



nr. 18 - Gennaio 2016

**L'ESERCIZIO DEL *RISK OVERSIGHT*
DA PARTE DEL CONSIGLIO
DI AMMINISTRAZIONE**

Gruppo di Ricerca Governance

ASSIREVI

nr. 18 - Gennaio 2016

**L'ESERCIZIO DEL *RISK OVERSIGHT*
DA PARTE DEL CONSIGLIO
DI AMMINISTRAZIONE**

ASSIREVI

INDICE

INTRODUZIONE	4
<i>EXECUTIVE SUMMARY</i>	6
CAPITOLO I – PANORAMICA SUI PRINCIPALI RIFERIMENTI NORMATIVI E DI <i>LEADING PRACTICE</i> IN MERITO AL RUOLO DEL CONSIGLIO DI AMMINISTRAZIONE SUL SISTEMA DI CONTROLLO INTERNO E DI GESTIONE DEI RISCHI	
1. Considerazioni generali	9
2. La normativa primaria, gli obiettivi ed i rischi dell’impresa	11
3. Il Codice di Autodisciplina del Comitato per la <i>Corporate Governance</i> delle società quotate	13
4. Le più recenti evoluzioni internazionali	15
5. Il gruppo di imprese	19
CAPITOLO II – PRESIDI DI <i>GOVERNANCE</i> E DI CONTROLLO: MODALITÀ DI COORDINAMENTO E FLUSSI INFORMATIVI VERSO IL <i>BOARD</i>	
1. Attori del Sistema di Controllo Interno e Gestione dei Rischi	21
1.1. Il ruolo del <i>Board</i>	22
1.2. Il ruolo del Collegio Sindacale	24
1.3. Il ruolo dell’ <i>Internal Audit</i> e del suo Responsabile	25
1.4. Il ruolo del Dirigente Preposto alla redazione dei documenti contabili societari	25
1.5. Il ruolo del <i>Chief Risk Officer</i>	26
1.6. Il ruolo del Comitato Controllo e Rischi	27
1.7. Il ruolo dell’Amministratore Incaricato del Sistema di Controllo Interno e Gestione dei Rischi	27
2. L’importanza dei flussi informativi	28
2.1. Assunzioni di fondo e direzione strategica	29
2.2. Individuazione della soglia di tolleranza e dell’appetito al rischio	29
2.3. Aggregazione ed integrazione dei rischi	30
3. Modelli di presidio del rischio	30
4. I ruoli all’interno dei gruppi	32

CAPITOLO III – MODALITÀ DI INTERVENTO DEL CONSIGLIO DI AMMINISTRAZIONE NEL PROCESSO DI *RISK MANAGEMENT*

1.	Modalità di intervento del Consiglio di Amministrazione nel processo di <i>Risk Management</i>	33
1.1.	<i>Risk governance</i>	36
1.2.	<i>Risk strategy & appetite</i>	37
1.3.	<i>Risk assessment & measurement</i>	38
1.4.	<i>Risk management & monitoring</i>	39
1.5.	<i>Risk reporting & insight</i>	40
2.	L'attività di <i>risk management</i> nei gruppi societari	40

CAPITOLO IV - IL RUOLO DEL CONSIGLIO DI AMMINISTRAZIONE NELLE ATTIVITÀ DI MONITORAGGIO (*ON GOING BASIS*) E *REVIEW* (*ANNUAL BASIS*) DEL SISTEMA DI CONTROLLO INTERNO E DI GESTIONE DEI RISCHI

1.	Considerazioni generali	42
2.	L'esercizio di <i>oversight</i> del Consiglio di Amministrazione: il monitoraggio continuo (<i>on going</i>)	46
3.	L'esercizio di <i>oversight</i> del Consiglio di Amministrazione: la <i>review</i> periodica (<i>annual basis</i>)	48

CAPITOLO V – LA RELAZIONE SUL GOVERNO SOCIETARIO E LA VALUTAZIONE DA PARTE DEL CONSIGLIO DI AMMINISTRAZIONE SULL'ADEGUATEZZA DEL SISTEMA DI CONTROLLO INTERNO E DI GESTIONE DEI RISCHI

1.	Gli adempimenti del Consiglio di Amministrazione nella valutazione di adeguatezza del Sistema di Controllo Interno e di Gestione dei Rischi	51
2.	I ruoli, le responsabilità ed i flussi informativi a supporto della valutazione del Consiglio di Amministrazione	53
3.	Il processo di valutazione	55
4.	Valutazione di eventuali carenze e approcci per la valutazione del Sistema di Controllo Interno e di Gestione dei Rischi	56

	BIBLIOGRAFIA	59
--	--------------	----

INTRODUZIONE

Assirevi da tempo si interessa di tematiche relative alla *governance* societaria, con particolare riguardo al sistema di controllo interno e di gestione dei rischi (d'ora in avanti anche SCIGR).

Un sistema di controllo interno e di gestione dei rischi adeguato, infatti, determina, tra gli altri, una maggiore affidabilità complessiva dell'informativa fornita dai responsabili delle attività di *governance* e dalla direzione aziendale al revisore esterno.

Con il presente Quaderno, redatto dai professionisti del Gruppo di Ricerca *Corporate Governance*, Assirevi intende approfondire in modo concreto l'esercizio del *risk oversight*¹ da parte del Consiglio di Amministrazione², tenendo in considerazione l'esperienza pratica e i principali *standard* internazionali.

Le recenti evoluzioni della *corporate governance*, anche a seguito delle analisi effettuate sulle cause della crisi finanziaria di questi ultimi anni, hanno evidenziato come al *Board* spetti un ruolo da protagonista nei processi di gestione dei rischi. Il suo tradizionale ruolo di indirizzo strategico, quindi, non si esaurisce nell'approvazione dei *business plan* e nella definizione degli assetti organizzativi più idonei al loro conseguimento. Il Consiglio è infatti chiamato ad assicurare che i piani strategici contengano un adeguato livello di rischio coerente con la remunerazione attesa del capitale investito e compatibile con la sostenibilità nel medio-lungo periodo e che gli assetti organizzativi siano strutturati per garantire il conseguimento degli obiettivi, considerando anche gli elementi del SCIGR funzionali al mantenimento dei livelli di rischio desiderati (*risk appetite*).

Sulla base di questo assunto, si è assistito in questi anni ad un intenso dibattito nella *business community*, animato da enti regolatori da un lato e da investitori, società e associazioni professionali dall'altro, sulle modalità con cui il *Board* dovesse intervenire nei processi di *risk management*³. È apparso subito evidente che ci si muoveva su un territorio di confine tra il ruolo di indirizzo strategico di competenza del *Board* e quello puramente gestionale che ricade nel campo di azione *management*. Le decisioni operative sui rischi sono prese dal *management* nelle attività *day by day* e sono integrate nei più ampi processi decisionali che attengono la gestione operativa del business e dei rischi correlati.

Alla luce della complessità delle tematiche e della rilevanza dell'argomento, il presente Quaderno si pone l'obiettivo di fornire in maniera organica una panoramica sul ruolo del Consiglio di Amministrazione nel sistema di controllo interno e di gestione dei rischi nonché fornire elementi utili alla comprensione delle modalità operative per lo svolgimento delle attività connesse alla sua funzione di *risk oversight*.

Si tratta di temi molto complessi che si intrecciano in un coacervo di problematiche legali, organizzative e di competitività delle imprese, con tempi di evoluzione e di sviluppo differenziati e che suscitano interrogativi e preoccupazioni, tanto all'interno che all'esterno della comunità imprenditoriale.

¹ Il termine "*risk oversight*" descrive pienamente il ruolo del Consiglio di Amministrazione nel processo di *risk management*; nei "*Principles of Corporate Governance*", emessi dal G20/OECD nel mese di settembre 2015, esso è definito come la supervisione da parte del *Board* dei ruoli e delle responsabilità nel processo di *risk management*, la definizione della tipologia e del livello di rischio che la società è disposta ad assumere per raggiungere i propri obiettivi (propensione al rischio) nonché le modalità con cui i rischi devono essere gestiti.

² *Board* oppure Consiglio di Amministrazione sono utilizzati indifferentemente per identificare gli organi amministrativi sia nel sistema tradizionale, sia in quello monistico o dualistico, per quanto compatibili.

³ Tra i più noti e richiamati all'interno di questo quaderno:

- FRC, *Boards and Risk: A summary of discussions with companies, investors and advisers*, 2011.
- FRC, *Guidance on Board Effectiveness*, 2011.
- NACD, *Advisory Council on Risk Oversight*, 2014.

La trattazione riguarda una panoramica sui principali riferimenti normativi e di *leading practice* sul ruolo del Consiglio di Amministrazione (Capitolo I), i modelli organizzativi di *risk management* e i relativi flussi informativi (Capitolo II), le modalità di intervento del Consiglio di Amministrazione nel processo di *risk management* (Capitolo III), il suo ruolo nelle attività di monitoraggio e *review* del sistema di controllo interno e di gestione dei rischi (Capitolo IV), nonché la valutazione dello stesso da parte del Consiglio di Amministrazione e la conseguente informativa da fornire all'interno della relazione sul governo societario, con focus specifico sulle attività operative relative all'attività di monitoraggio e di reporting (Capitolo V).

Nel testo viene fatto riferimento alle società che operano nei settori industriali e commerciali. Non sono trattate, invece, le società che operano in settori soggetti a discipline speciali, quali ad esempio le istituzioni finanziarie.

Nel Quaderno viene anche fatto riferimento alle norme del Codice Civile e al D.Lgs. 24 febbraio 1998, n. 58 (d'ora in avanti anche Testo Unico della Finanza o TUF), quali fonti normative primarie, con particolare riguardo a quelle relative alle responsabilità e alle attività del Consiglio di Amministrazione e del Collegio Sindacale, nonché alla normativa secondaria e a *standard* di autoregolamentazione quali il Codice di Autodisciplina predisposto dal Comitato per la *Corporate Governance* di Borsa Italiana, il cui ultimo aggiornamento risale a luglio 2015⁴ (d'ora in avanti il Codice di Autodisciplina).

⁴ Eventuali riferimenti ad edizioni precedenti del Codice di Autodisciplina sono espressamente specificati.

EXECUTIVE SUMMARY

Il Quaderno evidenzia che un efficace sistema di controllo interno e di gestione dei rischi deve necessariamente essere inteso come un processo pervasivo che preveda la partecipazione attiva e coordinata di molteplici attori e funzioni, dagli *owner* dei processi e dei rischi fino al *Board* nella sua collegialità.

Il ruolo del *Board* nel processo di *risk management* con compiti che vanno dall'indirizzo strategico nella definizione della propensione al rischio, alle attività di monitoraggio continuo dei principali rischi e dei processi di *risk management*, fino all'informativa periodica al pubblico in merito all'adeguatezza complessiva del sistema di controllo interno e di gestione dei rischi – è andato via via cristallizzandosi nelle nuove versioni dei principali codici di *corporate governance* e nella normativa di riferimento (in particolare per i settori vigilati, quali ad esempio il settore bancario e quello assicurativo) emessi successivamente alla crisi che ha colpito il sistema economico-finanziario a partire dal 2008.

Uno dei più recenti e autorevoli contributi in tema di *corporate governance* è rappresentato dai *Principles of Corporate Governance* emessi dall'OECD e dai Paesi del G20 (settembre 2015) che costituisce il principale riferimento per i prossimi aggiornamenti dei codici di *corporate governance* dei Paesi membri. Tra le novità introdotte nel capitolo VI dei *Principles of Corporate Governance*, dedicato alle responsabilità del *Board*, spicca il compito di *oversight of the company's risk management*. Tale compito prevede la supervisione da parte del Consiglio dei ruoli e delle responsabilità nel processo di *risk management*, la definizione della tipologia e del livello di rischio che la società è disposta ad assumere per raggiungere i propri obiettivi, nonché le modalità con cui i rischi devono essere gestiti.

Non vi sono quindi più dubbi in merito al ruolo del Consiglio di Amministrazione sul *risk oversight*; non è altresì immediato individuare le modalità più idonee, in funzione della complessità e delle dimensioni della società, che consentano al *Board* l'esercizio di tale compito ovvero l'efficace supervisione dei principali rischi della società e dei sottostanti processi di *risk management*.

L'obiettivo del Quaderno consiste quindi nel fornire gli elementi utili alle società ed ai membri dei relativi *Board* per attivare un processo di *risk management* in grado di soddisfare le nuove aspettative in tema di *corporate governance* in linea con i requisiti definiti dalle *leading practice* e dalla normativa di riferimento (Capitolo I).

Con riferimento al modello organizzativo, al fine di garantire piena efficacia al processo di gestione dei rischi, si dovrebbe considerare come prioritaria la necessità di una chiara definizione ed attribuzione delle responsabilità anche a livello di Gruppo, di gestione e coordinamento delle attività di individuazione, valutazione, misurazione e monitoraggio dei rischi. In particolare, il monitoraggio è principalmente finalizzato alla supervisione delle azioni di *mitigation* nel continuo, verificandone l'effettiva realizzazione e fungendo da elemento di raccordo con il Consiglio di Amministrazione, il Comitato Controllo e Rischi ed il *management*.

Tale ruolo di coordinamento, indipendentemente dall'adozione di modelli di *risk management* più o meno accentrati, è tipicamente attribuibile alla figura del *Chief Risk Officer* o ad altra funzione possibilmente non operativa e pertanto in grado di poter svolgere il proprio mandato con un adeguato livello di autonomia.

In merito alle possibili soluzioni organizzative, l'attribuzione dei ruoli per assicurare una corretta gestione del rischio è una scelta aziendale, alla cui base dovrebbe essere effettuata un'attenta valutazione di molteplici fattori, tra cui, *in primis*, la coerenza complessiva tra il sistema di *governance*, il *business model* e gli obiettivi strategici dell'organizzazione, il sistema di attribuzione dei poteri, le caratteristiche di complessità aziendale, la natura dei rischi che impattano sulle attività svolte.

Qualunque sia la soluzione organizzativa adottata è comunque fondamentale che:

- la gestione dei rischi sia orientata a supportare la governance nel processo di definizione degli indirizzi e degli obiettivi;
- il sistema di gestione dei rischi consenta di verificare nel continuo che il perseguimento degli obiettivi sia coerente con i livelli stabiliti di “appetito al rischio”;
- si attivi un processo virtuoso di individuazione dei nuovi rischi che faciliti la tempestiva definizione delle azioni di rimedio ed il relativo monitoraggio;
- siano definite opportune attività di informazione e formazione per accrescere la sensibilità e la cultura interna.

In tale contesto, nell’ambito del più ampio mandato di *risk oversight* affidato al Consiglio di Amministrazione, assicurare l’attuazione di un processo di risk management correttamente disegnato - sulla base delle effettive necessità della società e del business - e funzionante per tutte le attività aziendali senza alcuna preclusione (evitando cosiddette “no-go areas”), rappresenta un requisito fondamentale di buon governo (Capitolo II).

Con riferimento al funzionamento del processo, è fondamentale codificare un articolato sistema di flussi informativi che consenta il tempestivo controllo della differente esposizione ai rischi e la conseguente gestione di eventuali anomalie riscontrate, assicurando una tempestiva informazione agli organi deputati.

L’adozione e l’effettivo funzionamento di un processo di gestione dei rischi, in particolare nelle realtà di dimensioni più rilevanti, dovrebbero essere supportati da adeguati strumenti che, oltre a facilitare le attività di mappatura e analisi del rischio, siano contestualmente idonei ad ottimizzare la gestione e l’alimentazione del sistema dei flussi informativi.

La disponibilità di adeguati flussi, che possono supportare i processi decisionali atti ad intraprendere le misure di trattamento dei rischi o a perseguire le opportunità ad essi correlate, presuppone in ogni caso l’esistenza ed il funzionamento di processi di *risk management* strutturati e la diffusione di una piena consapevolezza dei rischi (*risk awareness*).

In tale contesto, il ruolo del Consiglio di Amministrazione è determinante per lo sviluppo di un’appropriata *risk culture* - da intendersi anche in termini di diffusione, a tutti i livelli dell’organizzazione, di un linguaggio comune e di strumenti idonei per l’individuazione, valutazione, gestione e monitoraggio dei rischi.

A questo proposito, una *risk governance* ben definita, in cui ciascun soggetto incaricato di assolvere a compiti di supervisione dei rischi fornisca il suo contributo secondo differenti gradi di autonomia e indipendenza, e che garantisca che le informazioni complessivamente generate siano idonee ad assicurare un appropriato livello di coinvolgimento da parte del Consiglio di Amministrazione sulla gestione dei rischi svolta dal *management*, facilita il monitoraggio continuo sulla natura e sul livello di rischio gestito nonché sui rischi nuovi ed emergenti, realizzando un ciclo virtuoso di allineamento tra strategie, obiettivi, rischi e rendimento nell’ottica della sostenibilità nel medio-lungo periodo e della creazione di valore (Capitolo III).

L’attività di monitoraggio del sistema da parte del Consiglio di Amministrazione dovrebbe essere anch’essa oggetto di specifica disciplina/regolamentazione (con riferimento in particolare a tempistiche e modalità di svolgimento, natura e frequenza del *reporting* dei risultati) e prevedere un opportuno bilanciamento tra attività di monitoraggio continuo (*on going*) e attività di *review* periodica (di norma su base almeno annuale), contemplando attività di *oversight* sia sull’organizzazione preposta alla gestione dei rischi (inclusi ruoli e responsabilità degli attori del processo) che sul processo (ossia sulle attività poste in essere). Perché ne sia assicurata piena efficacia, è opportuno:

- prevederne un'adeguata programmazione nell'agenda del *Board* (e dei suoi Comitati, specie il Comitato Controllo e Rischi),
- garantire che sia supportata da adeguati flussi e scambi informativi da parte delle funzioni e degli organi aziendali e societari con responsabilità sul SCIGR, inclusi quelli con finalità consultive ed istruttorie (Comitato Controllo e Rischi, Amministratore Incaricato del SCIGR, *Internal Audit*, *Chief Risk Officer*, ecc.), definiti e condivisi nella struttura, nei contenuti e nelle tempistiche con gli interessati;
- ispirarsi, ove possibile, a metodologie consolidate e *framework* internazionalmente riconosciuti (es. *CoSO⁵ Framework*, *Maturity Model Approach*, ecc.) (Capitolo IV).

