolare, sarà necessario:

a) individuare le aree di rischio e di opportunità prioritarie e contribuire a mitigare il grado di incertezza dei risultati attesi (con logica *top-down*);

b) focalizzare l'attenzione sui rischi e sulle opportunità che possano compromettere gli obiettivi strategici o intaccare asset critici sia tangibili che intangibili (*value driven*);

c) integrare la valutazione dei rischi nel processo di pianificazione sia di breve sia medio-lungo termine;

d) focalizzare l'attenzione su eventuali elementi di opportunità addizionali rispetto ai *target*;

e) sviluppare per ciascun rischio degli scenari attesi, eventualmente assegnando una distribuzione di probabilità e costruendo una matrice di correlazione tra le varie tipologie di rischio.

Pur sottolineando nuovamente l'impossibilità di individuare un'unica metodologia universalmente applicabile e la necessità di stimolare un approccio quanto più possibile allineato alla grandezza, alla natura e alla complessità dell'azienda, si evidenzia come generalmente gli approcci classici includono misure volte a valutare:

- **Impatto o Severity**: il risultato o l'effetto di un rischio;
- **Probabilità o Likelihood**: la possibilità che si verifichi un rischio (esprimibile mediante approcci quantitativi, qualitativi e/o di frequenza).

$$\mathbf{R} = \mathbf{I} \times \mathbf{P}$$

Il rischio (R), valutato nelle sue dimensioni di probabilità (P) e impatto (I), dovrà essere correttamente analizzato ai fini della verifica dell'effettivo rispetto dei limiti imposti dal *Risk Appetite Framework* aziendale in termini di:

- **Rischio Inerente**: l'ammontare di rischio in assenza di alcuna azione intrapresa dal management diretta e focalizzata ad alterarne la probabilità o la *severity*;
- **Rischio Residuale**: l'ammontare di rischio rimanente in seguito ad eventuali azioni intraprese dal management dirette e focalizzate a mitigarne la probabilità o la *severity*.

In questo contesto risulta chiaro come l'analisi e le simulazioni di impatto sul piano, debbano beneficiare di strumenti di *assessment* il più possibili quantitativi e/o quali-quantitativi sia probabilistici (quali le analisi quantitative integrate) sia non probabilistici (ad esempio le *What if analysis*). Mentre i primi associano una serie di eventi e l'impatto che ne deriva alla loro distribuzione di probabilità, i secondi utilizzano ipotesi soggettive al fine di stimare l'impatto degli eventi su un obiettivo di *business* senza quantificarne la probabilità associata. Entrambi gli approcci possono supportare le strutture e gli attori coinvolti nel processo decisionale strategico (p.e. i comitati manageriali rischi ed eventuali altri comitati endoconsiliari) nella:

- valutazione puntuale del livello *target* di esposizione complessiva ai rischi e/o opportunità nonché calcolo della volatilità massima attesa rispetto ai principali risultati economico-finanziari del gruppo;
- eventuale richiesta di piani di azione e/o indirizzi di "gestione" al fine di mantenere il livello di esposizione entro i limiti "*target*" prefissati (entro un certo livello di confidenza);

- costruzione scenari evolutivi alternativi a quelli considerati nella definizione del piano annuale e/o industriale al fine di valutare la "robustezza" delle assumption ed i possibili impatti sui risultati attesi;
- stima complessiva dei potenziali impatti derivanti da uno shock esogeno (e.g. macroeconomico, *country risk*, regolatorio, *climate change* etc.) su ipotesi originali di piano strategico.