Un adeguato processo di monitoraggio è elemento essenziale per esprimere la valutazione sull'adeguatezza complessiva del SCIGR. Con riferimento a tale aspetto, è da rilevarsi che alla luce delle disposizioni normative e autoregolamentari previste dal Codice Civile e dal Codice di Autodisciplina, il Consiglio di Amministrazione è chiamato ad esprimere – con cadenza almeno annuale – la propria valutazione di adeguatezza in merito a due differenti aspetti: da un lato, in relazione all'assetto organizzativo, amministrativo e contabile, dall'altro, in relazione al SCIGR dell'Emittente e delle società controllate aventi rilevanza strategica. A tali fini è possibile considerare l'opportunità di condurre una valutazione integrata o disgiunta.

Come ampiamente descritto nel Quaderno, il giudizio di adeguatezza del Consiglio di Amministrazione è necessariamente supportato dalle risultanze dei diversi soggetti che a vario titolo sono coinvolti nel SCIGR. Sebbene, per gli emittenti quotati, il Codice di Autodisciplina presupponga il coordinamento e l'interdipendenza dei diversi soggetti coinvolti nel SCIGR, è opportuno ribadire che rimane comunque in capo al Consiglio di Amministrazione l'onere di definire le modalità di tale coordinamento, i ruoli e le responsabilità di ciascun soggetto, nonché i principali flussi informativi a supporto del processo di valutazione periodica di adeguatezza del SCIGR effettuata dal *Board* che, a tal fine, definisce in prima istanza le linee di indirizzo del sistema dei controlli.

Tenendo conto delle evidenze ottenute dai diversi attori del SCIGR e sulla base dei propri approfondimenti, il Consiglio effettua autonome considerazioni sull'adeguatezza complessiva del sistema, valutando l'entità e le implicazioni di eventuali carenze riscontrate. L'esito di tali valutazioni, unitamente alle modalità attraverso cui il *Board* è informato circa l'adeguatezza e l'operatività del sistema, dovrebbe costituire oggetto di apposita informativa nella Relazione sul Governo Societario e gli Assetti Proprietari.

A questo proposito, in termini più generali, l'informativa - anche esterna - in merito alla capacità dell'azienda (e del Gruppo nel suo complesso) di affrontare e gestire i rischi può rappresentare un elemento distintivo a supporto della valutazione della sua capacità di creare e conservare valore (Capitolo V).

Un'efficace ed efficiente gestione dei rischi rappresenta pertanto per le organizzazioni un'importante opportunità: prevenire e mitigare i rischi significa poter trasformare le minacce in vantaggio competitivo, a beneficio di tutti gli *stakeholder* (azionisti, *management*, dipendenti, clienti, contesto sociale di riferimento, ecc.).

⁵ *Committee of Sponsoring Organization of the Treadway Commission.*

CAPITOLO I

PANORAMICA SUI PRINCIPALI RIFERIMENTI NORMATIVI E DI *LEADING PRACTICE* IN MERITO AL RUOLO DEL CONSIGLIO DI AMMINISTRAZIONE SUL SISTEMA DI CONTROLLO INTERNO E DI GESTIONE DEI RISCHI

1. Considerazioni generali - 2. La normativa primaria, gli obiettivi ed i rischi dell'impresa - 3. Il Codice di Autodisciplina del Comitato per la *Corporate Governance* delle società quotate - 4. Le più recenti evoluzioni internazionali - 5. Il gruppo di imprese

1. Considerazioni generali

Per introdurre il tema dell'esercizio del *risk oversight* da parte del Consiglio di Amministrazione, ricordiamo che l'impresa e l'imprenditore assumono dei rischi, patrimoniali e/o personali, per svolgere, in base ad una strategia imprenditoriale riproducibile nel tempo, una attività economica che produce un plusvalore, per sé e per i propri *stakeholder* (azionisti, clienti, fornitori, dipendenti, finanziatori, etc.). Gli elementi essenziali che quindi caratterizzano l'attività imprenditoriale sono:

- gli obiettivi di creazione di valore, di natura economica, espressi in forma qualitativa o quantitativa (ad esempio, conquistare la *leadership* in un mercato geografico);
- i rischi d'impresa assunti, che rappresentano tutti gli eventi o circostanze che, in estrema sintesi, rispondono alla domanda *what can go wrong?*. Essi, in parte, sono connaturati agli obiettivi perseguiti (ad esempio, all'obiettivo di aumentare la quota di mercato è connesso il rischio di una battaglia sui prezzi, con la conseguenza di una possibile perdita di posizionamento rispetto ai *competitor*);
- la strategia di gestione del rischio (ad esempio, la differenziazione del prodotto);
- il modello organizzativo ed operativo coerente alla strategia definita (ad esempio, il processo di *marketing* strategico per la differenziazione del prodotto).

Quando l'impresa viene svolta in forma societaria, il ruolo dell'imprenditore è svolto dal Consiglio di Amministrazione che assume quindi un ruolo centrale nella supervisione e nell'indirizzo del sistema di controllo interno e della gestione dei rischi.

Non essendovi spesso una coincidenza tra proprietà e imprenditore, l'attività del Consiglio di Amministrazione è centrale non solo per il ruolo imprenditoriale che ricopre, ma anche per i flussi informativi che riceve dagli altri organi aziendali e che deve veicolare agli azionisti e agli altri *stakeholder*.

In tale prospettiva, la gestione delle imprese ad alto livello consiste nel disegno e nell'attivazione di processi di *corporate governance* e di controllo interno che mantengano allineati e coordinati, anche rispetto alle evoluzioni ed alle aspettative degli *stakeholder*, tutti gli obiettivi, le strategie, ed i modelli organizzativi ed operativi di gestione dei rischi dell'impresa.

Non a caso, la recente crisi economica ha alimentato un acceso dibattito internazionale sulla validità delle attuali strutture di *corporate governance* e sull'efficacia dei sistemi di controllo per la competitività delle imprese nei mercati globali, ciò anche alla luce dei significativi scandali finanziari che hanno interessato più paesi, mercati ed ordinamenti.

Ad esempio, secondo l'*Organisation for Economic Co-operation and Development* (OECD), – organismo che rappresenta il c.d. *International Standard Setter* tra l'altro in materia di *corporate governance* – la recente crisi finanziaria ha costituito uno stress test dei sistemi di *corporate governance* non soltanto per l'applicazione dei

principi raccomandati dall'OECD, ma soprattutto sul ruolo della *corporate governance* nel soddisfare gli urgenti bisogni di ristabilire fiducia nei mercati finanziari e di promuovere la crescita economica⁶.

Le decisioni in merito all'approccio al rischio dovranno allora essere finalizzate a bilanciare crescita, target stabiliti e relativi rischi, nonché ad impiegare efficacemente le risorse nello sviluppo del sistema di controllo interno e di gestione dei rischi al fine di raggiungere gli obiettivi di impresa.

Da ciò deriva l'essenzialità dell'assunzione e gestione dei rischi in qualsivoglia attività imprenditoriale, grande o piccola, semplice o complessa che sia. Non è quindi sempre possibile separare compiti di gestione da compiti di controllo in quanto il sistema di controllo interno e di gestione dei rischi, è parte inscindibile, essenziale e necessaria, della gestione.

È opportuno sin da subito sottolineare che tali aspetti risulteranno più o meno strutturati a seconda delle dimensioni, della struttura e della complessità dell'impresa. Tali caratteristiche specifiche finiscono inevitabilmente anche per riflettersi sulle modalità di formalizzazione degli obiettivi individuati, che nelle realtà quotate o di dimensioni più significative trovano espressione e dettaglio attraverso piani strategici a medio e lungo termine (cd. *business plan*).

Gli obiettivi d'impresa strategici pianificati a medio e lungo termine hanno la caratteristica di essere obiettivi generali, stabiliti ai livelli più elevati della struttura organizzativa e strettamente allineati e collegati alla *mission* ed all'orientamento strategico di fondo. Essi dovranno poi essere declinati in chiave operativa negli obiettivi delle funzioni organizzative e dei processi aziendali a medio e lungo termine e, infine, a breve termine, in modo gerarchico in tutti i livelli dell'organizzazione aziendale (divisioni, funzioni, processi, unità operative, etc.) perché diventino obiettivi operativi di gestione corrente.

Quindi, fissati gli obiettivi generali e quelli più specifici a breve termine, l'impresa dovrà identificare i fattori critici od abilitanti del suo successo ed i relativi rischi, eventi e condizioni che possono minacciare o impedire il raggiungimento degli obiettivi prefissati.

Contestualmente all'evoluzione della dottrina aziendalistica, a partire dalla fine degli anni ottanta sono stati sviluppati alcuni importanti *framework* di controllo con la finalità di promuovere e supportare l'attuazione, da parte delle società, di idonei modelli di controllo interno e di gestione dei rischi, così che questi possano fornire una ragionevole certezza sul raggiungimento degli obiettivi aziendali⁷.

In linea con quanto riportato nei *framework* internazionali, il *management*, sotto la supervisione dell'organo di governo strategico, definisce gli obiettivi a livello aziendale, a loro volta allineati con la *mission* e le strategie dell'organizzazione. Gli obiettivi di alto livello riflettono le scelte fatte dal *management* e dagli amministratori relativamente a come l'organizzazione intende produrre e conservare valore per gli *stakeholder*.

⁶ OECD, OECD *Corporate Governance Committee in Corporate Governance, Value Creation and Growth*, 2012.

⁷ Nel 1992 il CoSO (*Committee of Sponsoring Organizations of the Treadway Commission*) ha pubblicato l'*Internal Control – Integrated Framework*, conosciuto anche come *CoSO Report*, aggiornato nel mese di maggio 2013, con l'obiettivo di supportare le società nel valutare e migliorare i propri sistemi di controllo interno e porsi come standard di riferimento per elaborare politiche gestionali, norme di legge e regolamenti per indirizzare le attività aziendali verso gli obiettivi prestabiliti, attraverso un'efficace gestione del controllo interno.

Negli anni successivi, anche a seguito degli scandali finanziari e dei fallimenti che hanno coinvolto importanti società a livello mondiale, sono state promulgate alcune leggi, tra cui il *Sarbanes – Oxley Act* (2002) negli Stati Uniti e la Legge 262/2005 in Italia. Questo cruciale passaggio ha posto il tema dei controlli interni e della gestione dei rischi tra le priorità dell'agenda delle società quotate nei mercati regolamentati e la prassi di disporre di efficaci sistemi di controllo interno è diventata un obbligo di legge.

2. La normativa primaria, gli obiettivi ed i rischi dell'impresa

Gli articoli 2380 e seguenti del Codice Civile individuano compiti e responsabilità attribuiti al Consiglio di Amministrazione.

In particolare, l'art. 2380-*bis*⁸ dispone che la gestione dell'impresa spetti esclusivamente agli amministratori, i quali compiono le operazioni necessarie per l'attuazione dell'oggetto sociale.

L'art. 2381⁹ sancisce, al comma 3, che il Consiglio di Amministrazione, sulla base delle informazioni ricevute, valuta l'adeguatezza dell'assetto organizzativo, amministrativo e contabile della società e esamina i piani strategici, industriali e finanziari della società, quando elaborati.

L'espressione "piani strategici, industriali e finanziari" potrebbe dunque costituire un richiamo, anche se indiretto e in certa misura circoscritto, agli obiettivi aziendali.

La dottrina giuridica che si è occupata della materia ha ritenuto che la presenza dell'inciso "quando elaborati" renderebbe per gli amministratori della società non obbligatoria la predisposizione dei piani. Ciò in quantotale adempimento, nelle società di piccole dimensioni e scarsamente dinamiche, potrebbe rappresentare un inutile aggravio dei costi senza reali benefici.

Diversamente, la predisposizione di documenti complessi, articolati e di ampio respiro come i piani appare più appropriata nelle società di maggiori dimensioni.

⁸ Art. 2380-*bis* cod. civ.: "La gestione dell'impresa spetta esclusivamente agli amministratori, i quali compiono le operazioni necessarie per l'attuazione dell'oggetto sociale.

L'amministrazione della società può essere affidata anche a non soci.

Quando l'amministrazione è affidata a più persone, queste costituiscono il Consiglio di Amministrazione.

Se lo statuto non stabilisce il numero degli amministratori, ma ne indica solamente un numero massimo e minimo, la determinazione spetta all'assemblea.

Il Consiglio di Amministrazione sceglie tra i suoi componenti il presidente, se questi non è nominato dall'assemblea."

⁹ Art. 2381 cod. civ.: "Salvo diversa previsione dello statuto, il presidente convoca il Consiglio di Amministrazione, ne fissa l'ordine del giorno, ne coordina i lavori e provvede affinché adeguate informazioni sulle materie iscritte all'ordine del giorno vengano fornite a tutti i consiglieri.

Se lo statuto o l'assemblea lo consentono, il Consiglio di Amministrazione può delegare proprie attribuzioni ad un comitato esecutivo composto da alcuni dei suoi componenti, o ad uno o più dei suoi componenti.

Il Consiglio di Amministrazione determina il contenuto, i limiti e le eventuali modalità di esercizio della delega; può sempre impartire direttive agli organi delegati e avocare a sé operazioni rientranti nella delega. Sulla base delle informazioni ricevute valuta l'adeguatezza dell'assetto organizzativo, amministrativo e contabile della società; quando elaborati, esamina i piani strategici, industriali e finanziari della società; valuta, sulla base della relazione degli organi delegati, il generale andamento della gestione.

Non possono essere delegate le attribuzioni indicate negli articoli 2420-*ter*, 2423, 2443, 2446, 2447, 2501-*ter* e 2506-*bis*.

Gli organi delegati curano che l'assetto organizzativo, amministrativo e contabile sia adeguato alla natura e alle dimensioni dell'impresa e riferiscono al Consiglio di Amministrazione e al Collegio Sindacale, con la periodicità fissata dallo statuto e in ogni caso almeno ogni sei mesi, sul generale andamento della gestione e sulla sua prevedibile evoluzione nonché sulle operazioni di maggior rilievo, per le loro dimensioni o caratteristiche, effettuate dalla società e dalle sue controllate.

Gli amministratori sono tenuti ad agire in modo informato; ciascun amministratore può chiedere agli organi delegati che in consiglio siano fornite informazioni relative alla gestione della società."

Oltre a quello dell'art. 2381, comma 3, cod. civ., la disciplina delle società di capitali contempla altri episodici riferimenti a concetti riconducibili a quello di obiettivi aziendali. Si tratta di alcune norme eterogenee, da cui emerge un concetto di obiettivi di natura determinata e/o in relazione a fattispecie specifiche, quali le operazioni sulle azioni proprie (art. 2358 cod. civ.¹⁰), il contenuto della nota integrativa (art. 2427 cod. civ.¹¹), le operazioni di fusione a seguito dell'acquisizione con indebitamento (art. 2501-*bis* cod. civ.¹²).

In relazione alle norme citate il legislatore richiede agli amministratori di indicare gli obiettivi aziendali perseguiti in quanto connotati da un elevato profilo di rischio per gli *stakeholder*.

Al di là della mancanza di una chiara indicazione normativa con valenza generale, dalle norme appena citate emerge come, anche nell'ottica del legislatore, i concetti di obiettivo e di rischio risultino tra loro strettamente legati. Neppure il concetto di rischi aziendali è più del tutto estraneo alla disciplina societaria. In effetti, l'art. 2428, comma 1, cod. civ., come modificato dal D.Lgs. 2 febbraio 2007, n. 32, prevede che la relazione sulla gestione debba contenere, oltre ad una analisi della situazione della società e dell'andamento e del risultato della gestione, anche "una descrizione dei principali rischi e incertezze cui la società è esposta"¹³.

La prevista descrizione dei principali rischi nell'ambito della relazione sulla gestione pare necessariamente presupporre, quale premessa logica indispensabile, che gli amministratori provvedano preventivamente all'individuazione dei rischi oggetto di successiva descrizione.

Anche il concetto di "rischi" appare poi riscontrabile nella normativa primaria con riferimento ad alcune ipotesi specifiche. Ci si riferisce, in particolare, alle previsioni dell'art. 2428, comma 3, n. 6-*bis* cod. civ. e dell'art. 40, comma 2, lett. d-*bis*, del D.Lgs. 127/1991, sempre in ordine al contenuto della relazione sulla gestione, e a quella di cui all'art. 2358, comma 3, cod. civ. in tema di operazioni sulle proprie azioni.

In sintesi, l'attuale formulazione della normativa primaria non pare, allo stato, sufficiente per chiarire che la fissazione degli obiettivi aziendali e l'individuazione dei rischi da parte degli amministratori è un'attività sempre doverosa.

Né, d'altro canto, una qualche indicazione generale pare potersi ricavare dalle altre norme "particolari" sopra richiamate, che pure evocano i concetti di "obiettivi aziendali" e "rischi", ma in relazione a situazioni specifiche.

Inoltre, come già precedentemente indicato, ai sensi dell'art. 2381 comma 3 del Codice civile il Consiglio è chiamato a formulare una valutazione di adeguatezza circa gli assetti interni dell'impresa (organizzativo, amministrativo e contabile), da assolvere sulla base delle informazioni ricevute.

¹⁰ L'art. 2358, comma 3 cod. civ. (rubricato "Altre operazioni sulle proprie azioni"), sancisce che gli amministratori di una società che ponga in essere operazioni sulle proprie azioni (vale a dire che accordi prestiti o fornisca garanzie a terzi per l'acquisto o la sottoscrizione delle stesse, cfr. art. 2358, comma 1), sono tenuti a predisporre una relazione che illustri, tra l'altro, gli "obiettivi imprenditoriali" che giustificano l'operazione, lo "specifico interesse" che l'operazione presenta per la società e i "rischi" che essa comporta in termini di liquidità e di solvibilità.

¹¹ L'art. 2427, comma 1 cod. civ. (rubricato "Contenuto della nota integrativa") richiama il concetto di obiettivi aziendali al n. 22-*ter*), laddove si prevede che debbano essere indicati nella nota integrativa la natura e "l'obiettivo economico" di accordi non risultanti dallo stato patrimoniale ogniqualevolta "i rischi e i benefici" da essi derivanti siano significativi e l'indicazione degli stessi sia necessaria al fine della valutazione della situazione patrimoniale e finanziaria e del risultato economico della società.

¹² L'art. 2501-*bis*, comma 3 cod. civ. (rubricato "Fusione a seguito di acquisizione con indebitamento"), stabilisce che la relazione dell'organo amministrativo sull'operazione di *leveraged buy-out* deve, tra l'altro, descrivere gli "obiettivi che si intendono raggiungere" con l'operazione medesima.

¹³ Per completezza, si ricorda che l'art. 40 del D.Lgs. 9 aprile 1991, n. 127, con riguardo alla relazione sul bilancio consolidato e a seguito dello stesso D.Lgs. 32/2007, contiene una previsione analoga all'art. 2428, comma 1, cod. civ..

Tale principio, di carattere generale, non fornisce di per sé indicazioni circa i termini di raffronto ed i criteri da adottare per la valutazione dell'adeguatezza degli assetti.

A tale adempimento da parte del Consiglio si affianca quanto previsto al comma 5 dell'art. 2381 che pone in capo agli organi delegati il dovere di curare che "l'assetto organizzativo, amministrativo e contabile sia adeguato alla natura e alle dimensioni dell'impresa".

In una prospettiva di ripartizione dei compiti di *governance*, gli organi delegati curano, sulla base delle linee di indirizzo definite dagli amministratori, che l'assetto organizzativo, amministrativo e contabile sia adeguato alla natura e alle dimensioni dell'impresa (art. 2381, comma 5 cod. civ.); spetta invece al Consiglio di Amministrazione valutarne l'adeguatezza, sulla base delle informazioni ricevute (art. 2381, comma 3 cod. civ.).

Tali aspetti saranno meglio trattati all'interno del Capitolo V, cui si rimanda per maggiori approfondimenti e per ottenere spunti sulle linee operative da seguire ai fini dell'emissione del giudizio di adeguatezza.

In conclusione, per quanto non manchino oggi nella normativa primaria utili riferimenti per porre in capo agli amministratori di tutte le società l'obbligo di individuazione di obiettivi e rischi aziendali, il quadro normativo vigente appare ancora frammentato. Le disposizioni dell'autodisciplina delle società quotate, seppur applicabili ad un limitato ambito di società, costituiscono allo stato attuale, come si vedrà nel successivo paragrafo, il punto più avanzato nella disciplina della materia.

3. Il Codice di Autodisciplina del Comitato per la Corporate Governance delle società quotate

Con le carenze del quadro giuridico scaturente dalla normativa primaria precedentemente descritta la possibilità di intervento della c.d. *soft law*, rappresentata dal Codice di Autodisciplina, per definire ruolo e responsabilità del Consiglio di Amministrazione è stata ampia.

Come noto, il Codice di Autodisciplina, in linea con l'esperienza dei principali mercati internazionali, indica le *best practice* in materia di governo societario raccomandate dal Comitato per la Corporate Governance delle Società Quotate, da applicarsi secondo il principio del "*comply or explain*", come rappresentato al Cap.II, Par.1.

Per quanto qui maggiormente interessa, il vigente art. 7 del Codice, ovvero nella versione approvata nel dicembre 2011 e rimasta sostanzialmente invariata all'esito della recente rivisitazione del luglio 2015, pone Principi, Criteri Applicativi e Commenti sul "*Sistema di controllo interno e di gestione dei rischi*".

Nel fare ciò, tale importante documento assegna un ruolo centrale all'"*identificazione, la misurazione, la gestione e il monitoraggio dei principali rischi*" che possono impattare sul raggiungimento degli obiettivi aziendali (cfr. Principio 7.P.1), rafforzando l'attenzione alla gestione dei rischi quale strumento gestionale per contribuire alla conduzione dell'impresa coerente con gli obiettivi e all'assunzione di decisioni consapevoli (cfr. Principio 7.P.2).

La stessa ridenominazione del "sistema di controllo interno" in "sistema di controllo interno e di gestione dei rischi" ("SCIGR") e del "comitato per il controllo interno" in "comitato controllo e rischi" confermano la specifica attenzione rivolta dagli estensori del Codice proprio ai temi oggetto del presente Quaderno.

Le scelte ora richiamate paiono essere il frutto dalla presa d'atto, da parte dei redattori del Codice di Autodisciplina, che "la moderna concezione dei controlli ruota attorno alla nozione di rischi aziendali, alla loro identificazione, valutazione e monitoraggio" (così il commento all'art. 7, terzo capoverso). È anche per tale motivo che "*la normativa e il Codice si riferiscono al sistema di controllo interno e di gestione dei rischi come a un sistema unitario di cui il rischio rappresenta il filo conduttore*".

L'art. 7 del Codice di Autodisciplina fornisce poi una chiara definizione di SCIGR, in linea con quanto previsto dal CoSO Report, vale a dire *“l'insieme delle regole, delle procedure e delle strutture organizzative volte a consentire l'identificazione, la misurazione, la gestione e il monitoraggio dei principali rischi”* (cfr. Principio 7.P.1).

Il Principio 7.P.3 individua, in coerenza con gli orientamenti più avanzati della dottrina aziendalistica e dei *framework* internazionali, anche gli attori coinvolti a vario titolo nell'indirizzo, nella gestione, nella valutazione e nel monitoraggio del SCIGR, ciascuno per le proprie rispettive competenze.

Ci si riferisce, più precisamente, a:

- il Consiglio di Amministrazione, sia collegialmente, nel suo ruolo di indirizzo e definizione delle linee guida del sistema, sia attraverso l'individuazione di soggetti delegati (l'amministratore incaricato del sistema di controllo interno e di gestione dei rischi) e di comitati al suo interno (il comitato controllo e rischi);
- *il management*;
- le funzioni aziendali di primo e secondo livello con compiti di gestione del SCIGR;
- la funzione *internal audit* quale linea di difesa di terzo livello;
- il Collegio Sindacale quale organo di controllo.

I successivi Criteri Applicativi da 7.C.1 a 7.C.6 forniscono una ricognizione puntuale dei principali compiti di ciascuno degli attori del SCIGR sopra richiamati. È senz'altro agevole riconoscere nello schema di ruoli e competenze proposto dal Codice i principi organizzativi elaborati dalla prassi aziendalistica e dai principali *framework* internazionali.

Il ruolo centrale è senza dubbio affidato al Consiglio di Amministrazione, il quale, tra l'altro, *“definisce le linee di indirizzo del sistema di controllo interno e di gestione dei rischi, in modo che i principali rischi afferenti all'emittente e alle sue controllate risultino correttamente identificati, nonché adeguatamente misurati, gestiti e monitorati”* (cfr. Criterio Applicativo 7.C.1, lett. a)).

Il Consiglio di Amministrazione è altresì chiamato, ai sensi del criterio applicativo 1.C.1, a definire *“la natura e il livello di rischio compatibile con gli obiettivi strategici dell'emittente”* (in termini analoghi, cfr. anche il Criterio Applicativo 7.C.1, lett. a), ultima parte).

Si può facilmente ravvisare in tale disposizione il riferimento al concetto di *risk appetite* (ovvero il livello di rischio complessivo che l'emittente è disposto ad assumere per raggiungere i propri obiettivi), ad ulteriore conferma della stretta e ineludibile connessione tra i richiamati concetti oggetto del presente Quaderno.

Il Commento all'art. 7 del Codice di Autodisciplina fa riferimento al modello delle cosiddette tre “linee di difesa” contro i rischi che minacciano il raggiungimento degli obiettivi dell'impresa, elaborato dalla dottrina aziendalistica e dai *framework* internazionali. In particolare, il Codice evidenzia chiaramente la distinzione tra le funzioni aziendali con specifici compiti in tema di controllo interno e gestione dei rischi, cui sono affidati i cosiddetti controlli “di secondo livello”, rispetto alla terza linea di difesa costituita dalla funzione *Internal Audit*.

Fermo quanto sopra, emerge, quale considerazione di carattere generale, che: *“un sistema dei controlli, per essere efficace, deve essere “integrato”: ciò presuppone che le sue componenti siano tra loro coordinate e interdipendenti e che il sistema, nel suo complesso, sia a sua volta integrato nel generale assetto organizzativo, amministrativo e contabile della società”* (cfr. Commento all'art. 7, terzo capoverso). Il già richiamato Principio 7.P.3 raccomanda inoltre agli emittenti l'individuazione di modalità di coordinamento

tra i vari soggetti coinvolti nel SCIGR: “*al fine di massimizzare l’efficienza del sistema di controllo interno e di gestione dei rischi e di ridurre le duplicazioni di attività*”.

Anche sotto questo profilo, si tratta senza dubbio di una presa d’atto significativa di quel concetto di necessaria integrazione di tutte le componenti del sistema di controllo interno di un’impresa e della centralità del ruolo del Consiglio di Amministrazione.

In particolare, il Consiglio di Amministrazione esplica la sua centralità nella definizione dei limiti di rischio assumibili e delle linee guida per la gestione del rischio, la cui effettiva applicazione è demandata all’intera struttura organizzativa, attraverso la:

- definizione dei piani strategici, finanziari e industriali della Società, al fine di accertare la coerenza delle strategie e degli obiettivi delineati con i livelli di rischio assumibili, nonché fornire le linee di indirizzo del SCIGR riguardo i livelli di rischio ritenuti accettabili (che possono essere rivisti sulla base degli esiti delle attività di monitoraggio);
- valutazione dell’adeguatezza e dell’efficacia del SCIGR rispetto alle caratteristiche dell’impresa e del Gruppo ed al profilo di rischio assunto. Tale valutazione si traduce nella verifica di:
 - limiti o vincoli nell’assunzione di rischi;
 - processi di gestione e controllo strutturalmente efficaci ed efficienti;
- sistema delle deleghe, con relativo conferimento di poteri al *management*, a cui il Consiglio di Amministrazione affida la gestione del rischio assunto.

Annualmente il Consiglio di Amministrazione esprime la valutazione del SCIGR nella Relazione sul Governo Societario e gli Assetti Proprietari, che, ai sensi dell’art. 123-*bis* del TUF, può rappresentare una parte della Relazione sulla Gestione o un documento autonomo. Quest’ultima costituisce uno dei principali strumenti che gli azionisti hanno a disposizione per acquisire piena contezza sull’andamento della gestione societaria. Una corretta e chiara valutazione del SCIGR da parte del Consiglio di Amministrazione impatta direttamente sull’informativa fornita al mercato, con l’obiettivo prioritario della creazione di valore per gli azionisti in un orizzonte di medio lungo periodo (cfr. Principio I.P.2. del Codice di Autodisciplina). Tale aspetto integra la valutazione sull’adeguatezza degli assetti societari, come meglio dettagliato nel Capitolo V del presente Quaderno.

Affinché il Consiglio di Amministrazione possa acquisire tutte le informazioni necessarie per definire gli obiettivi attesi coerentemente con i livelli di rischio sostenibili, nonché per monitorare il perseguimento degli stessi e l’efficacia di sistemi di controllo e di gestione dei rischi, i flussi informativi tra tutti gli attori del SCIGR devono imprescindibilmente essere affidabili, chiari, completi e tempestivi; essi rappresentano dunque un elemento cruciale su cui si fonda l’intero sistema di *risk oversight*.

Da tutto quanto sopra si evince chiaramente come il Codice di Autodisciplina rappresenti, allo stato, il punto più avanzato di elaborazione della materia qui in discorso nell’ambito del nostro ordinamento.

4. Le più recenti evoluzioni internazionali

Uno tra i più recenti e autorevoli contributi in tema di *corporate governance* è rappresentato dai “*Principles of Corporate Governance*” emessi dal G20/OECD nel mese di settembre 2015. Molte raccomandazioni presenti nella precedente versione (2004) sono rimaste invariate ritenendosi ancora le stesse valide per l’implementazione di un’efficace *governance*.

Oltre a trattare il ruolo del Consiglio di Amministrazione nella *governance* societaria già citato nel primo paragrafo, i principi forniscono linea guida e raccomandazioni secondo 6 direttive differenti che riguardano:

- i *framework* di *corporate governance*, quali strumenti efficaci di promozione della trasparenza dei mercati finanziari e dell'efficiente allocazione delle risorse attraverso l'aumento della qualità della regolamentazione, dell'effettivo recepimento della stessa da parte delle società quotate nonché del livello di supervisione svolto dalle *authority* di riferimento. In particolare, un nuovo principio è stato dedicato al ruolo dei gestori dei mercati azionari per lo sviluppo di una buona *governance*;
- i diritti degli azionisti ed i relativi meccanismi di voto, sottolineando l'uso dell'*information technology* all'interno dell'assemblea, le procedure per l'approvazione delle operazioni con parti correlate nonché per la partecipazione degli azionisti nelle decisioni in merito alla remunerazione degli amministratori;
- il ruolo di investitori istituzionali, intermediari e altri soggetti che operano nei mercati azionari (società di *rating*, consulenti, ecc.), rafforzando la gestione dei potenziali conflitti di interesse e l'informativa al mercato;
- il ruolo degli *stakeholder* nella *corporate governance*, incoraggiando la cooperazione tra le società quotate e i loro *stakeholder* basata sul rispetto dei diritti di quest'ultimi derivanti sia dalla normativa sia da altri riferimenti di autodisciplina. Con tale finalità, è previsto l'accesso da parte degli *stakeholder* alle informazioni aziendali in modo che possano valutare l'effettivo rispetto dei propri diritti ed eventualmente ottenere risarcimenti in caso di violazioni;
- l'importanza dell'informativa da fornire nei documenti societari, identificando negli obiettivi, risultato economico, parti correlate, remunerazione, fattori di rischio i principali elementi di cui fornire informativa in bilancio. Si richiama inoltre anche la ricognizione delle tendenze in atto in merito all'informativa non finanziaria da fornire su base volontaria, ad esempio sull'ambiente, il sociale, i diritti umani, etc. al fine di accrescere la qualità delle relazioni tra le società e le comunità in cui operano;
- le responsabilità degli amministratori, fornendo una guida per le attività principali del Consiglio quali ad esempio la revisione della strategia societaria. Nuovi riferimenti sono inclusi in merito al ruolo del Consiglio nell'attività di *risk management* e controllo interno. Un nuovo principio include la raccomandazione di istituire comitati specializzati in temi quali remunerazioni, e gestione dei rischi.

Con riferimento a quest'ultimo punto, che regola le responsabilità del Consiglio di Amministrazione, tra le novità introdotte dal G20/OECD compare il compito di "*oversight of the company's risk management*" ovvero la supervisione da parte del consiglio dei ruoli e delle responsabilità nel processo di *risk management*, la definizione della tipologia e del livello di rischio che la società è disposta ad assumere per raggiungere i propri obiettivi (propensione al rischio) nonché le modalità con cui i rischi devono essere gestiti.

Un'altra autorevole fonte in tema di *corporate governance* è rappresentata dal "*The UK Corporate Governance Code*" (più comunemente conosciuto con il nome di *Combined Code*), emesso dal *Financial Reporting Council* (September 2014) – che prevede quale principio di *accountability* del Consiglio di Amministrazione, tra l'altro, la responsabilità di determinare la natura e il potenziale impatto – *extent* – dei rischi di impresa che intende assumere per raggiungere i propri obiettivi strategici, congiuntamente alla responsabilità di mantenere un ragionevole (*sound*) sistema di controllo interno e di gestione dei rischi. In sostanza, il Consiglio di Amministrazione si compenetra nell'impresa, suoi sono i rischi, gli obiettivi e la responsabilità di controllo della gestione¹⁴.

¹⁴ UK Corporate Governance Code–settembre 2014: "*The board is responsible for determining the nature and extent of the principal risks it is willing to take in achieving its strategic objectives. The board should maintain sound risk management and internal control systems*".

Tale principio, del *Combined Code* viene ulteriormente declinato in 3 criteri applicativi (*Code Provisions*, C.2.1., C.2.2. e C.2.3.) che prevedono in capo al Consiglio di Amministrazione il compito di:

- monitorare il sistema di controllo interno e di gestione dei rischi ed almeno annualmente svolgere una verifica (*review*) della sua efficacia, di cui riferire gli esiti nella relazione sulla gestione;
- monitorare che la verifica comprenda tutti i principali (*material*) controlli, compresi quelli relativi ai controlli contabili, operativi e di conformità delle operazioni alla legge;
- confermare nella relazione sulla gestione di aver svolto una valutazione (*assessment*) dei principali rischi dell'impresa, inclusi quelli che minacciano il *business model*, la solvibilità e la liquidità dell'impresa.

A tal fine, lo stesso UK *Corporate Governance Code* ammette la possibilità dell'esistenza di distinti comitati consiliari di audit e di rischio, prevedendo la formalizzazione delle rispettive funzioni e ruolo (*terms of reference*) nonché delle loro modalità di reporting al Consiglio di Amministrazione.

Il codice anglosassone prevede, allo stesso modo di quanto definito dal Codice di Autodisciplina italiano, la predisposizione da parte del Consiglio di Amministrazione di una *disclosure* annuale da effettuarsi nell'*annual report* e sottolinea quali oggetto del monitoraggio, al fine della valutazione, tutti i "*material controls*". Tale principio è inoltre integrato da quanto previsto nelle "*Disclosure and Transparency Rules*"¹⁵, ossia che all'interno dell'informativa sul governo societario sia contenuta una descrizione delle principali caratteristiche del sistema di controllo interno e di gestione dei rischi, in relazione al processo di informativa finanziaria.

Il mandato affidato al Consiglio di Amministrazione sul tema dei rischi appare pertanto chiaro: definire la natura e il livello di rischio compatibile con gli obiettivi strategici. Al fine di supportare il *Board* nell'assolvimento di questo compito e di fare chiarezza in merito alle responsabilità di quest'ultimo rispetto a quelle del *management* sull'attività di *risk management*, lo stesso *Financial Reporting Council* ha emesso (settembre 2014) la "*Guidance on Risk Management, Internal Control and Related Financial and Business Reporting*" a seguito di un lungo dibattito tra *Regulator*, associazioni professionali e società quotate iniziato nel 2011.

Tale Guida - che aggiorna un precedente documento emesso sempre dal *Financial Reporting Council* "*Internal Control Revised Guidance for directors on the Combined Code*" (più comunemente noto come *Turnbull Guidance on Internal Control*) - risponde alla necessità di chiarire più in dettaglio i contenuti dell'attività richiesta al Consiglio di Amministrazione, prevedendo tra i compiti del *Board*:

- "*ensuring the design and implementation of appropriate risk management and internal control systems that identify the risks facing the company and enable the Board to make a robust assessment of the principal risks;*
- "*determining the nature and extent of the principal risks faced and those risks which the organisation is willing to take in achieving its strategic objectives (determining its "risk appetite");*
- "*ensuring that appropriate culture and reward systems have been embedded throughout the organisation;*

¹⁵ *Disclosure and Transparency Rules 7.2.5 R - The corporate governance statement must contain a description of the main features of the company's internal control and risk management systems in relation to the financial reporting process.*

- *agreeing how the principal risks should be managed or mitigated to reduce the likelihood of their incidence or their impact;*
- *monitoring and reviewing the risk management and internal control systems, and the management's process of monitoring and reviewing, and satisfying itself that they are functioning effectively and that corrective action is being taken where necessary; and*
- *ensuring sound internal and external information and communication processes and taking responsibility for external communication on risk management and internal control”.*

Il documento chiarisce quindi la distinzione di responsabilità tra il Consiglio di Amministrazione e il *management*. Il Consiglio di Amministrazione deve acquisire evidenza che il *management* abbia compreso i rischi, implementato adeguati presidi di controllo ed informato tempestivamente il Consiglio di Amministrazione mettendolo in condizione di svolgere il suo ruolo di supervisione¹⁶; dall'altra parte il *management* deve assicurarsi che il Consiglio di Amministrazione abbia chiaramente definito ruoli e responsabilità e che gli stessi siano stati attuati a tutti i livelli dell'organizzazione coerentemente con la cultura aziendale in tema di sistema di controllo interno e di gestione dei rischi.