L'orizzonte temporale da considerare durante la fase di *assessment* dovrà essere il medesimo utilizzato in fase di pianificazione strategica e di declinazione degli obiettivi strategici di *business*, senza tuttavia perdere di vista l'orizzonte di più lungo termine sul quale eventuali rischi emergenti potrebbero impattare significativamente, andando a compromettere il perseguimento della mission aziendale. Inoltre, l'elemento temporale è un parametro importante anche nella scelta del modello, poiché può incidere in maniera significativa sulla capacità di stima dell'accadimento di un rischio in relazione alle ipotesi strategiche di piano; per valutare la volatilità intrinseca negli scenari di piano di breve e medio periodo possono essere utilizzati modelli di tipo *target@risk*, mentre, per analisi che abbracciano anche il lungo periodo, possono essere utilizzati modelli di tipo what-if al fine di poter valutare la resilienza dei target rispetto a una ipotesi di cambiamento strutturale del contesto in cui l'azienda opera.

2.5.1 Analisi quantitative integrate: il Target@Risk

L'elevata volatilità delle principali variabili economico/finanziarie derivante sia dall'evoluzione del *business* di riferimento sia da fattori esogeni (e.g. shock macroeconomico, conflitti, nuovo contesto competitivo etc.), richiede la necessità di valutare gli eventi di rischio e le relative opportunità attraverso tecniche d'inferenza statistica con l'obiettivo di misurare i potenziali impatti per il gruppo verso le ipotesi di piano e le sue variabili *target* (e.g. *Profit* , *Earning*, Ebit, *Cash Flow*, etc.). La tecnica delle simulazioni stocastiche (e.g. simulazione Montecarlo), è quella maggiormente utilizzata a questo scopo perché consente l'aggregazione dei rischi e delle opportunità nonché la rappresentazione della volatilità attesa dei principali *target* economico-finanziari con la possibilità di integrare nelle simulazioni anche la matrice che rappresenta il livello di correlazione tra i differenti rischi analizzati. La metodologia proposta si articola in fasi:

I. prima identificazione degli eventi di rischio e delle opportunità verso i *target* di piano attraverso l'utilizzo di *self-assessment*;
II. interlocuzione con *risk owner* per la valutazione più approfondita delle principali opportunità e rischi evidenziati e per comprenderne la correlazione e l'impatto;
III. sviluppo del modello simulativo e dei suoi parametri di *input* e ottimizzazione della numerosità dei percorsi simulati per garantire la stabilità dei risultati;
IV. lancio delle simulazioni e valutazione dei risultati e della significatività degli errori attesi.

L'analisi dei rischi e delle opportunità, alla base delle suddette simulazioni, dovrebbe essere eseguita periodicamente nel corso dell'anno con un processo che, come detto, dovrebbe essere guidato e declinato tenendo anche conto del modello organizzativo aziendale e con un adeguato coinvolgimento dei *risk owner* che avranno il compito di facilitare l'individuazione di tutti gli elementi di rischio e di opportunità che potrebbero andare ad impattare i *target* aziendali (*self-assessment*).

Ad ogni evento di rischio/opportunità viene associata una distribuzione di probabilità, attribuita sulla base della natura dell'evento, previa approvazione del responsabile del dato[10] e, ove possibile, viene sviluppata una matrice di correlazione dei vari rischi. Gli eventi di rischio e di opportunità vengono così simulati in maniera casuale (cercando di ottimizzare la numerosità dei percorsi) tenendo conto delle distribuzioni di probabilità di manifestazione dell'evento e dei possibili scenari d'impatto che si vuole

[10] Permane quindi un elemento qualitativo anche all'interno del modello proposto dato dal giudizio del business rispetto alla probabilità di accadimento del rischio\opportunità. Ove possibile, tale elemento qualitativo deve essere supportato\guidato da un'analisi storica.

simulare: base (caso più probabile), *best*, *worst*. Il *target@risk* che emerge dalla simulazione stocastica è definito come il valore atteso della variabile tenuto conto dei possibili impatti dei rischi e delle opportunità. La possibilità di poter modellizzare in maniera sempre più accurata il *business model* grazie alla possibilità di incorporare correlazioni tra eventi sia in termini di probabilità di accadimento sia in termini di scenario d'impatto - trasforma il sistema di *target@risk* in uno strumento strategico, oltre che di *governance* dei rischi, offrendo una maggiore accuratezza nella definizione dei target rispetto al classico approccio deterministico adottato nella definizione delle forecast da parte del controllo di gestione.