Il Codice di *corporate governance* sudafricano, King III, ritenuto un altro esempio di *best practice* internazionale in tema di gestione dei rischi, richiede al Consiglio di Amministrazione di effettuare una valutazione non solo del sistema di controllo interno ma dell'intero processo di *risk management*.

Così come nel Codice di Autodisciplina di Borsa Italiana, anche al Consiglio di Amministrazione delle società che applicano il King III è richiesto di esprimere un giudizio di adeguatezza del sistema di controllo interno e di gestione dei rischi. A tale scopo¹⁷, il King III prevede il coordinamento tra le funzioni di controllo e in generale tra tutte le funzioni che svolgono attività di *assurance* (cosiddetto “*combined assurance model*”) e in particolare che:

- il *management* provveda a garantire l'integrazione del sistema dei controlli interni nelle attività dell'impresa;
- l'*internal audit* emetta una relazione sull'adeguatezza del Sistema di Controllo Interno e di Gestione dei Rischi e sui *financial controls*¹⁸;
- un soggetto indipendente effettui una valutazione di adeguatezza dei controlli IT¹⁹;
- il Consiglio riceva dal *management* o dalla funzione compliance un giudizio di adeguatezza dei controlli inerenti il rispetto di leggi, regole, codici e altri *standard*²⁰.

¹⁶ Si riporta il testo in lingua originale: “*It is the role of management to implement and take day-to-day responsibility for board policies on risk management and internal control. But the board needs to satisfy itself that management has understood the risks, implemented and monitored appropriate policies and controls, and are providing the board with timely information so that it can discharge its own responsibilities. In turn, management should ensure internal responsibilities and accountabilities are clearly established, understood and embedded at all levels of the organization. Employees should understand their responsibility for behaving according to the culture.*”

¹⁷ King Code of Corporate Governance (2009) 4.9. - *The board should receive assurance regarding the effectiveness of the risk management process.*

¹⁸ King Code of Corporate Governance (2009) 7.3.5 - *Internal audit should provide a written assessment of the system of internal controls and risk management to the board; King Code of Corporate Governance (2009) 7.3.6 - Internal audit should provide a written assessment of internal financial controls to the audit committee.*

¹⁹ King Code of Corporate Governance (2009) 5.1.5 - *The board should receive independent assurance on the effectiveness of the IT internal controls.*

²⁰ King Code of Corporate Governance (2009) 6.4.2 - *The board should receive assurance on the effectiveness of the controls around compliance with laws, rules, codes and standards.*

5. Il gruppo di imprese

Con riferimento al tema del *risk oversight* nell'ambito di un gruppo di imprese, l'approccio aziendalistico è diretto ad una migliore allocazione ed utilizzo delle risorse all'interno del gruppo per le finalità strategiche complessive, nonché a ridurre le possibilità di sovrapposizione o confusione di compiti e di responsabilità del consiglio di amministrazione della controllante e delle controllate, tenuto conto del bilanciamento degli interessi delle società che vi partecipano.

Anche sotto questo profilo la normativa primaria di riferimento forma un quadro non esauriente. In presenza di rilevanti rischi di una controllata è opportuno infatti considerare anche la responsabilità concorrente del *management* e del Consiglio di Amministrazione della controllante per la tutela del valore dell'*asset* aziendale a rischio rappresentato dalla partecipazione nella società controllata.

Ciò comporta un'incerta allocazione di compiti e responsabilità tra Consiglio di Amministrazione della controllante e Consiglio di Amministrazione delle controllate per la gestione dei rischi della controllata. Ad esempio, il rischio di produrre rendiconti incompleti ed inaccurati è connesso all'obiettivo di *compliance* normativa di competenza del Consiglio di Amministrazione della controllata, pur rimanendo comunque anche obiettivo di *reporting* della controllante, quanto meno ai fini di gestione del *business* di gruppo.

Il tema del necessario coordinamento di ruoli e responsabilità nell'ambito della gestione dei rischi di gruppo è stato affrontato nel Codice di Autodisciplina di Borsa Italiana adottando una soluzione che prevede la responsabilità del Consiglio di Amministrazione della capogruppo in alcuni "passaggi-chiave":

- nell'esame ed approvazione dei piani strategici, industriali e finanziari dell'emittente e del gruppo di cui esso sia a capo, monitorandone periodicamente l'attuazione, e definendo la natura e il livello di rischio compatibile con gli obiettivi strategici dell'emittente;
- nella valutazione dell'adeguatezza dell'assetto organizzativo, amministrativo e contabile dell'emittente nonché quello delle controllate aventi rilevanza strategica, con particolare riferimento al sistema di controllo interno e di gestione dei rischi;
- nel deliberare in merito alle operazioni dell'emittente e delle sue controllate, quando tali operazioni abbiano un significativo rilievo strategico, economico, patrimoniale o finanziario per l'emittente stesso, stabilendo criteri generali per individuare le operazioni di significativo rilievo;
- nel definire le linee di indirizzo del sistema di controllo interno e di gestione dei rischi, in modo che i principali rischi afferenti all'emittente e alle sue controllate risultino correttamente identificati, nonché adeguatamente misurati, gestiti e monitorati, determinando inoltre il grado di compatibilità di tali rischi con una gestione dell'impresa coerente con gli obiettivi strategici individuati;
- nel valutare, con cadenza almeno annuale, l'adeguatezza del sistema di controllo interno e di gestione dei rischi rispetto alle caratteristiche dell'impresa e al profilo di rischio assunto, nonché la sua efficacia. Tali aspetti si riferiscono all'impresa, e non in senso più restrittivo all'emittente, e quindi comprendono anche le società controllate.

A tali responsabilità si accompagnano quelle attribuite dal Consiglio di Amministrazione all'Amministratore Incaricato del Sistema di Controllo Interno e di Gestione dei Rischi di curare l'identificazione dei principali rischi aziendali, tenendo conto delle caratteristiche delle attività svolte dall'emittente e dalle sue controllate, e di sottoporli periodicamente all'esame del Consiglio di Amministrazione nonché di dare esecuzione alle linee di indirizzo definite dal Consiglio di Amministrazione, curando la progettazione, realizzazione e gestione del Sistema di Controllo Interno e di Gestione dei Rischi e verificandone costantemente l'adeguatezza e l'efficacia anche in funzione delle dinamiche delle condizioni operative e del panorama legislativo e regolamentare.

Come meglio dettagliato nel Capitolo V del presente Quaderno, anche la valutazione del SCIGR deve essere svolta non soltanto con riferimento all'emittente, ma anche con riferimento alle controllate aventi rilevanza strategica, identificate anche sulla base del *business plan* del gruppo. La valutazione in merito alla rilevanza delle società è lasciata all'Emittente che può utilizzare criteri sia qualitativi (es. rilevanza del business della società controllata rispetto agli obiettivi strategici del Gruppo) che quantitativi (es. ricavi, EBITDA, utile ante imposte, *transfer price*).

La prassi organizzativa generalizzata, in Italia, prevede in questi casi una struttura c.d. «a matrice», contraddistinta dalla previsione di plurimi riporti organizzativi, di tipo funzionale e di tipo gerarchico, all'interno del gruppo economico e societario. Con tale organizzazione, il *management* delle società controllate è sottoposto, per la gestione dei rischi, tanto a direttive di tipo gerarchico e funzionale emanate dagli organi societari della società controllata di appartenenza quanto a direttive di tipo c.d. funzionale impartite dal *management* della società controllante.

Pur in presenza di una pluralità di modalità applicative del modello «a matrice», che rendono impossibile tipicizzare la struttura ideale di riferimento, le sue caratteristiche di fondo possono essere sintetizzate così:

- il controllo di tipo funzionale è principalmente presente nelle attività strategiche di business di gruppo (quali le vendite, la produzione e gli acquisti) e viene esercitato dalla controllante mediante disposizioni e controlli di tipo preventivo (statuizione di principi e modalità di gestione dei rischi, criteri applicativi, metodologie e standard operativi, sistemi e flussi informativi, etc.), nonché mediante controlli successivi, quali la supervisione, l'analisi delle *performance* e l'*internal audit*;
- alcune attività possono essere svolte centralmente dalla controllante per conto delle società controllate (ad es. finanza ed amministrazione, ricerca e sviluppo, sistemi informatici, servizi fiscali e legali, etc.), anche mediante contratti di *service* infragruppo, per realizzare economie di scala oppure per gestire centralmente alcune tipologie di rischi;
- a fronte dei potenziali conflitti organizzativi (ad es. in materia di allocazione delle risorse) tra il *management* della controllante e quello delle società controllate, i meccanismi risolutivi possono assumere la forma di strutture collegiali di coordinamento (es. comitati), a composizione mista.

CAPITOLO II

PRESIDI DI GOVERNANCE E DI CONTROLLO: MODALITÀ DI COORDINAMENTO E FLUSSI INFORMATIVI VERSO IL BOARD

1. Attori del Sistema di Controllo Interno e Gestione dei Rischi - 1.1. Il ruolo del *Board* - 1.2. Il ruolo del Collegio Sindacale - 1.3. Il ruolo dell'*Internal Audit* e del suo Responsabile - 1.4. Il ruolo del Dirigente Preposto alla redazione dei documenti contabili societari - 1.5. Il ruolo del *Chief Risk Officer* - 1.6. Il ruolo del Comitato Controllo e Rischi - 1.7. Il ruolo dell'Amministratore Incaricato del Sistema di Controllo Interno e Gestione dei Rischi - 2. L'importanza dei flussi informativi - 2.1 Assunzioni di fondo e direzione strategica - 2.2 Individuazione della soglia di tolleranza e dell'appetito al rischio - 2.3 Aggregazione ed integrazione dei rischi - 3. Modelli di presidio del rischio - 4. I ruoli all'interno dei gruppi

1. Attori del Sistema di Controllo Interno e Gestione dei Rischi

Come sottolineato, il SCIGR è noto come l'insieme delle regole, delle procedure e delle strutture organizzative volte a consentire l'identificazione, la misurazione, la gestione e il monitoraggio dei principali rischi (Codice di autodisciplina, Principio 7.P.1.); il suo efficace ed efficiente funzionamento necessita di idonei presidi organizzativi.

Gli attori del SCIGR, intesi in senso ampio come Organi, Comitati e Funzioni Aziendali, sono:

- il Consiglio di Amministrazione, il quale svolge un ruolo di indirizzo e di valutazione dell'adeguatezza del SCIGR;
- il Collegio Sindacale, che vigila sul rispetto dei principi di corretta amministrazione ed in particolare sull'adeguatezza dell'assetto organizzativo, amministrativo e contabile ai sensi dell'art. 2403 cod. civ.;
- il Comitato per il controllo interno e per la revisione contabile ai sensi dell'art. 19 del D.Lgs. 39/2010, tenuto a vigilare su: i) processo di informativa finanziaria; ii) l'efficacia dei sistemi di controllo interno, di revisione interna, e di gestione del rischio; iii) la revisione legale dei conti annuali e dei conti consolidati; iv) l'indipendenza del revisore legale o della società di revisione legale, in particolare per quanto concerne la prestazione di servizi non di revisione all'ente sottoposto alla revisione legale dei conti. Tale ruolo è attribuito dalla regolamentazione primaria nazionale all'organo di controllo, identificato in funzione del modello di governo adottato;
- la Funzione di *Internal Audit* ed il suo Responsabile, che hanno l'obiettivo di verificare che il SCIGR sia funzionante e adeguato;
- il Dirigente Preposto alla redazione dei documenti contabili societari, nominato dalle società quotate o dagli emittenti di strumenti finanziari diffusi, ai sensi dell'art. 154-*bis* del TUF, che ha la responsabilità di rilasciare le attestazioni e le dichiarazioni relative ai bilanci annuali, semestrali, trimestrali ed alla comunicazione delle informazioni *price sensitive*;
- gli altri ruoli e funzioni aziendali, con specifici compiti in tema di controllo interno e gestione dei rischi (es. Organismo di Vigilanza ex D.Lgs. 231/2001, *Risk Management*, *Compliance*, Comitati manageriali, etc.)²¹.

²¹ Codice di Autodisciplina, Commento all'art. 7 – Sistema di Controllo Interno e di gestione dei rischi: “Un ruolo di particolare rilevanza nell'ambito del sistema di controllo interno e di gestione dei rischi è normalmente ricoperto dalle funzioni legali e di *compliance*, con particolare riferimento al presidio del rischio legale e di non conformità, ivi incluso anche il rischio della commissione di illeciti penali a danno e nell'interesse dell'azienda.”

Inoltre, il *Board* può individuare al proprio interno:

- un Comitato Controllo e Rischi, con il compito di supportare con un'adeguata attività istruttoria, le valutazioni e le decisioni del *Board* relative al SCIGR, nonché quelle relative all'approvazione delle relazioni finanziarie periodiche (Codice di Autodisciplina, Principio 7.P.3, a), (ii));
- uno o più amministratori incaricati (questa figura generalmente corrisponde all'Amministratore Delegato) dell'istituzione e del mantenimento di un efficace SCIGR (Codice di Autodisciplina Principio 7.P.3, a), (i)). L'amministratore incaricato del SCIGR può coinvolgere il *Management* aziendale e può inoltre avvalersi di strutture totalmente dedicate (es. *Chief Risk Officer*) in casi di particolare complessità organizzativa e del profilo di rischio assunto.

Premesso che le società quotate aderiscono volontariamente al Codice di Autodisciplina ovvero documentano le motivazioni che hanno portato alla disapplicazione dei relativi principi (approccio "*comply or explain*"), si ritiene che le soluzioni organizzative previste possano costituire un valido riferimento anche per le aziende di maggiori dimensioni, seppur non quotate. Qualora invece non si ritenesse necessario o opportuno dotarsi di una struttura così articolata, i compiti e le responsabilità delegati ai Comitati ricadrebbero direttamente sul *Board*.

1.1. Il ruolo del *Board*

Con riferimento al ruolo e alle responsabilità del *Board*, esse risultano definite dalla normativa primaria e secondaria, dai requisiti di autodisciplina e dalle *leading practice* come ampiamente descritti nel Capitolo I. Tuttavia, ai fini del presente Capitolo, occorre sottolineare la cruciale importanza del ruolo del *Board* nel cosiddetto *oversight* dei rischi attraverso l'indirizzo strategico e la supervisione dei compiti e dei contributi di competenza degli altri "attori" del SCIGR, come descritti di seguito.

La centralità dell'organo di governo strategico nella definizione della strategia imprenditoriale è generalmente riconosciuta nei principali *framework* di controllo interno e di *risk management*. In particolare, secondo i principi dell'OECD²² in materia di *corporate governance*, il *Board* è responsabile dell'effettivo monitoraggio delle attività manageriali e del modello di *corporate governance*, rispondendo all'impresa e agli *stakeholder*.

Essi prevedono che: "*The corporate governance framework should ensure the strategic guidance of the company, the effective monitoring of management by the Board and the Board accountability to the company and to the shareholders*". Sempre secondo i medesimi principi, l'organo di governo strategico – *Board* – è chiamato a:

- "*Reviewing and guiding corporate strategy, major plans of action risk management policies and procedures, annual budgets and business plans*;
- *setting performance objectives*;
- *monitoring implementation and corporate performance*; and
- *overseeing major capital expenditures, acquisitions and divestitures*".

²² Cfr. G20/OECD *Principles of Corporate Governance*, September 2015.

Ed ancora, il *Financial Stability Board* prevede nelle c.d. “*Sound risk governance practice*” che l’organo di governo strategico – *Board*:

- definisca l’ambiente di controllo interno (*tone at the top*) e si preoccupi di trasmettere efficacemente nell’organizzazione d’impresa una adeguata cultura di gestione dei rischi ad ogni livello;
- sia responsabile di vigilare (*overseeing*) l’efficace implementazione da parte del *management* di un modello onnicomprensivo di gestione dei rischi e delle *policies* relative;
- approvi la propensione al rischio dell’impresa (*risk appetite*) e si assicuri che essa sia direttamente riflesso nella strategia aziendale, nell’utilizzo del capitale, nei piani finanziari e nelle remunerazioni.

Su tali basi, l’organo di governo strategico dovrà quindi approvare un modello di gestione e di *governance* dei rischi (*corporate risk management framework*) che, per ciascuna categoria di rischio rilevante, identifichi la strategia e le modalità di gestione previste (obiettivi di gestione, standard e metodologie di gestione), il limite di rischio ottimale (*risk appetite*) ed il limite di rischio massimo tollerabile – *risk tolerance*.

Infine, in base al CoSO Report, “*the Board of Directors retains oversight responsibility for management’s design, implementation and conduct of internal control*”; pertanto, l’organo di governo, quale “*process owner*” del sistema di controllo interno, riceve la responsabilità propria, eventualmente delegabile a uno o più amministratori al suo interno, di definire alcuni importanti aspetti, tra i quali, in base al modello CoSO Report, quelli di:

- definire le aspettative e valutare le *performance*, l’integrità ed i valori etici degli organi delegati alla gestione;
- stabilire la struttura e le modalità di esercizio della propria vigilanza coerentemente agli obiettivi d’impresa;
- considerare i fattori di rischio esterni ed interni che influenzano il raggiungimento o la sostenibilità nel tempo degli obiettivi d’impresa;
- valutare la capacità dell’impresa di identificare i rischi collegati all’innovazione ed ai cambiamenti;
- interrogare il *management* in merito alle specifiche decisioni prese in materia di sviluppo, selezione ed implementazione delle attività di controllo in senso stretto;
- comunicare nell’organizzazione d’impresa le aspettative etico comportamentali;
- discutere con i revisori interni ed esterni le valutazioni in merito all’allineamento tra le strategia d’impresa, le evoluzioni di mercato e d’ambiente, gli obiettivi specifici ed i connessi rischi con le relative implicazioni di controllo interno.

Nello svolgere i suoi compiti, l’organo di governo, coadiuvandosi anche con ulteriori organi di controllo interno che svolgono funzioni di monitoraggio, può avvalersi del supporto di alcuni comitati, secondo quanto definito dal contesto di riferimento (es. il Comitato Controllo e Rischi disciplinato dal Codice di Autodisciplina).

²³ Art. 2403 cod. civ.: “Il Collegio Sindacale vigila sull’osservanza della legge e dello statuto, sul rispetto dei principi di corretta amministrazione ed in particolare sull’adeguatezza dell’assetto organizzativo, amministrativo e contabile adottato dalla società sul suo concreto funzionamento.”

1.2. Il ruolo del Collegio Sindacale

Il Collegio Sindacale ricopre un ruolo primario nel sistema di vigilanza di una Società, come si evince dalle disposizioni riportate nel Codice Civile (artt. 2403²³ e segg.) e dal Testo Unico della Finanza (art. 149²⁴).

Nel definire le modalità di esercizio del proprio ruolo, il Collegio Sindacale pianifica le attività da eseguire, sulla base della rilevanza dei rischi aziendali indicati nei flussi informativi ricevuti dai vari attori del SCIGR tenendo in considerazione le dimensioni, la complessità e le altre caratteristiche, anche organizzative, della società. Tenuto conto dell'ambito di intervento del Collegio Sindacale, l'attività di vigilanza è fondata sull'analisi del rischio (*risk approach*).

L'attività di vigilanza viene quindi svolta sulla base dei flussi informativi acquisiti dal Collegio Sindacale, con particolare riferimento a quelli forniti dalle funzioni aziendali con specifici compiti in tema di controllo interno e gestione dei rischi. Detti flussi informativi devono consentire al Collegio Sindacale di pianificare la propria attività in funzione della rilevanza dei rischi aziendali, così come risultanti dalla documentazione acquisita. Il patrimonio informativo reso disponibile deve essere esaminato e valutato, attraverso la competenza e l'esperienza professionale²⁵.

Ai sensi delle norme comportamentali di riferimento per l'Organo di Controllo, laddove l'attività di vigilanza dovesse evidenziare rischi significativi, il Collegio Sindacale richiede all'Amministratore Delegato l'adozione di un piano di azioni correttive di cui monitora la realizzazione nel corso dell'incarico; nel caso in cui rilevi il permanere delle criticità ne informa il *Board* affinché adotti i necessari provvedimenti.

Il Collegio Sindacale scambia con il Comitato Controllo e Rischi, ove nominato, le informazioni rilevanti per l'espletamento dei rispettivi compiti di vigilanza.

Alle valutazioni sul sistema di controllo interno e di gestione dei rischi effettuate dal Consiglio di Amministrazione si affianca anche la valutazione da parte del Collegio Sindacale "sull'efficacia dei sistemi di controllo interno, di revisione interna, se applicabile, e di gestione del rischio", secondo quanto previsto all'art. 19 dal D.Lgs. 39/2010, e la valutazione "sull'adeguatezza della struttura organizzativa della società per gli aspetti di competenza, del sistema di controllo interno e del sistema amministrativo-contabile nonché sull'affidabilità di quest'ultimo nel rappresentare correttamente i fatti di gestione", secondo quanto previsto dall'art. 149, comma 1, lettera c) del TUF.

L'organo di controllo nello svolgimento dei propri compiti si avvale, analogamente al Consiglio di Amministrazione, di appositi flussi informativi a supporto provenienti dalle funzioni di controllo interno e, per le attività svolte delle società controllate, acquisisce e scambia informazioni con gli organi amministrativi e di controllo di queste ultime.

Tali valutazioni sono espresse da parte del Collegio Sindacale, ai sensi dell'art. 153 del TUF, nella relazione trasmessa all'assemblea dei Soci convocata per l'approvazione del bilancio, e solo successivamente alle delibere del Consiglio di Amministrazione in merito alla valutazione dell'assetto organizzativo amministrativo e contabile e alla valutazione del Sistema di Controllo Interno e di Gestione dei Rischi.

²⁴ Art. 149 del TUF: "Il Collegio Sindacale vigila:

- a) sull'osservanza della legge e dell'atto costitutivo;
- b) sul rispetto dei principi di corretta amministrazione;
- c) sull'adeguatezza della struttura organizzativa della società per gli aspetti di competenza, del sistema di controllo interno e del sistema amministrativo contabile nonché sull'affidabilità di quest'ultimo nel rappresentare correttamente i fatti di gestione;

c-bis) sulle modalità di concreta attuazione delle regole di governo societario previste da codici di comportamento redatti da società di gestione di mercati regolamentati o da associazioni di categoria, cui la società, mediante informativa al pubblico, dichiara di attenersi 737;

d) sull'adeguatezza delle disposizioni impartite dalla società alle società controllate ai sensi dell'articolo 114, comma 2."

²⁵ CNDCEC, "Norme di comportamento del Collegio Sindacale di Società quotate" del 15 aprile 2015.

CNDCEC, "Principi di comportamento del Collegio sindacale di società non quotate" del 21 settembre 2015.

1.3. Il ruolo dell'*Internal Audit* e del suo Responsabile

L'*Internal Audit* è una funzione indipendente, non coinvolta nella gestione del *business*, che ha il compito primario di verificare che il SCIGR sia funzionante, adeguato e rispetti le normative vigenti e le procedure aziendali. Il Responsabile della funzione di *Internal Audit* dovrebbe dipendere gerarchicamente dal *Board* e non essere responsabile di alcuna area operativa.

E' opportuno che il Responsabile della funzione di *Internal Audit* rediga un piano di *audit* «*risk based*», fondato su un processo strutturato di analisi e prioritizzazione dei principali rischi; tale piano diventa vincolante una volta approvato dal *Board*, sentito il Collegio Sindacale. Il piano di *audit* costituisce lo strumento attraverso cui la funzione di *Internal Audit* verifica in via continuativa l'operatività e l'adeguatezza del sistema di controllo interno e di gestione dei rischi. La funzione di *Internal Audit* può effettuare specifiche verifiche anche su richiesta del Comitato Controllo e Rischi e del Collegio Sindacale, nonché su apposita richiesta dei vertici aziendali (ad es. l'Amministratore Delegato che, in alcuni casi, coincide con l'Amministratore Incaricato del SCIGR, come dettagliato più avanti).

Inoltre, il Responsabile dovrebbe rendicontare periodicamente al *Board* l'attività svolta dalla funzione, fornendo anche informazioni sull'adeguatezza dell'operatività e dell'idoneità del SCIGR, nonché sul rispetto del piano di *audit* definito; è tenuto a procedere altresì a comunicare tempestivamente al *Board* in merito ad eventi di particolare rilevanza nell'esercizio dei suoi compiti.

1.4. Il ruolo del Dirigente Preposto alla redazione dei documenti contabili societari

Il Dirigente Preposto alla redazione dei documenti contabili societari è responsabile, nell'ambito del sistema di controllo amministrativo e contabile, di predisporre procedure amministrativo-contabili per la formazione del bilancio nonché di altre comunicazioni di carattere finanziario (come previsto dall'art. 154-*bis* TUF²⁶) e di svolgere periodiche verifiche sull'efficacia operativa dei controlli a supporto del processo di attestazione dell'informativa finanziaria verso i soci, i terzi ed il mercato.

Il Dirigente Preposto supporta il Consiglio di Amministrazione nel processo di formazione del bilancio e di ogni altra comunicazione di tipo finanziario, garantendo allo stesso la correttezza e veridicità dei dati contabili in esso contenuti. In occasione dell'emissione del bilancio d'esercizio, del bilancio semestrale abbreviato nonché del bilancio consolidato, il Dirigente Preposto, unitamente agli organi amministrativi delegati, è chiamato ad emettere una relazione che attesti, tra le altre cose, l'adeguatezza e l'effettiva applicazione delle procedure amministrativo-contabili, la conformità dei documenti ai principi contabili internazionali, l'idoneità dei documenti a fornire una rappresentazione veritiera e corretta della situazione patrimoniale, economica e finanziaria dell'emittente²⁷.

²⁶ Art. 154-*bis*, comma 3 TUF – Il Dirigente preposto predisporre adeguate procedure amministrative e contabili per la formazione del bilancio di esercizio e, ove previsto, del bilancio consolidato nonché di ogni altra comunicazione di carattere finanziario.

²⁷ Art. 154-*bis*, comma 5 TUF: "Gli organi amministrativi delegati e il dirigente preposto alla redazione dei documenti contabili societari attestano con apposita relazione sul bilancio di esercizio, sul bilancio semestrale abbreviato e, ove redatto, sul bilancio consolidato: a) l'adeguatezza e l'effettiva applicazione delle procedure di cui al comma 3 nel corso del periodo cui si riferiscono i documenti; b) che i documenti sono redatti in conformità ai principi contabili internazionali applicabili riconosciuti nella Comunità europea ai sensi del regolamento (CE) n. 1606/2002 del Parlamento europeo e del Consiglio, del 19 luglio 2002; c) la corrispondenza dei documenti alle risultanze dei libri e delle scritture contabili; d) l'idoneità dei documenti a fornire una rappresentazione veritiera e corretta della situazione patrimoniale, economica e finanziaria dell'emittente e dell'insieme delle imprese incluse nel consolidamento; e) per il bilancio d'esercizio e per quello consolidato, che la relazione sulla gestione comprende un'analisi attendibile dell'andamento e del risultato della gestione, nonché della situazione dell'emittente e dell'insieme delle imprese incluse nel consolidamento, unitamente alla descrizione dei principali rischi e incertezze cui sono esposti; f) per il bilancio semestrale abbreviato, che la relazione intermedia sulla gestione contiene un'analisi attendibile delle informazioni di cui al comma 4 dell'articolo 154-*ter*."

Si aggiunge inoltre in capo al Consiglio di Amministrazione l'onere di vigilare affinché il Dirigente Preposto alla redazione dei documenti contabili societari disponga di adeguati poteri e mezzi per l'esercizio dei compiti a lui attribuiti nonché sull'effettivo rispetto delle procedure amministrativo-contabili dallo stesso predisposte²⁸.

1.5. Il ruolo del *Chief Risk Officer*

In relazione alla complessità organizzativa ed al profilo di rischio aziendale, il presidio continuativo dei processi di analisi oltre alla necessità di aggregazione e *reporting* dei rischi potrebbero rendere opportuna l'istituzione di una figura o struttura dedicata non direttamente coinvolta nel *business* e diversa dalla funzione di *Internal Audit*. Esso rappresenta l'elemento di sintesi per il *Board* e l'Amministratore Delegato ovvero l'Amministratore Incaricato del SCIGR, contribuendo alla diffusione della cultura del rischio nell'organizzazione e portando contestualmente un punto di vista "obiettivo" sul profilo di rischio aziendale e sull'efficacia delle azioni/contromisure intraprese.

La nomina del *Chief Risk Officer* è più opportuna in realtà aziendali con particolare complessità organizzativa ed aventi un profilo di rischio elevato, per cui potrebbe rendersi necessario prevedere una struttura dedicata con competenze specialistiche, che vada ad integrare i risultati delle attività svolte da altre funzioni coinvolte.

Il *Chief Risk Officer* può fornire un punto di vista finalizzato a valutare i fenomeni in una prospettiva complessiva aziendale, intervenendo nella definizione delle scelte di *mitigation* ed a supporto dell'individuazione delle strategie, nonché fungere da collettore tra gli *owners* dei rischi, le funzioni di presidio del rischio dedicate (*Compliance, Credit, Financial, Operational Risk Management*) ed il *Board* o Comitato Controllo e Rischi, attraverso un'attività di coordinamento e supporto al *management* in sede di valutazione dei rischi, di aggregazione e consolidamento dei risultati del *riskassessment* e di individuazione delle strategie e delle azioni di risposta ad essi associati.

Tale soggetto non si occupa necessariamente della gestione di specifici rischi ma è il responsabile della gestione e dell'implementazione del processo di *risk management* integrato e di conseguenza è il soggetto più adatto a supportare l'attività di *risk oversight* del Consiglio di Amministrazione. Il ruolo del *Chief Risk Officer* dovrebbe essere quello di analizzare i differenti rischi identificati dalle unità operative e successivamente presentare una valutazione complessiva su questi temi al Consiglio di Amministrazione. Inoltre il *Chief Risk Officer* (d'ora in avanti anche CRO) fornisce supporto, ad alto livello, nella diffusione della *risk culture*, anche attraverso strumenti, tecniche e conoscenze necessarie all'attuazione del processo di gestione dei rischi all'interno della società. Proprio per questo suo ruolo di "alto livello" il CRO dovrebbe avere accesso diretto al Consiglio di Amministrazione e dovrebbe confrontarsi periodicamente con l'Amministratore Delegato, ovvero con il *Chief Executive Officer* (d'ora in avanti anche CEO) in modo da poter tempestivamente riportare eventuali eventi, comportamenti o elementi che potrebbero pregiudicare il corretto andamento dell'operatività societaria.

Al fine di perseguire tali finalità, il *Chief Risk Officer* partecipa di norma, ove costituiti, ai Comitati interni di gestione (es: Comitato di Direzione, Comitato Prodotti, Comitato Investimenti, etc.), peraltro con l'obiettivo di valutare i possibili impatti – in termini di esposizione ai rischi – delle varie tematiche oggetto di discussione collegiale all'interno di tali organismi; in particolare, a tali organismi è attribuito il compito di dare indicazioni e impulso a orientamenti condivisi che contemperino i diversi interessi presenti all'interno della Società e del Gruppo, assumendo – nei limiti delle facoltà eventualmente conferite – le necessarie determinazioni.

²⁸ Art. 154-bis, comma 4 TUF: "Il Consiglio di Amministrazione vigila affinché il dirigente preposto alla redazione dei documenti contabili societari disponga di adeguati poteri e mezzi per l'esercizio dei compiti a lui attribuiti ai sensi del presente articolo, nonché sul rispetto effettivo delle procedure amministrative e contabili".

1.6. Il ruolo del Comitato Controllo e Rischi

Tra i Comitati endo-consiliari con funzioni propositive e consultive nei confronti del *Board*, la cui costituzione è suggerita dal Codice di Autodisciplina²⁹, un ruolo importante nell'ambito del SCIGR è svolto dal Comitato Controllo e Rischi. Esso è composto da amministratori indipendenti o da amministratori non esecutivi in maggioranza indipendenti.

Il Comitato Controllo e Rischi ha il compito di supportare il *Board* mediante un'adeguata attività istruttoria, rilasciando tra l'altro pareri su specifici aspetti inerenti l'identificazione dei principali rischi aziendali a seguito dell'esame sulle relazioni finanziarie periodiche aventi per oggetto la valutazione del SCIGR. In particolare, il Comitato Controllo e Rischi, nell'assistere il Consiglio di Amministrazione:

- valuta, unitamente al Dirigente Preposto alla redazione dei documenti contabili societari e sentiti il revisore legale e il Collegio Sindacale, il corretto utilizzo dei principi contabili e, nel caso di gruppi, la loro omogeneità ai fini della redazione del bilancio consolidato;
- esprime pareri su specifici aspetti inerenti alla identificazione dei principali rischi aziendali;
- esamina le relazioni periodiche, aventi per oggetto la valutazione del sistema di controllo interno e di gestione dei rischi, e quelle di particolare rilevanza predisposte dalla funzione di *Internal Audit*;
- monitora l'autonomia, l'adeguatezza, l'efficacia e l'efficienza della funzione di *Internal Audit*;
- può chiedere alla funzione di *Internal Audit* lo svolgimento di verifiche su specifiche aree operative, dandone contestuale comunicazione al presidente del Collegio Sindacale;
- riferisce al *Board*, almeno semestralmente, in occasione dell'approvazione della relazione finanziaria annuale e semestrale, sull'attività svolta nonché sull'adeguatezza del sistema di controllo interno e di gestione dei rischi.

Il Comitato svolge anche un'intensa attività di verifica dell'autonomia, dell'adeguatezza, dell'efficacia e dell'efficienza della funzione di *Internal Audit*, potendo anche richiedere a quest'ultima, lo svolgimento di verifiche su specifiche aree operative o processi aziendali.

1.7. Il ruolo dell' Amministratore Incaricato del Sistema di Controllo Interno e Gestione dei Rischi

Ulteriore figura nominata dal *Board* è l'Amministratore Incaricato del SCIGR, normalmente coincidente con un Amministratore Delegato, che cura l'identificazione dei principali rischi aziendali, in coerenza con le caratteristiche delle attività svolte dalla Società e dalle sue controllate, e li sottopone periodicamente all'esame del *Board*.

L'Amministratore Incaricato, secondo le previsioni del Codice di Autodisciplina, provvede a dare esecuzione alle linee di indirizzo definite dal *Board*:

- curando la progettazione, la realizzazione e la gestione del SCIGR;
- verificandone costantemente l'adeguatezza e l'efficacia;
- adattandolo alla dinamica delle condizioni operative e del panorama legislativo e regolamentare.

²⁹ Cfr. Codice di Autodisciplina, art. 5 Comitato Nomine, art. 6 Comitato Remunerazione, art. 7 Comitato Controllo e Rischi.

Come il Comitato Controllo e Rischi, anche l'Amministratore Incaricato svolge un'attività di monitoraggio sulla funzione di *Internal Audit*, potendo chiedere a quest'ultima lo svolgimento di verifiche su specifiche aree operative e sul rispetto delle procedure interne nell'esecuzione di operazioni aziendali; qualora siano rilevate problematiche o criticità, riferisce tempestivamente al Comitato Controllo e Rischi.

L'Amministratore Incaricato del SCIGR, a sua volta, può coinvolgere il management aziendale e può avvalersi di funzioni totalmente dedicate, quali il *Chief Risk Officer*.

2. L'importanza dei flussi informativi

Una delle maggiori difficoltà attualmente affrontate dagli attori della *corporate governance* riguarda la qualificazione e la quantificazione (livello di dettaglio, periodicità, ecc.) dei flussi di informazioni in favore sia del Consiglio di Amministrazione, in qualità di organo collegiale responsabile della gestione, sia degli amministratori singolarmente considerati. Essi infatti hanno il dovere di agire informati sulla base delle informazioni che ottengono o che, quando necessario (ad esempio, in presenza di indicatori di rischio, anomalie, etc.), dovranno richiedere agli organi delegati e che gli stessi dovranno periodicamente fornire al Consiglio di Amministrazione.

Su tali basi, adeguati flussi informativi rappresentano il fulcro del SCIGR, in quanto permettono di assicurare il tempestivo controllo delle esposizioni ai rischi e la conseguente gestione delle anomalie riscontrate; è auspicabile che i flussi informativi consentano anche di ottenere una visione organica ed integrata degli esiti delle attività di controllo sui rischi; a tal fine, questi saranno veicolati in modo da consentire valutazioni complessive sulla gestione del rischio all'interno del SCIGR e sui processi di mitigazione, prevedendo lo sviluppo di idonei meccanismi di interazione, nonché di un complesso strutturato di contributi e di flussi informativi tra gli organi di gestione e gli organi e le funzioni con compiti di controllo.