2.5.2 What If Analysis

Questa seconda tecnica risulta utile alla luce di un contesto esterno caratterizzato da una sempre maggiore dinamicità, volatilità e interconnessione dei fenomeni, in cui è fondamentale supportare i comitati manageriali rischi e i comitati endoconsiliari:

I. nella comprensione degli impatti associati a potenziali shock (esogeni) che comportino un cambio significativo al contesto in cui l'impresa opera,

II. nell'analisi delle possibili azioni di risposta e, infine,

III. nella valutazione del livello di resilienza dei *target* (sia *soft* sia *hard*).

Le *What If analysis* approfondiscono tutti gli aspetti sopra indicati, a partire dal disegno di un "potenziale shock" e dalla messa a punto di ipotesi di stress che possono riguardare sia una **sola variabile** di contesto particolarmente rilevante per il *business* (ad es. il prezzo di una *commodity*) sia uno scenario più articolato (es. l'evoluzione di un contesto paese).

Pur concentrandosi spesso sullo studio di *scenari worst* utili per testare il livello di resilienza dell'impresa, tuttavia può risultare talvolta utile sviluppare tali metodologie a partire da *scenari best* in modo da valutare la *readiness* dell'azienda a cogliere opportunità nonché adeguare velocemente ed efficacemente le proprie azioni.

In entrambi i casi l'analisi delle correlazioni e dei legami tra i potenziali eventi (rischi e opportunità) è uno *step* fondamentale al fine di costruire una visione integrata e completa degli impatti derivanti dal potenziale shock.

Nel primo caso avrà l'obiettivo di cogliere e integrare tutti gli impatti di natura economica, finanziaria, operativa e produttiva, nonché valutare l'effetto complessivo sui corrispondenti *target* di piano prima e dopo le possibili azioni di risposta dell'impresa; nel secondo l'annalisi avrà l'obiettivo di mettere a fuoco la natura degli impatti (misurarne la severità con metriche "*qualitative*" opportunamente calibrate e approfondendone le modalità di gestione in termini di contenuto, tempi, costi.

APPENDICE

A - La tassonomia dei rischi

Risk Category View		Risk View
Rischi Reputazionali	Rischi Strategici	Evoluzione contesto macroeconomico
		Evoluzione contesto competitivo
		Rischi legati al Business Plan (linee di business, mercati di vendita e approvvigionamento, innovazione tecnologica, canali, etc.)
		Rischio Geopolitico
		Rischio Paese
		Altri Rischi Globali e sistemici
	Rischi di Finanziari	Rischio di cambio
		Rischio azionario
		Rischio di tasso di interesse
		Rischio di liquidità
		Rischio di commodity
		Rischio di credito/controparte
	Rischi Operativi	Rischio frode fisica interna e altri eventi esterni (es. sicurezza fisica impianto, sabotaggio, furti)
		Rischio produzione e delivery prodotto/servizio (es. impattanti qualità, tempi, costi)
		Rischio interruzione attività e processi produttivi
		Rischio risorse umane (es. impattanti il recruiting, lo sviluppo, e il retain)
	Rischi Digital, ICT, Cyber	Rischio cybersicurezza (es. sistema pagamenti, sistema informativo)
		Rischio informatico (es. obsolescenza asset informatici)
		Rischio interruzione servizi
	Rischi di Compliance & Legal	Rischio violazione norme imperative (231/2001, Antitrust, Privacy, conformità prodotto, giuslavoristici)
		Rischio violazione norme volontarie (es. standard ISO)
		Rischio compliance informativa contabile/di bilancio/fiscale
		Rischio regolatorio
	Rischi ESG	Rischio ambientale interno (pollution, waste)
		Rischio ambientale esterno (climate, natural resources, raw material)
		Rischi sociali (human rights, HSE, Supply chain labor standard)
		Rischi di governance (es. corporate behavour, ethics, corruption)