Appare necessario sottolineare altresì come la criticità del tema sia stata affrontata anche nel Codice di Autodisciplina laddove esso prevede, nel paragrafo 5.C.1, la facoltà del Comitato Controllo e Rischi, ma non dei singoli amministratori, di ottenere informazioni anche direttamente dalle funzioni aziendali e di avvalersi di consulenti esterni.

In sostanza, la disponibilità di sistematici, rilevanti, esaurienti ed affidabili flussi informativi rivolti al Consiglio di Amministrazione ed al Comitato Controllo e Rischi è un cruciale aspetto di *corporate governance* e di controllo interno delle imprese, soprattutto se di grandi dimensioni e complessità.

Per tali motivi, tipologia, tempistica e modalità dei flussi informativi è bene che siano definiti in via preventiva nella definizione del *framework* di controllo interno. L'esigenza complessiva è sicuramente quella di rafforzare la comunicazione interna aumentando la trasparenza dei flussi informativi a tutti i livelli, ovvero diffondere una cultura del rischio e del controllo all'interno di tutta l'organizzazione³⁰.

In particolare, per permettere al Consiglio di Amministrazione ed al Comitato Controllo e Rischi di focalizzarsi sugli aspetti fondamentali, i flussi informativi in materia di SCIGR dovranno essere:

- opportunamente sintetici, assicurando una chiara ed univoca interpretazione;
- affidabili, ovvero che garantiscano l'accuratezza delle informazioni riportate;
- completi, ovvero che siano esaustivi ed includano tutti i dettagli necessari in funzione dei relativi destinatari;

³⁰ FRC, *Boards and Risk: A summary of discussions with companies, investors and advisers*, 2011; si veda in particolare par. "The Quality and Use of Information".

- tempestivi, in termini di tempistiche di predisposizione e alimentazione, assicurando che siano ricevuti nei tempi previsti;
- tracciabili, in termini di possibilità di riconduzione alle relative fonti;
- comparabili, affinché permettano di avere una visione olistica del perimetro di riferimento (tipologia di rischio, *business unit*, processi, società del Gruppo, etc.).

Ciascun attore coinvolto nell'attività di *risk reporting* dovrà pertanto assicurare che i flussi informativi siano qualitativamente adeguati, cosicché il sistema di gestione del rischio potrà funzionare correttamente e contribuire all'attuazione delle misure necessarie a garantire un'adeguata gestione e l'effettivo monitoraggio dei rischi.

A prescindere dal modello di presidio del rischio che la società adotta, è dunque necessario che i flussi informativi tra le strutture di controllo menzionate sopra siano chiaramente formalizzati in termini di contenuti, tempistiche e responsabilità delle diverse funzioni di controllo al fine di favorire una comunicazione efficace verso l'alta direzione, i comitati e gli organi sociali.

In particolare, il Consiglio di Amministrazione deve incentivare la definizione di un efficace *reporting* basato su processi strutturati per fornire adeguati flussi informativi, come di seguito dettagliati.³¹

2.1. Assunzioni di fondo e direzione strategica

Ogni piano a lungo a termine è basato su numerose assunzioni che includono la previsione di futuri *trend* di mercato, delle tecnologie che hanno impatto sulle attività e di molte altre variabili che inevitabilmente contengono un livello di incertezza più o meno elevato. È quindi necessario valutare la consistenza delle assunzioni di fondo su cui si basa il processo di definizione delle strategie e delle informazioni necessarie al monitoraggio dell'effettivo perseguimento, anche in termini di piani d'azione o di correzione. Di conseguenza, il *Board* deve disporre di reportistica adeguatamente strutturata e con l'opportuno livello di dettaglio informativo, affinché possa analizzarne il contenuto intervenendo laddove ritenga che le proposte pervenute siano particolarmente rischiose o non in linea con i limiti di rischio adottati.

Pertanto, il *management* dovrà integrare le proprie analisi ed indicazioni con tutti gli elementi necessari a comprendere le motivazioni alla base di ogni valutazione, le leve su cui agire e gli effetti presumibili, in modo da facilitare il *Board* nell'attuazione delle proprie responsabilità decisionali e deliberative.

2.2. Individuazione della soglia di tolleranza e dell'appetito al rischio

Spetta al Consiglio di Amministrazione determinare il livello di *risk tolerance* (soglia di tolleranza), ovvero la devianza massima consentita dal *risk appetite* (livello di rischio che la società intende assumere per il perseguimento dei suoi obiettivi). La soglia di tolleranza deve essere fissata in modo da assicurare in ogni caso alla società margini sufficienti per operare anche in condizioni di *stress*, cioè nei limiti della *risk capacity* (intesa come massimo rischio assumibile senza comportare la violazione di limiti di solidità patrimoniale e, ove previsti, dei requisiti regolamentari o di altri vincoli eventualmente imposti). A tal fine devono essere predisposti adeguati flussi informativi che consentano al Consiglio di Amministrazione di definire le soglie di *risk appetite* e *tolerance* relative ai principali rischi aziendali e attivare le conseguenti attività di monitoraggio per verificare il rispetto dei limiti identificati.

³¹ Si veda NACD, "Risk Governance: Balancing Risk and Reward", 2009.

2.3. Aggregazione ed integrazione dei rischi

I rischi individuati sono spesso presentati come esposizioni separate. Queste esposizioni, tuttavia, raramente possono essere analizzate in maniera autonoma e svincolata da un contesto più ampio, ma devono essere correlate tra loro, in quanto sono in grado di creare effetti a catena.

La mancanza di interrelazioni può rappresentare un ostacolo che non permette di pervenire ad una rappresentazione complessiva del rischio d'impresa.

Il *management* ha il compito e la responsabilità di sviluppare un processo di comprensione dell'impatto aggregato e olistico dei rischi sull'organizzazione. Tuttavia, oltre ad accertarsi che il *management* abbia sviluppato un processo che sia concretamente attuato ed efficiente, il Consiglio di Amministrazione svolge anche un ruolo fondamentale nel supervisionare e supportare il processo di identificazione delle interrelazioni tra i rischi.

Un approccio in tale direzione può essere rappresentato dalla chiara attribuzione di responsabilità di gestione di rischi specifici a figure/unità che operino in tutti i livelli dell'organizzazione e di cui siano misurate e valorizzate le relative performance. Nell'ambito di imprese di grande dimensione e/o di complessità organizzativa, al fine di migliorare e rendere realmente efficace il sistema di *reporting* aziendale sui rischi può divenire essenziale prevedere il ruolo del *Chief Risk Officer* il cui ruolo è stato descritto al precedente paragrafo 1.5.

3. Modelli di presidio del rischio

Dal punto di vista organizzativo è possibile individuare due modelli estremi di presidio del rischio, il Modello Centralizzato ed il Modello Decentrato. Le effettive applicazioni possono prevedere opportuni aggiustamenti e calibrature che determinano soluzioni "Miste". La scelta relativa all'applicazione dei modelli è legata alla complessità ed alla natura della singola Società. Di seguito una descrizione delle diverse opzioni e dei relativi vantaggi e punti d'attenzione.

Il Modello Centralizzato di presidio del rischio prevede che i ruoli e le responsabilità in ordine alla valutazione e gestione del rischio siano attribuiti ad una funzione accentrata di *risk management* che si ritiene possa risultare meglio attrezzata per definire e attuare una metodologia coerente e misure uniformi per supportare l'aggregazione dei rischi. Tale modello è riconducibile all'implementazione di un evoluto modello di *risk management – Enterprise Risk Management* – con eventuale nomina di un *Chief Risk Officer* o comunque di una figura di coordinamento.

Tale Modello può presentare alcuni vantaggi:

- politiche, metodologie, procedure e processi sono standardizzati facilitando l'aggregazione dei rischi e il *reporting*;
- tecniche di misurazione del rischio uniformi consentono un confronto diretto dei rischi per *business unit*, società del gruppo, tipologia di rischio, ecc., utili per creare un profilo di rischio a livello di gruppo;
- esistono chiare linee di comunicazione e responsabilità.

Tra i punti di attenzione di un Modello Centralizzato sono da considerare i seguenti:

- i rischi individuali delle *business unit* o società del gruppo variano e potrebbero non essere modellati accuratamente mediante l'utilizzo di un'unica metodologia;

- l'eventuale incapacità di identificare specifici livelli di rischio in specifici prodotti, funzioni o attività;
- il personale del *risk management* potrebbe non avere abbastanza familiarità con i rischi, a causa della relativa specificità, per permettere un'accurata identificazione e valutazione degli stessi.

Un Modello Centralizzato richiede sicuramente una disponibilità di risorse finanziarie e un buon sistema di *corporate governance*, nonché un'elevata frequenza dell'attività di *assessment* e di *reporting* oltre ad una rafforzata comunicazione delle politiche di assunzione del rischio. Ciò spiega come le società che adottano un tale sistema siano solitamente società di grandi dimensioni e con elevata complessità, normalmente operanti in settori regolamentati.

Il Modello Decentralizzato di presidio del rischio prevede ruoli e responsabilità in ordine alla valutazione e gestione del rischio attribuiti a unità organizzative specifiche e specializzate che, soprattutto per vicinanza alle rispettive operatività, si ritiene possano essere maggiormente in grado di selezionare e valutare le diverse tipologie di rischio. Tale modello può presentare i seguenti vantaggi:

- il personale delle *business unit* o Società del Gruppo è in una posizione migliore per valutare e selezionare i rischi;
- è presumibile una maggiore tempestività nel prendere decisioni che ottimizzano le *performance* individuali.

Tra i punti di attenzione di un Modello Decentrato possono essere citati i seguenti:

- le decisioni a “compartimenti stagni” possono compromettere il rispetto delle soglie di rischio complessive;
- può comportare la mancata analisi di correlazione dei rischi;
- persiste la necessità di assicurare comunque un'azione di coordinamento a valle, che risulterebbe più onerosa e meno efficace.

Il Modello Misto di presidio del rischio prevede che i ruoli e le responsabilità connessi alla valutazione e gestione del rischio, quali ad esempio la definizione del profilo di rischio complessivo della società, il relativo *reporting* al vertice aziendale e agli organi societari nonché il presidio diretto di alcune tipologie di rischi sono centralizzati; altre responsabilità rimangono decentralizzate, con presidi nelle funzioni di *business*. Un esempio di applicazione del Modello Misto potrebbe prevedere un *Chief Risk Officer* con il compito di definire le metodologie e gli strumenti a livello di gruppo, predisporre il reporting sui principali rischi per il vertice e gli organi societari e sovrintendere direttamente al monitoraggio dei rischi finanziari e industriali. Altre tipologie di rischio, quali ad esempio i rischi ambientali, i rischi di *compliance*, i rischi dei progetti di investimento, etc., potrebbero essere gestiti da presidi specialistici fuori dall'area di responsabilità del CRO che tuttavia svolgerebbe un ruolo di coordinamento metodologico, di monitoraggio e di *reporting* ai fini del consolidamento del portafoglio dei rischi.

Nella pratica, la soluzione che si ritiene debba essere perseguita in funzione della natura del *business*, della complessità dell'organizzazione, dello stile di *management*, delle caratteristiche delle risorse, ecc., è quella che consente:

- l'analisi fondata su conoscenze tecniche e competenze specialistiche;
- una visione e valutazione integrata sull'intero SCIGR;
- la diffusione delle sensibilità al rischio in modo maggiormente pervasivo all'interno dell'azienda.

L'applicazione di un Modello Centralizzato, Decentrato o Misto deve essere quindi contestualizzata nelle diverse realtà aziendali; un modello calibrato *ad hoc* in una società, potrebbe ritenersi inefficiente ed oneroso da applicare per un'altra.

A prescindere dal Modello di presidio del rischio utilizzato dalla Società, come già richiamato nel Capitolo I, la valutazione del sistema di gestione dei rischi da parte del Consiglio di Amministrazione è effettuata sempre con riferimento al gruppo di cui la società è capofila.

4. I ruoli all'interno dei gruppi

L'organizzazione della gestione del rischio all'interno di un gruppo, fatti salvi tutti i principi sopraesposti, deve tenere in considerazione due componenti principali:

- il modello di *governance*, inteso come attribuzione dei ruoli di indirizzo, coordinamento e controllo alla capogruppo, che può essere assolto in maniera più o meno stringente;
- il sistema delle deleghe adottate.

Un sistema che prevede il conferimento di deleghe e poteri decisionali significativamente decentrati richiede il coinvolgimento di un numero maggiore di *owner* del rischio, anche presso le società controllate.

Viceversa, in una situazione in cui le deleghe sono molto concentrate, anche la valutazione del rischio può essere realizzata a livello centrale, in quanto i referenti delle aree operative di riferimento hanno completa visibilità su tutti gli aspetti rilevanti, quali quelli riferibili all'attività di natura maggiormente operativa e sul rispetto delle linee di indirizzo tipiche della periferia.

In ogni caso, il Consiglio di Amministrazione della società capogruppo è tenuto ad assolvere al suo ruolo di *oversight* dei rischi per l'intero gruppo e pertanto il processo di *risk management* e i relativi presidi organizzativi devono essere idonei ad assicurare, attraverso approcci omogenei, la corretta esecuzione delle attività di identificazione, valutazione, gestione e monitoraggio dei rischi.

Questo presuppone che il *framework* di *risk management* adottato dalla capogruppo dovrà essere implementato nelle società controllate e che, in funzione delle dimensioni e della complessità del gruppo, tale *deployment* potrebbe richiedere l'istituzione di funzioni di *risk management* a livello locale con un legame di tipo funzionale rispetto al *Chief Risk Officer* centrale. Anche le modalità operative potrebbero richiedere degli adattamenti: ad esempio, le metriche utilizzate per la valutazione dei rischi potrebbero richiedere di essere scalate (con soglie finanziarie di impatto inferiori rispetto a quelle della capogruppo) al fine di cogliere i *top risk* a livello di controllata che invece non sarebbero rilevanti per la controllante.

L'adozione di un *framework* di gruppo risulta essere un fattore determinante anche ai fini del *reporting*, che deve raggiungere sia il Consiglio di Amministrazione della controllata sia, dopo opportune attività di consolidamento, quello della controllante.

CAPITOLO III

MODALITÀ DI INTERVENTO DEL CONSIGLIO DI AMMINISTRAZIONE NEL PROCESSO DI RISK MANAGEMENT

1. Modalità di intervento del Consiglio di Amministrazione nel processo di *risk management* - 1.1. *Risk governance* - 1.2. *Risk strategy & appetite* - 1.3. *Risk assessment & measurement* - 1.4. *Risk management & monitoring* - 1.5. *Risk reporting & insight* - 2. L'attività di *risk management* nei gruppi societari

1. Modalità di intervento del Consiglio di Amministrazione nel processo di *risk management*

Come già evidenziato nel Capitolo I, l'impegno del Consiglio di Amministrazione nel processo di *risk management* è riscontrabile in numerosi codici di *corporate governance* emessi o raccomandati dalle autorità preposte a supportare e promuovere lo sviluppo delle *leading practices* nei sistemi di gestione e controllo delle società quotate.

Per descrivere tale ruolo, è di uso sempre più frequente l'utilizzo dell'espressione *Board Risk Oversight*, ovvero il ruolo del Consiglio di Amministrazione nel processo di *risk management*. Nello specifico con l'espressione *Board Risk Oversight*, ci si riferisce alle attività attraverso cui il Consiglio di Amministrazione valuta se il *management* ha implementato un affidabile processo per l'identificazione, l'apprezzamento o valutazione, la gestione, il monitoraggio dei rischi rilevanti e si assicura che il processo venga aggiornato continuamente per tener conto dei cambiamenti intercorsi nell'ambiente di riferimento.

Tali momenti del processo di *risk management* rientrano nel più ampio contesto dell'implementazione di strategie di gestione del rischio, che possono essere diversificate come segue:

- rifiuto e/o *avoidance*: il rischio identificato viene evitato (ad esempio, il rischio di credito verso paesi politicamente instabili non viene assunto; il SCIGR sarà disegnato ed applicato per identificare e bloccare vendite non garantite da pagamento anticipato);
- trasferimento: il rischio identificato viene trasferito e/o condiviso (ad esempio, il SCIGR sarà disegnato ed applicato per identificare e bloccare spedizioni prive del rilascio di una accettabile garanzia bancaria);
- mitigazione: il rischio censito viene accettato entro un certo limite di tolleranza di perdita massima (ad esempio, il SCIGR sarà disegnato ed applicato per identificare e bloccare vendite eccedenti una predeterminata soglia monetaria);
- accettazione: il rischio censito viene accettato integralmente e nessun trattamento del rischio sarà, ipoteticamente, previsto per evitarlo trasferirlo e/o condividerlo o mitigarlo.

Ogni rischio è composto da due componenti: *upside*, ovvero l'opportunità sottostante l'evento, e *downside*, identificata con il rischio e la potenziale perdita da esso derivante. Al Consiglio di Amministrazione spetta il difficile compito di orientare la gestione verso il bilanciamento continuativo tra questi due elementi; le diversità di approccio al rischio si riflettono anche nei costi e ricavi di gestione e nella volatilità dei risultati, e quindi nel valore, dell'impresa³². Infatti, in presenza di

³² Si consideri ad esempio che strategie di mitigazione o di trasferimento dei rischi comportano dei costi interni ed esterni (ad es. spese assicurative e bancarie, costi del personale di controllo, sistemi informativi, etc.) che sono invece inesistenti nel caso di accettazione o di rifiuto del rischio; inoltre, la maggiore redditività di attività più rischiose (accettazione del rischio) e la conseguente maggiore volatilità dei risultati o la minore redditività delle attività prive di rischio (rifiuto del rischio) si riflettono in un minor valore dell'impresa per i suoi *stakeholders*.

incertezze, ciascuna decisione deve essere assunta avendo riguardo tanto ai rischi quanto alle opportunità che l'incertezza presenta, che possono distruggere ovvero creare valore.³³

Quindi, considerando l'impossibilità di creare valore nel tempo senza assumere alcun rischio, le decisioni in merito all'approccio al rischio dovranno essere finalizzate a bilanciare crescita, *target* stabiliti e relativi rischi, nonché ad impiegare efficacemente le risorse nello sviluppo del SCIGR al fine di raggiungere gli obiettivi di impresa. Il SCIGR rappresenta pertanto il fattore abilitante per il raggiungimento degli obiettivi aziendali di medio e lungo periodo e per la creazione di valore delle imprese.

Il Consiglio di Amministrazione dovrebbe incoraggiare la *management* nel perseguire un livello di rischio tale da generare valore per la società nel medio-lungo termine. Al tempo stesso però il Consiglio di Amministrazione deve assicurarsi che la componente *downside* delle varie attività sia sempre presa in considerazione, evitando così conseguenze inattese che potrebbero impattare negativamente sulla performance aziendale.³⁴

Il *risk oversight* del Consiglio di Amministrazione non si limita, quindi, ad un semplice controllo sull'avvenuta implementazione delle attività di gestione dei rischi, bensì comporta che il Consiglio di Amministrazione debba stimolare la *management* affinché gli fornisca tutte le informazioni rilevanti di cui dispone cosicché possa svolgere al meglio il suo ruolo in modo efficace e tempestivo.

Sebbene sia impensabile che il Consiglio di Amministrazione abbia tutte le informazioni che gli consentano di conoscere a fondo ogni aspetto dei diversi *business* e quindi dei diversi rischi che riguardano la società, la presenza di membri del Consiglio di Amministrazione costantemente informati e con visioni, competenze e conoscenze diverse rende il processo di *risk oversight* più efficiente e completo.

Il problema dell'asimmetria informativa resta comunque uno dei temi di maggior rilevanza per quanto riguarda l'argomento in discussione; l'impatto che si ha ogniqualvolta informazioni rilevanti non raggiungono il Consiglio di Amministrazione può avere conseguenze rilevanti. Considerando che la gestione errata di un rischio può portare, alle estreme conseguenze, al fallimento dell'azienda, si comprende l'importanza che il Consiglio di Amministrazione si assicuri che la *management* abbia ben chiare quali siano le informazioni rilevanti sui rischi e che sia in grado di fornirle nei tempi richiesti.

Sebbene questo ruolo di "*challenging*" da parte del Consiglio di Amministrazione abbia sicuramente un impatto positivo nel garantire l'efficace svolgimento del processo di *risk management*, bisogna sempre tenere in considerazione che, se attuato in modo improprio, questo compito potrebbe avere l'effetto opposto, stimolando la nascita di una *risk culture* avversa al rischio con tutte le conseguenze negative che ne potrebbero derivare.

Affinché il Consiglio di Amministrazione svolga il suo ruolo nel modo corretto è molto importante che abbia raggiunto una comprensione dell'esposizione dell'impresa ai rischi principali e che valuti se l'esposizione sia in linea con due elementi: il *risk appetite*, o propensione al rischio e la *risk tolerance*, o livello di variazione accettabile nel raggiungimento degli obiettivi così come definiti nel Capitolo II.

³³ Ad esempio, il sostenimento di costi per il potenziamento del proprio sistema informativo di prevenzione delle frodi permetterà ad una compagnia assicurativa di assumere quei clienti che le altre compagnie sue concorrenti non sono in grado di assumere a causa del rischio di frode. Al riguardo, è importante sottolineare che il rischio aggiuntivo assunto dalla prima compagnia è ridotto dall'investimento da essa fatto sui propri sistemi informativi rispetto a tale rischio, tale per cui il suo c.d. rischio residuo – *residual risk* – non è superiore a quello delle altre compagnie, mentre le sue performance aziendali, a parità di rischio residuo con i competitor, sono superiori perché ha più premi da clienti assicurati.

³⁴ Il Consiglio di Amministrazione dovrebbe anche chiedersi se, per esempio, per la definizione della strategia si sia partiti da assunti realistici e quali potrebbero essere le conseguenze qualora questi non si realizzassero. Ugualmente, al momento di effettuare un nuovo investimento, se il *management* detiene il ruolo di fornire i dettagli che rendono l'operazione appetibile per la società, il Consiglio di Amministrazione deve assicurare che tutti gli elementi connessi a quell'investimento siano stati considerati e come questa operazione si inserisca all'interno delle strategie di crescita dell'azienda nel rispetto della *risk tolerance* dell'organizzazione.

A questi elementi si accompagna il fattore determinante alla base del corretto funzionamento del SCIGR che è la *risk culture*, che può essere definita come il sistema di valori e comportamenti presenti all'interno dell'organizzazione che fa sì che le persone siano in grado di individuare i rischi, di comprenderli, di accettarli e di agire su questi valutando di volta in volta quale possa essere l'azione più indicata nella specifica situazione. Seppur inconsciamente è questo l'elemento che guida le azioni degli individui ad ogni livello aziendale quando si trovano a doversi confrontare con tematiche connesse ai rischi; ciò rende quindi la *risk culture* elemento prioritario tra i compiti di *risk oversight* affidati al Consiglio di Amministrazione.

Infatti, la conoscenza e la comprensione delle tematiche connesse ai rischi, unitamente ad altri elementi, quali ad esempio i valori etici, l'integrità e le competenze del personale, rappresentano la base del processo di *risk management* ed è responsabilità del Consiglio di Amministrazione e del *management* assicurare un adeguato atteggiamento verso il rischio all'interno dell'organizzazione.

In tale ambito, bisogna riconoscere come non sia solo una prerogativa del *management* quella di dare il buon esempio in tema di *risk management*, ma anche del Consiglio di Amministrazione che dovrebbe mettere in evidenza l'importanza prioritaria di queste tematiche incoraggiando ad ogni livello la tenuta di comportamenti improntati alla gestione dei rischi (c.d. *Tone from the top*). Assegnando una tale rilevanza ai comportamenti dei componenti del Consiglio di Amministrazione e del *management* nel promuovere la *risk culture*, il Consiglio di Amministrazione dovrebbe poi interrogarsi su quali siano le conseguenze e, soprattutto, come venga gestito un comportamento che si discosta da quello desiderato.

Costruire una cultura aziendale in grado di riconoscere e trattare in modo corretto i rischi, richiede tempo e sforzi, non è sufficiente l'intenzione del Consiglio di Amministrazione di diffondere un determinato tipo di cultura all'interno dell'organizzazione. È infatti indispensabile che i sistemi di *risk management* e controllo interno riescano a comprendere le aspettative del Consiglio di Amministrazione in tema di rischio e che le attività di *risk management* siano comunicate in modo adeguato alle persone/funzioni aziendali.

Compito del Consiglio di Amministrazione è anche quello di assicurare la diffusione di un linguaggio comune in tema di *risk management* affinché tutte le persone che fanno parte dell'organizzazione siano in grado di comprendere e condividere le tematiche connesse ai rischi. Un mezzo utile per raggiungere questo obiettivo potrebbe essere l'emissione di *policy* interne, strumento in grado di raggiungere le persone ai differenti livelli aziendali attraverso la formalizzazione, in uno o più documenti, di concetti che per molti soggetti potrebbero non essere scontati e di facile comprensione, tra cui, ad esempio la creazione di un catalogo di rischi integrato: il cosiddetto "*risk model*".

Il *training* e la comunicazione sono gli strumenti principali utilizzati per la diffusione della cultura e dei comportamenti desiderati all'interno delle imprese; la scelta di quali strumenti adottare può avere un impatto significativo in termini di efficacia nella diffusione della *risk culture* all'interno del sistema aziendale.

Il Consiglio di Amministrazione inoltre, di concerto con il *management*, deve valutare anche quali siano i migliori sistemi di *training* e di comunicazione stabilendo anche dei meccanismi formali a livello di struttura, sistema o processo utili nel promuovere la *risk culture*. Si potrebbe, ad esempio, pensare di considerare i contributi forniti nel processo di *risk management* quali elementi della valutazione e retribuzione del *management* e del personale. Proprio su questo ultimo punto il Consiglio di Amministrazione potrebbe avere un'influenza diretta nel modificare i piani di retribuzione del *management* e del personale aggiornando il sistema di retribuzione affinché includa non unicamente obiettivi di breve periodo, come ad esempio i parametri economici annuali, ma anche obiettivi collegati alle attività di gestione dei rischi che per definizione sono legati ad una visione di medio-lungo periodo.

Altri elementi su cui potrebbe far leva il Consiglio di Amministrazione al di là della remunerazione potrebbero essere il sistema di assunzione, di valutazione delle *performance* e di promozione. Un sistema premiante che tenga conto della gestione dei rischi è sicuramente uno strumento in grado di

motivare fortemente il personale ad agire tenendo conto dell'interesse della società stessa piuttosto che del loro interesse specifico o di quello della loro *business unit*. Anche in ottica futura, il Consiglio di Amministrazione deve tenere conto dell'importanza delle competenze in ambito di *risk management* per le posizioni manageriali chiave, prevedendo quindi dei piani di sviluppo che formino i propri dipendenti su queste tematiche.

Infine è molto importante che il Consiglio di Amministrazione si assicuri che esista un processo che renda gli insuccessi passati un importante momento di apprendimento e un'opportunità per rafforzare la *risk culture* e più in generale il sistema di *risk management*. Le cosiddette "*lessons learned*", per essere efficaci, devono essere individuate, valutate e infine comunicate a tutti i livelli della società affinché il processo di *risk management* evolva verso modelli sempre più avanzati.

Il Consiglio di Amministrazione, mantenendo una visione d'insieme sui diversi rischi, deve relazionarsi costantemente con il *management* incoraggiandolo, da un lato, a svolgere il suo ruolo di gestione dell'impresa e dall'altro mettendo alla prova le assunzioni alla base delle sue decisioni, anche attraverso l'utilizzo di schemi controintuitivi (cosiddetto "*challenge*"). Il Consiglio di Amministrazione non dovrebbe svolgere, quindi, meramente un ruolo formale di osservatore esterno, quanto piuttosto dovrebbe utilizzare le competenze e l'esperienza dei suoi membri per testare continuamente le assunzioni alla base delle scelte del *management* mettendo in evidenza elementi nuovi e assicurando così che tutti i fattori collegati siano stati presi in considerazione.

Tutto ciò premesso, il ruolo del Consiglio di Amministrazione è indubbiamente complesso considerando che deve costantemente assicurare che la gestione aziendale avvenga coerentemente con quanto disposto nei piani strategici, con la cultura aziendale e che, nella scelta di quali attività implementare, si debba sempre tener conto della *risk tolerance* e del *risk appetite* dell'organizzazione. Nel seguito del Capitolo saranno meglio approfondite le diverse aree di intervento del Consiglio di Amministrazione nell'ambito del *risk oversight* quali:

- *Risk governance*;
- *Risk strategy & appetite*;
- *Risk assessment & measurement*;
- *Risk management & monitoring*;
- *Risk reporting & insight*.

1.1. *Risk Governance*

Il Consiglio di Amministrazione deve essere organizzato e strutturato in modo da poter condividere efficacemente con gli altri livelli della struttura societaria (persone/funzioni) compiti, responsabilità, autorità e ruoli nell'ambito delle attività di *risk oversight*.

È compito del Consiglio di Amministrazione sincerarsi che il sistema di ruoli, responsabilità, *policy* e procedure sia integrato operativamente nell'organizzazione in modo da garantire una risposta rapida ed efficace a qualunque imprevisto si possa presentare, indipendentemente dal fatto che si tratti di un evento legato al contesto interno piuttosto che al contesto esterno di riferimento.

Nell'ambito della *risk governance* le società, seguendo le *best practice* nazionali e internazionali, strutturano il SCIGR in base a un modello costituito da tre livelli di controllo.

Il primo livello di controllo è formato dai responsabili delle aree operative che identificano, valutano, gestiscono e monitorano i rischi di propria competenza implementando specifiche azioni di trattamento. Il secondo livello di controllo è invece formato dalle cosiddette *Business-enabling functions*³⁵ che hanno il compito di presidiare i principali rischi attraverso un'attività di definizione delle regole e degli strumenti necessari e di monitoraggio dell'adeguatezza e dell'operatività dei controlli. Tra i soggetti che compongono il secondo livello di controllo, ci sono ad esempio le funzioni di *risk management* e di *compliance*. A tal proposito una figura che si colloca a questo livello e che sta acquisendo sempre maggior importanza all'interno delle strutture organizzative è quella del *Chief Risk Officer*. Il terzo livello di controllo è invece rappresentato dall'*Internal Audit* che svolge un compito di monitoraggio indipendente dell'interno SCIGR.

1.2. Risk strategy & appetite

Una delle principali responsabilità del Consiglio di Amministrazione nello svolgimento del proprio ruolo nell'ambito del processo di *risk management* è quella di assicurare che vi sia un collegamento continuo, coerente e compatibile tra la strategia aziendale e la gestione del rischio.

Il Consiglio di Amministrazione deve tener conto dell'importanza che riveste una strategia di gestione del rischio strutturata nel facilitare il raggiungimento degli obiettivi societari. Considerare tutti i possibili scenari che si potrebbero presentare nel perseguimento della strategia aziendale permette alla *management* di porre in essere tutte quelle attività di mitigazione che potrebbero rivelarsi fondamentali nel ridurre l'impatto o la probabilità di un evento di rischio con chiare conseguenze sul raggiungimento degli obiettivi strategici.

Il Consiglio di Amministrazione, nelle fasi di approvazione di nuovi progetti (M&A, investimenti, ecc.) e nella discussione di modifiche significative al piano strategico, dovrebbe sempre tener conto di quali siano i rischi collegati alle decisioni da prendere.

Il Consiglio di Amministrazione determina la natura e l'impatto dei rischi significativi che la società è disposta ad accettare nel raggiungimento dei suoi obiettivi strategici assicurandosi che non vi siano delle aree "scoperte".

I rischi di cui il Consiglio di Amministrazione deve tenere conto differiscono a seconda delle caratteristiche della singola società, ma possono includere rischi interni e rischi esterni. Quest'ultima categoria è formata da rischi come, ad esempio, il rischio di mercato o il rischio normativo, rispetto ai quali, benché il Consiglio di Amministrazione non abbia la possibilità di attivare alcun controllo diretto, è importante che venga implementato il processo di *risk management*. Altre tipologie di rischio comunemente presenti sono quelle finanziarie, operative, organizzative, etico-comportamentali e reputazionali direttamente collegate alla gestione aziendale.

È necessario che il Consiglio di Amministrazione, proprio per la sua funzione centrale nella definizione degli obiettivi strategici, proceda, inoltre, ad una chiara definizione di un elemento che solo un organismo con tale autorità, competenza e visione strategica può delineare: il *risk appetite*.

Nel definire la propensione al rischio, il cosiddetto *risk appetite*, il Consiglio di Amministrazione dovrebbe tenere conto di numerosi elementi: è necessario considerare la natura e l'entità dei diversi rischi analizzando a fondo la probabilità che questi rischi si manifestino e l'impatto che avrebbero sulla gestione aziendale. È altresì essenziale valutare le capacità della società di ridurre, attraverso l'implementazione di attività di trattamento e mitigazione, la probabilità di accadimento e le conseguenze derivanti da un evento sfavorevole.

³⁵ CoSO, *Internal Control - Integrated Framework*, 2013.

Il Consiglio di Amministrazione dovrebbe sempre essere consapevole che porre un'insufficiente attenzione ai rischi e trattare le attività connesse ad essi unicamente come tematiche di *compliance* piuttosto che come elementi centrali del processo decisionale potrebbe, in molti casi, mettere in pericolo non solo la sostenibilità delle attività coinvolte, ma anche la loro stabilità, e di conseguenza, la loro operatività.

I rischi spesso vengono considerati separatamente ma può capitare che siano collegati tra loro e che, di conseguenza, siano in grado di creare una reazione a catena. L'incapacità di cogliere l'interrelazione tra i diversi rischi è sicuramente un ostacolo nella loro gestione, soprattutto nelle grandi società caratterizzate da un numero di *business unit* molto elevato. Il Consiglio di Amministrazione dovrebbe, quindi, identificare il modo in cui i diversi rischi sono interrelati e garantire che il management abbia sviluppato un processo efficace ed efficiente per la comprensione dell'impatto aggregato dei rischi. Il *Chief Risk Officer* e/o i vari comitati interni possono supportare il Consiglio di Amministrazione in questa attività di aggregazione (v. *supra* Capitolo II, par. 2.3.).

1.3. Risk assessment & measurement

Questa fase del processo di *risk management*, come anche le fasi successive, si compone di una serie di attività di natura più operativa che coinvolgono in misura minore il Consiglio di Amministrazione ed in misura maggiore il management e le differenti funzioni aziendali che supportano il Consiglio di Amministrazione nel suo ruolo di *risk oversight*.

Le attività che compongono questo processo sono numerose e vanno dalla definizione, identificazione e valutazione dei rischi fino alla loro quantificazione. Il Consiglio di Amministrazione deve far sì che la progettazione del sistema di *risk assessment e measurement* sia in grado di individuare i rischi e di stimare l'impatto che questi avrebbero sull'azienda, qualora si manifestassero. La struttura del processo di *risk management* definita, deve tener conto della complessità, della dimensione e della situazione della società.

Nell'ambito del portafoglio dei rischi identificati, il Consiglio di Amministrazione dovrebbe focalizzarsi in particolar modo su quelli che, indipendentemente da come siano classificati o da quali siano le ragioni per cui possano emergere, potrebbero minacciarne il modello di *business*, le future *performance*, la solvibilità e la liquidità.

Considerando l'impossibilità di prevederne l'effetto o di quantificarne l'impatto, spesso sono i rischi emergenti o non conosciuti a presentare la minaccia maggiore per la società. Non tutti rischi in cui si può incorrere sono sempre conosciuti: "*There are known knowns. These are things we know that we know. There are known unknowns. That is to say, there are things that we know we don't know. But there are also unknown unknowns. There are things we don't know we don't know*"³⁶. Concentrarsi sull'identificazione tempestiva di questa tipologia di rischi potrebbe avere un impatto positivo sull'andamento aziendale evitando così, anticipatamente, possibili perdite finanziarie. Sebbene la finalità del processo di *risk management* sia quella di assicurare la pronta risposta della società ad eventi inaspettati, ci si chiede spesso come si possano identificare i rischi sconosciuti e di conseguenza quali siano le azioni da implementare per prepararsi per gli effetti che seguono. In questo caso, il Consiglio di Amministrazione è il soggetto che meglio di altri può fare delle valutazioni sullo scenario futuro e sulla situazione contingente della società, tenendo conto del modello di *business*, delle *performance*, della strategia, dei processi operativi e della fase di sviluppo raggiunta dall'organizzazione all'interno del ciclo di *business*.