Figura 6 - Esempio di tassonomia dei rischi

B - La tassonomia dei rischi elaborata sulla base degli Accordi di Basilea

Rielaborando la normativa bancaria definita dagli Accordi di Basilea 2 e 3, i rischi possono essere classificati anche nelle seguenti macrocategorie:

- **Rischi di mercato**, generati dalla variabilità dei parametri finanziari e dai prezzi di mercato degli strumenti finanziari e degli asset sottostanti;
- **Rischi di credito e di controparte**, generati dal mancato adempimento di obbligazioni contrattuali di terze parti nei confronti dell'impresa (controparti in transazioni finanziarie, in attività commerciali, in operatività nei mercati finanziari o su *commodity*, fornitori e partner per progetti d'investimento e attività di *business*, etc.);
- **Rischi operativi**, generati dall'inadeguatezza o dalla disfunzione di procedure, risorse umane e sistemi interni, oppure da eventi esogeni;
- **Rischi globali** o sistemici, generati dalla variabilità di fattori di rischio interconnessi a livello globale quali il rischio Paese, il rischio regolatorio, il climate change, etc.;
- **Altri rischi**, quali i rischi reputazionali, strategici, rischio di modello, rischio di *compliance*, *cyber risk*, etc.

Articolando le categorie citate, si possono individuare le seguenti tipologie di rischio:

RISCHI DI MERCATO

Tra le principali classi di rischio riconducibili ai rischi di mercato troviamo:

- il rischio di cambio, generato dalla volatilità dei tassi di cambio rispetto alla valuta di riferimento (per esempio l'euro per le imprese europee);
- il rischio azionario (anche rischio *equity*), generato dalla variabilità dei prezzi dei titoli azionari;
- il rischio di tasso d'interesse, generato dalla variazione dei tassi di mercato (e quindi del costo delle risorse finanziarie e del rendimento degli investimenti finanziari);
- il rischio di liquidità, generato dalla capacità dell'impresa di far fronte agli impegni di pagamento assunti in relazione alle proprie disponibilità liquide o finanziarie di breve termine;
- il rischio commodity, generato dalla variabilità del costo di negoziazione delle materie prime.

RISCHI DI CREDITO O CONTROPARTE

Tra le principali classi di rischio riconducibili ai rischi di credito o controparte troviamo:

- rischio di *default*, in caso d'inadempimento della controparte a causa della propria insolvenza;
- rischio di *delivery*, che sussiste qualora le controparti abbiano reciproci e contestuali obblighi di consegna o pagamento ed una delle due parti risulti insolvente;
- rischio di sostituzione, presente nei contratti a termine con prestazioni corrispettive e consistente nel maggior costo o nel mancato guadagno che la parte solvente sopporta qualora la controparte non adempia alle proprie obbligazioni;
- rischio di *spread*, dovuto alla variazione di valore di attivi creditizi dovuti al deterioramento del merito creditizio della controparte;
- rischio di concentrazione, derivante da esposizioni verso controparti, gruppi di controparti connesse e controparti del medesimo settore economico o che esercitano la stessa attività (concentrazione settoriale) o appartenenti alla medesima area geografica (concentrazione geografica).

RISCHI OPERATIVI

I rischi operativi sono definiti in ambito bancario (Regolamento 575/2013/UE, Art. 4, "Definizioni" 52) come i rischi derivanti dall'inadeguatezza o dalla disfunzione di procedure, risorse umane e sistemi interni, oppure da eventi esogeni, articolati in relazione a categorie di eventi specifici definiti nel citato Regolamento, Parte III, Titolo III, Art. 324 (Tabella 2).

Tabella 2 - Categorie di eventi dei rischi operativi

Categoria di eventi	Definizione
Frode interna	Perdite dovute ad attività non autorizzata, frode, appropriazione indebita o violazione di leggi, regolamenti o direttive aziendali che coinvolgano almeno una risorsa interna.
Frode esterna	Perdite dovute a frode, appropriazione indebita o violazione di leggi da parte di soggetti esterni.
Rapporto d'impiego e sicurezza sul lavoro	Perdite derivanti da atti non conformi alle leggi o agli accordi in materia d'impiego, salute e sicurezza sul lavoro, dal pagamento di risarcimenti a titolo di lesioni personali o da episodi di discriminazione o di mancata applicazione di condizioni paritarie.
Clientela, prodotti e prassi professionali	Perdite derivanti da inadempienze relative a obblighi professionali verso clienti ovvero dalla natura o dalle caratteristiche del prodotto o del servizio prestato.
Danni da eventi esterni	Perdite derivanti da eventi esterni, quali catastrofi naturali, terrorismo, atti vandalici.
Interruzioni dell'operatività e disfunzioni dei sistemi	Perdite dovute a interruzioni dell'operatività, a disfunzioni o a indisponibilità dei sistemi.
Esecuzione, consegna e gestione dei processi	Perdite dovute a carenze nel perfezionamento delle operazioni o nella gestione dei processi, nonché perdite dovute alle relazioni con controparti commerciali, venditori e fornitori.

RISCHI SISTEMICI

Ai rischi sistemici è possibile ricondurre:

- il rischio Paese connesso – semplificando la definizione di Duncan H. Meldrum (Country Risk and Foreign Direct Investment, 2000) - a fattori economici, di localizzazione geografica (contagio da Paesi vicini), al rischio sovrano (capacità o volontà del debitore sovrano di onorare i propri impegni di pagamento), al rischio politico (eventi di natura non economica derivanti da conflitti, mutamenti istituzionali e atti unilaterali dei governi);
- il rischio *climate change*, generato da cambiamenti climatici globali con impatti sugli *asset* per la produzione di beni o per la fornitura di servizi, in conseguenza alla mancata, errata o ritardata esecuzione di azioni e strategie volte alla mitigazione del rischio;
- alti rischi emergenti, legati a fattori macroeconomici, ambientali o sociali.

ALTRI RISCHI

Tra gli altri rischi si potrebbero menzionare:

- il rischio di leva finanziaria eccessiva, ossia il rischio che un livello di indebitamento particolarmente elevato rispetto alla dotazione di mezzi propri renda la società vulnerabile, rendendo necessaria l'adozione di misure correttive al piano industriale, compresa la vendita di attività con contabilizzazione di perdite che potrebbero comportare esigenze di impairment anche delle restanti attività;
- il rischio strategico, connesso a cambiamenti del contesto operativo, decisioni aziendali errate, attuazione inadeguata di decisioni, scarsa reattività a variazioni del contesto competitivo;

- il rischio reputazionale, derivanti dalla percezione dell'immagine dell'impresa da parte dei suoi principali *stakeholder*s quali clienti, controparti, azionisti, investitori o autorità di vigilanza etc. Spesso i rischi reputazionali possono essere interpretati come rischi "trasversali" ovvero che si manifestano come conseguenza del verificarsi di altre tipologie di rischio;
- il rischio di *compliance*, derivante dalle normative esterne e interne applicabili all'attività di impresa, incluse le normative a carattere volontario (es. standard ISO) nonché da cambiamenti dell'impianto regolatorio;
- rischi connessi a reati oggetto di responsabilità amministrativa, ex d.lgs. 231/01;
- il *cyber risk* e più in generale il rischio informatico, generato da eventi non pianificati che interessano le risorse informatiche con impatti negativi sull'integrità, la disponibilità, la riservatezza, l'autenticità e/o la continuità dei servizi o dei processi dell'organizzazione nonché la violazione o l'imminente minaccia di violazione delle norme e delle prassi aziendali in materia di sicurezza delle informazioni (Circolare n. 285, Titolo IV, Capitolo 4, Sezione I, 3, Banca di Italia);
- il rischio di modello, inteso come la perdita potenziale a seguito di decisioni basate sui risultati di modelli interni, a causa di errori nello sviluppo, nell'attuazione o nell'utilizzo degli stessi (Direttiva 2013/36/UE, Art. 3).

RIFERIMENTI BIBLIOGRAFICI CITATI

- Associazione Italiana Internal Auditors (2016), *La cultura del rischio.*
- Beasley M.S., Branson B.C., Hancock B.V (COSO) (2010), *Developing Key Risk Indicators to Strengthen Enterprise Risk Management*.
- Cineas – Mediobanca (2020), *Osservatorio sul Risk Management nelle Medie imprese manufatturiere italiane.*
- Comitato per la Corporate Governance (2020), *Codice di Corporate Governance*.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2017), *Enterprise Risk Management—Integrating with Strategy and Performance*.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2012), *Understanding and Communicating Risk Appetite*.
- Duncan H. Meldrum (2000), *Country Risk and Foreign Direct Investment.*
- Financial Stability Board (2014), *Guidance on Supervisory Interaction with Financial Institutions on Risk Culture: A framework for assessing Risk Culture.*
- Financial Stability Board (2013), *Principles for An Effective Risk Appetite Framework.*
- Financial Stability Board (2013), *Thematic Review on Risk Governance.*
- Florio C., Leoni G. (2016), "Enterprise risk management and firm performance: The Italian case", in *The British Accounting Review* ,49 (1), pp 56 – 74.
- Institute International of Finance (2009), *Riforma nel settore dei servizi finanziari: rafforzare le pratiche per un sistema più stabile.*
- International Organization for Standardization (2018), *ISO 31000:2018 Risk Management - Guidelines*.
- Lechner P., Gatzert N. (2017), "Determinants and value of enterprise risk management: empirical evidence from Germany", in *European Journal of Finance,* 24 (2), pp. 1 – 27.
- NED Community (2013), *Amministratori e componenti del Comitato controllo e rischi: Come valutare la governance in tema di rischi e controlli.*
- OECD (2015)*, G20/OECD Principles of Corporate Governance, OECD Publishing, Paris. http://dx.doi.org/10.1787/9789264236882-en*.
- Risk Management Association e Protiviti (2014), *Strengthening Your Risk Culture.*

INDICE DELLE FIGURE

INDICE DELLE TABELLE

GLOSSARIO[11]

Azienda Corporate: Impresa non finanziaria

Contesto (di business): Le tendenze, gli eventi, le relazioni e tutti gli altri fattori che possono influenzare, chiarire o cambiare la strategia e gli obiettivi di *business* correnti e futuri dell'azienda.

Cultura del rischio: L'insieme di valori comuni, comportamenti e attitudini di singoli individui, sottogruppi e gruppi all'interno di un'organizzazione che determinano come i componenti dell'organizzazione stessa identificano, valutano, discutono e gestiscono i rischi.

Enterprise Risk Management: La cultura, le capacità e le prassi integrate con l'impostazione della strategia e nell'operatività dell'impresa, su cui le organizzazioni fanno affidamento per gestire il rischio nella creazione, conservazione e realizzazione del valore.

Evento: Un accadimento occorso o potenziale.

Impatto (o Severity): Il risultato o l'effetto di un rischio.

Key Performance Indicators: Indicatori di *performance*, progettati e selezionati al fine di fornire una panoramica circa le prestazioni raggiunte dall'organizzazione nonché dalle sue principali funzioni e/o unità di *business* in un determinato intervallo temporale.

Key Risk Indicators: Indicatori di tipo predittivo, focalizzati sull'analisi delle cause che potrebbero generare il rischio, individuati con l'obiettivo di fornire una percezione dell'ammontare del profilo di rischio in essere ovvero cogliere in anticipo l'eventuale possibilità di un mancato raggiungimento dei *performance target* prefissati.

Mission: Descrive lo scopo fondamentale dell'azienda, la motivazione che ha portato alla costituzione della stessa.

Obiettivi di business: Qualsiasi *step* misurabile che l'azienda fissa al fine di perseguire la propria strategia.

Probabilità: La possibilità che si verifichi un determinato evento.

Rischio: L'Evento il cui verificarsi influenzerebbe il raggiungimento della strategia e degli obiettivi di *business*.

Risk Appetite: La tipologia e la quantità di rischio, a livello generale, che un'azienda è disposta ad accettare nel perseguimento del valore.

Risk Appetite Framework (RAF): Approccio e/o processo valido al fine di determinare la propensione al rischio desiderata, in termini di entità e tipologie di rischio che l'impresa è disposta ad assumere rispetto alla propria capacità massima di assunzione dei rischi e in coerenza con le soglie di tolleranza e i limiti stabiliti, nel perseguire i propri obiettivi di *business*.

Risk Appetite Statement: Dichiarazione formale del livello aggregato e dei tipi di rischio che un'azienda è disposta ad accettare, o ad evitare, per raggiungere i propri obiettivi strategici.

Risk Capacity: La massima quantità di rischio che un'azienda è in grado di assorbire nel perseguimento della strategia e degli obiettivi di *business*.

Rischio Inerente: L'ammontare di rischio in assenza di alcuna azione intrapresa dal *management* diretta e focalizzata ad alterarne la probabilità o la *severity*.

Risk Limit: Soglie di rischio che, in coerenza con gli obiettivi aggregati di *risk appetite*, devono essere assegnati come obiettivo/vincolo alle singole unità *risk taking* (*business unit* e *legal entities*) per assicurare che esse prendano decisioni coerenti con la propensione al rischio deliberata.

Risk Management (unità/funzione di): Unità o funzione indipendente responsabile dei controlli di secondo livello.

Rischio Residuale: L'ammontare di rischio rimanente in seguito ad eventuali azioni intraprese dal management dirette e focalizzate a mitigarne la probabilità o la *severity*.

[11] Glossario principalmente basato sulle definizioni disponibili nelle pubblicazioni degli standard setters internazionali

Risk Profile: Il livello di rischio assunto dall'impresa a una determinata data (*point in time*) qualificato in termini di KRI e/o di scostamento economico-finanziario dai risultati di *business*.

Risk Tolerance: Deviazione massima dal *risk appetite* che l'azienda ritiene di essere in grado di sopportare senza compromettere il raggiungimento degli obiettivi strategici o addirittura senza incorrere nel rischio di fallimento per perdite, problemi operativi o danni reputazionali.

Stakeholder: Qualsiasi parte abbia un interesse reale o acquisito nell'entità. Gli *stakeholders* interni sono coloro che lavorano all'interno dell'azienda, come dipendenti, direzione e consiglio di amministrazione; gli *stakeholders* esterni sono gli interlocutori che, pur non essendo coinvolti direttamente nell'attività dell'impresa, ne sono a vario titolo interessati, e possono influenzare l'ambiente aziendale o la reputazione, il marchio e la fiducia dell'azienda.

Standard Setters: Società, soggetti pubblici o privati, autorità o enti di regolamentazione o vigilanza che definiscono standard nazionali o internazionali per il governo di tematiche specifiche.

Valori (di fondo): Principi, modi di agire e ideali considerati fondamentali che ispirano il modo di agire dell'azienda e dei suoi dipendenti.

Vision: Esprime una situazione tendenziale e rappresenta l'ideale al quale l'impresa mira, le sue aspirazioni per ciò che intende raggiungere nel tempo.

Vista/logica a/di portafoglio: Una visione integrata del rischio che l'azienda deve fronteggiare, che mette in condizione il *management* e il consiglio di amministrazione di considerare la tipologia, la gravità e le correlazioni dei rischi e come questi possono influenzare la *performance* dell'azienda relativamente alla sua strategia e agli obiettivi di *business*.