Nel percorso evolutivo di un processo di *risk management* verso sistemi più avanzati, il Consiglio di Amministrazione dovrebbe altresì assicurarsi che, oltre all'identificazione degli eventi potenziali con

³⁶ Rumsfeld D., *Known and Unknown*, Penguin Group, 2011.

impatto negativo sulla creazione e preservazione di valore, il *management* sia in grado di identificare e cogliere proattivamente anche eventuali opportunità, quali eventi con effetti positivi sul conseguimento degli obiettivi aziendali. Le opportunità emerse dovrebbero essere valutate riconsiderando le strategie formulate in precedenza o i processi di definizione degli obiettivi in atto, al fine di elaborare nuovi piani per cogliere i vantaggi che ne potrebbero derivare.

A livello complessivo il Consiglio di Amministrazione deve, infine, assicurare che il processo di *risk management* sia consistente, cioè che la valutazione del rischio avvenga in modo oggettivo e puntuale, mediante l'utilizzo di tecniche quantitative e qualitative, e continuo ossia, che il profilo di rischio della società tenga sempre conto di eventuali cambiamenti intercorsi.

1.4. Risk Management & Monitoring

Prerogativa di fondamentale importanza per il Consiglio di Amministrazione è quella di garantire un'adeguata gestione dei principali rischi in cui la società potrebbe incorrere. Il Consiglio di Amministrazione, una volta individuati i principali rischi, dovrebbe stabilire chiaramente il modo in cui, questi, debbano essere gestiti o mitigati considerando anche come potrebbe cambiare l'esposizione della società in seguito alle azioni di trattamento volte a ridurre probabilità o impatto dei singoli rischi.

Compito del Consiglio di Amministrazione è quindi assicurare anche la presenza di un sistema di controllo che garantisca la copertura di numerosi aspetti di *business* tra cui quelli strategici, finanziari, operativi e di *compliance* garantendo che l'adozione del sistema non avvenga solo formalmente, ma che l'intero processo sia implementato in modo efficace e tempestivo.

Nello stabilire quali azioni di mitigazione implementare, il Consiglio di Amministrazione dovrebbe indicare le operazioni e le attività che compongono i principali processi di controllo pronunciandosi sulla capacità del modello di ottemperare alle funzioni necessarie per garantire che sia svolto in modo efficace ed efficiente e con una costante attenzione ai cambiamenti sia interni che esterni.

Inoltre il Consiglio di Amministrazione, nell'ottica di assicurarsi che la gestione del rischio avvenga in modo efficiente, dovrebbe garantire la coerenza tra il sistema di *risk management* e di controllo interno ed il *business model* aziendale, attraverso analisi dei costi-benefici derivanti dall'adozione di un determinato sistema di controllo interno.

Nello strutturare il sistema di controllo interno e gestione dei rischi, un'altra decisione che spetta al Consiglio di Amministrazione è relativa alla definizione di cosa costituisca un fallimento dei controlli e quali siano le azioni da implementare dopo aver riscontrato una simile situazione per porre rimedio ad un tale evento.

E' molto importante che, in questa fase, si tenga conto della possibilità che gli obiettivi, il settore e l'ambiente di riferimento della società cambino, e di come questo potrebbe avere conseguenze negative qualora la società non fosse abbastanza rapida nel valutare nuovamente i rischi aziendali e nel modificare il sistema di controllo. Bisogna quindi procedere costantemente ad una *review* del sistema affinché i processi e i controlli siano migliorati laddove presentino evidenti carenze operative e siano costantemente aggiornati secondo quelli che sono i rischi emergenti e i mutamenti intercorsi nell'ambiente esterno.

Le attività di *risk monitoring* nelle sue declinazioni operative sono oggetto di trattazione specifica nell'ambito del Capitolo IV.

1.5. Risk Reporting & Insight

Un sistema efficace e funzionante di *risk reporting* supporta il Consiglio di Amministrazione nello svolgimento delle attività di *risk oversight*. La mancanza di informazioni rilevanti e tempestive infatti può avere effetti negativi considerevoli soprattutto nella fase decisionale facendo sì che le decisioni vengano prese senza tener conto di tutti gli elementi di valutazione disponibili. Il Consiglio di Amministrazione deve assicurarsi sia di aver comunicato in modo appropriato al management quelle che sono le sue aspettative in tema di *risk reporting* sia che il *management* ne abbia una percezione chiara; qualora vi fosse un disallineamento tra Consiglio di Amministrazione e *management*, questo potrebbe tradursi in uno scambio di informazioni incompleto e inaccurato causando inefficienza e inefficacia nello svolgimento del processo di *risk management*.

Il Consiglio di Amministrazione, al fine di valutare la qualità del sistema di *reporting*, deve considerare numerosi elementi. In particolare si deve considerare:

- se le informazioni fornite soddisfano o meno lo scopo per cui sono state richieste,
- se provengono da un numero di fonti sufficienti, se sono qualitativamente rilevanti e se vengono fornite in tempi utili.

Elemento a supporto del corretto svolgimento del *reporting* e dell'intero processo di gestione dei rischi è la presenza di un adeguato sistema informativo in grado di gestire le informazioni (in termini di disponibilità, integrità e riservatezza) e di assicurare il funzionamento dell'attività di *reporting* verso le parti coinvolte.

Sulla base dei flussi di *reporting* ottenuti da parte di tutti gli attori della *governance* e del controllo interno, il Consiglio di Amministrazione effettua una valutazione di adeguatezza del sistema di controllo interno e di gestione dei rischi, il cui processo è dettagliato nell'ambito del Capitolo V.

2. L'attività di *risk management* nei gruppi societari

All'interno dei gruppi societari il sistema di controllo interno e di gestione dei rischi coinvolge Consiglio di Amministrazione, *top management* e strutture organizzative sia a livello di gruppo che di singola società.

Come indicato nel Codice di Autodisciplina, le strategie di gestione dei rischi delle singole società del gruppo di rilevanza strategica sono definite coerentemente con quanto previsto nella *mission* e negli obiettivi strategici del gruppo. La presenza di un processo di *risk management* strutturato deve assicurare la corretta esecuzione delle analisi di rischio anche nelle società controllate a rilevanza strategica a partire dal contributo che le stesse sono chiamate a fornire nell'ambito del piano strategico nonché dei rischi gestionali connaturati al proprio business e al contesto in cui operano.

La capogruppo, considerato il suo ruolo di direzione e coordinamento, ha il compito di diffondere le procedure relative al processo di *risk management* lungo tutta la struttura del gruppo societario. Pur mantenendo costante il suo ruolo di direzione, è necessario che la capogruppo garantisca un certo grado di autonomia alle società controllate affinché queste possano istituire un adeguato processo di *risk management*, sempre in linea con quanto definito dalla società controllante.

Prima dell'avvio della fase di identificazione e valutazione dei rischi è necessario procedere alla definizione dell'ambito del *risk assessment* coerentemente con gli indirizzi che vengono definiti dal Consiglio di Amministrazione e sulla base degli obiettivi strategici definiti dalla società, a livello di gruppo. Bisogna pertanto individuare i processi, le funzioni e il *management* da coinvolgere sia per quel che riguarda la capogruppo sia per le società controllate. Sono in questo modo selezionate le società controllate che si prevede contribuiranno in termini rilevanti al raggiungimento degli obiettivi

societari e/o che presentano elementi di attenzione nell'ambito della gestione e controllo dei rischi o potenziali esposizioni a rischi specifici.

E' necessario che, per la valutazione dei rischi delle società controllate, si definiscano delle metriche di valutazione dei rischi di livello inferiore con soglie ridotte e parametrare sulla rilevanza della singola società in termini economico-finanziari, in modo da distinguere i rischi che rileveranno unicamente per la controllata da quelli che potrebbero avere, invece, un impatto più elevato e, quindi, rilevante anche a livello di gruppo.

Elemento da considerare al fine di strutturare in modo appropriato un sistema di *risk management* in grado di funzionare correttamente anche in realtà complesse come i gruppi di società è la "dimensione" delle entità controllate. Comunemente accade che le società controllate su cui condurre il *risk assessment* sono selezionate in base al superamento di determinate soglie di rilevanza. In taluni casi, le attività condotte dalla società controllata possono richiedere un processo di analisi dei rischi più pervasivo, con il coinvolgimento di diverse funzioni aziendali. In società controllate meno strutturate, invece, può risultare sufficiente svolgere una singola attività di *assessment* con l'Amministratore Delegato o con una figura equivalente.

Il coinvolgimento del Consiglio di Amministrazione della capogruppo e del Consiglio di Amministrazione delle società controllate avviene, quindi, in momenti distinti e chiaramente prevede che questi soggetti svolgano compiti differenti secondo le loro diverse responsabilità. Come descritto in precedenza, all'interno della capogruppo si definiscono le linee guida del processo di *risk management*, ed è il Consiglio di Amministrazione di quest'ultima ad avere la responsabilità di valutare il processo di gestione dei rischi implementato dalla funzione di *risk management*.

Il Consiglio di Amministrazione delle controllate riceve i *report* sui rischi di sua competenza, preliminarmente alla fase di consolidamento e presentazione al Consiglio di Amministrazione della capogruppo. Il Consiglio di Amministrazione delle società controllata riveste quindi un ruolo fondamentale nell'assicurare che il processo venga svolto secondo le direttive stabilite a livello di gruppo e garantisce che tutti i rischi afferenti alle unità appartenenti alla sua organizzazione siano adeguatamente presi in considerazione.

CAPITOLO IV

IL RUOLO DEL CONSIGLIO DI AMMINISTRAZIONE NELLE ATTIVITÀ DI MONITORAGGIO (ON GOING BASIS) E REVIEW (ANNUAL BASIS) DEL SISTEMA DI CONTROLLO INTERNO E GESTIONE DEI RISCHI

1. Considerazioni generali - 2. L'esercizio di *oversight* del Consiglio di Amministrazione: il monitoraggio continuo (*on going*) - 3. L'esercizio di *oversight* del Consiglio di Amministrazione: la *review* periodica (*annual basis*)

1. Considerazioni generali

L'esistenza di un processo ("Sistema") di Controllo Interno e Gestione dei Rischi, anche formalizzato, non rappresenta, di per sé, una garanzia del fatto che i rischi aziendali siano efficacemente presidiati e gestiti.

Elemento essenziale del sistema, a garanzia dell'adeguatezza ed efficacia nel tempo del SCIGR, e attività propedeutica alla sua valutazione, è un'appropriata attività di monitoraggio e riesame, come parte integrante dello stesso processo.

In termini generali, un efficace processo di gestione dei rischi e controllo interno richiede – tra i suoi elementi costitutivi - un monitoraggio continuo finalizzato ad assicurare, *in primis*, che le risposte al rischio pianificate siano state implementate e operino efficacemente nel continuo, ma anche l'esistenza di un adeguato processo finalizzato ad identificare i nuovi rischi che dovessero emergere nell'operatività aziendale o dal contesto esterno, al fine di identificarne i relativi trattamenti necessari. Non appena il *management* è consapevole di nuovi rischi, dovrebbe infatti essere considerato l'impatto delle possibili strategie di risposta al rischio.

Oltre ad assicurare che la struttura preposta alla gestione del processo sia adeguata ed operi con efficacia, dovrebbe essere in ogni caso favorita un'adeguata "cultura" che responsabilizzi tutto il personale nell'evidenziare le potenziali *issues* e nell'intraprendere azioni finalizzate a proteggere l'organizzazione; indipendentemente dalle caratteristiche dei processi e dell'organizzazione aziendale, è determinante, a questo proposito, che il personale percepisca una responsabilità individuale nel contribuire alla gestione dei rischi dell'organizzazione.

Come anche evidenziato dalla norma ISO 31000³⁷, al fine di assicurare che la gestione del rischio sia efficace e continui a supportare le prestazioni dell'organizzazione, le attività di monitoraggio e riesame – che dovrebbero tipicamente essere svolte da strutture indipendenti da quelle che hanno posto in essere le attività da valutare – dovrebbero avere ad oggetto sia l'"organizzazione" che il "processo", ovvero sia la "struttura di riferimento" sia le "attività".

Con riferimento alla "struttura di riferimento", il monitoraggio ed il riesame dovrebbero prevedere:

- la misurazione del processo di gestione dei rischi facendo riferimento a indicatori, periodicamente riesaminati in termini di adeguatezza;
- la misurazione e la rendicontazione periodica del piano di gestione dei rischi e degli eventuali scostamenti rispetto alle politiche di *risk management* adottate;
- il riesame dell'efficacia della struttura di riferimento per la gestione dei rischi;

³⁷ ISO 31000:2010, *Gestione del rischio – Principi e linee guida*, si vedano in particolare paragrafi 4.5 e 5.6.

- la valutazione periodica di adeguatezza della struttura, della politica e del piano di gestione dei rischi, in relazione al contesto interno ed esterno dell'organizzazione.

In merito al “processo”, il riesame ed il monitoraggio dovrebbero essere una parte pianificata del processo di gestione dei rischi e comportare anche verifiche e attività di supervisione regolari, periodiche oper specifici obiettivi, le cui responsabilità dovrebbero essere chiaramente definite.

L'ambito di tali attività dovrebbe essere tutto il processo di gestione dei rischi, con l'obiettivo di:

- assicurare che i controlli/le risposte al rischio siano efficaci ed efficienti, sia nella progettazione che nell'operatività;
- ottenere ulteriori informazioni per migliorare la gestione dei rischi;
- analizzare ed apprendere dagli eventi (compresi i “near-miss”);
- rilevare i cambiamenti nel contesto esterno ed interno, comprese le modifiche ai criteri di rischio ed ai rischi stessi, che possano richiedere revisioni dei trattamenti del rischio/risposte al rischio e delle priorità;
- identificare i rischi emergenti.

I risultati del monitoraggio e riesame dovrebbero essere documentati e riportati internamente ed esternamente, come appropriato, e dovrebbero anche essere utilizzati come dati in ingresso al riesame della struttura di riferimento per la gestione del rischio.

A questo riguardo, come introdotto nel Capitolo precedente (cfr. in particolare Capitolo III, paragrafo 1.4), nelle attività di monitoraggio e riesame un ruolo fondamentale è svolto dal Consiglio di Amministrazione.

Un'appropriata attività di *oversight* da parte del Consiglio di Amministrazione, infatti, attraverso attività proprie di monitoraggio (*on going*) e di *review* (periodica) del “Sistema”, è elemento essenziale per consentire al *Board* di poter concludere se e in che misura la gestione aziendale è allineata agli obiettivi strategici dell'organizzazione e se le modalità di gestione dei rischi sono appropriate e ne supportano il raggiungimento, attraverso una struttura di riferimento adeguata.

Obiettivo generale delle attività di monitoraggio e *review* da parte del *Board* dovrebbe pertanto essere un'accurata e ponderata valutazione dell'adeguatezza del SCIGR, da intendersi come la sua effettiva capacità di contribuire ad una conduzione dell'impresa coerente con gli obiettivi aziendali definiti dallo stesso Consiglio di Amministrazione, favorendo il processo di assunzione delle decisioni. Esso dovrebbe essere idoneo a concorrere effettivamente ad assicurare la salvaguardia del patrimonio sociale, l'efficienza e l'efficacia dei processi aziendali, l'affidabilità dell'informazione finanziaria, il rispetto di leggi e regolamenti nonché dello statuto sociale e delle procedure interne³⁸.

³⁸ Oltre a definirne le linee di indirizzo finalizzate a garantire che i principali rischi risultino correttamente identificati, ma anche adeguatamente misurati, gestiti e monitorati, nonché a determinare il grado di compatibilità di tali rischi con una gestione dell'impresa coerente con gli obiettivi strategici individuati, il Consiglio di Amministrazione è, inoltre, chiamato a valutare l'adeguatezza del sistema di controllo interno e di gestione dei rischi rispetto alle caratteristiche dell'impresa e al profilo di rischio assunto, come pure la sua efficacia. Le caratteristiche del sistema e l'esito di tale valutazione dovrebbero trovare espressione nell'informativa finanziaria (formalmente, con cadenza almeno annuale).

È opportuno che il Consiglio di Amministrazione definisca le modalità di svolgimento delle proprie attività di monitoraggio e di *review*, inclusi:

- i presupposti/requisiti da assicurare nel processo di monitoraggio e *review*;
- le modalità di svolgimento delle attività di *assurance* del sistema;
- l'ambito e la frequenza del reporting, da intendersi nell'accezione di documentazione degli approfondimenti condotti.

Ancorché formalmente previste, tali attività, infatti, spesso non trovano debita regolamentazione e formalizzazione.

Al fine di garantire che la gestione dei rischi abbia una trattazione adeguata nell'ambito delle discussioni e delle decisioni, il *Board* dovrebbe assicurare e verificare che sia sempre dedicato tempo sufficiente nel dibattito consiliare. Per garantire tale requisito, è utile che venga prestata specifica attenzione nell'articolazione del calendario e dell'agenda delle riunioni (del Consiglio e dei suoi Comitati).

In relazione alla complessità dell'organizzazione, ma anche alle competenze possedute dai consiglieri ed alle tempistiche necessarie per lo svolgimento di tali attività, il Consiglio può avvalersi del supporto di organi/strutture specifiche³⁹ nell'espletamento dei compiti di monitoraggio e *review*, con particolare riguardo alle attività istruttorie. In tal caso, è di fondamentale importanza una puntuale identificazione delle responsabilità (del Consiglio nella sua collegialità e dei singoli Comitati) e dell'*iter* di svolgimento delle attività.

Una valutazione equilibrata dei rischi e dell'efficacia dei sistemi di *risk management* e controllo interno da parte del Consiglio di Amministrazione, anche attraverso l'attività istruttoria ed il supporto consultivo da parte dei suoi Comitati (specie il Comitato Controllo e Rischi) dovrebbe essere in ogni caso supportata da un regolare flusso di *reporting* (dati, informazioni, ecc.) da parte del *management* e dagli organi e funzioni aziendali preposte al controllo (specie di secondo e terzo livello), nonché – ove individuato – dall'Amministratore Incaricato del SCIGR⁴⁰.

A questo proposito, è essenziale che il Consiglio identifichi puntualmente le informazioni di cui necessita per le proprie attività di monitoraggio e *review*, comunicando e condividendo tali aspetti con il management (struttura, contenuti e tempistiche delle informazioni da produrre). Ancorché sia diffusa la trasmissione al *Board* di periodiche risultanze dei rischi aziendali, non altrettanto frequente⁴¹ ma particolarmente importante per un'efficace comprensione dell'adeguatezza del processo è l'informativa in merito⁴²:

- all'individuazione e trattazione specifica dei *top risk*;
- alle analisi di scenario correlate agli impatti di potenziali cambiamenti nel contesto esterno di riferimento con potenziali impatti sull'organizzazione;

³⁹ Con particolare riferimento ai Comitati endoconsiliari, ci si riferisce in particolare, a tale riguardo, al Comitato Controllo e Rischi.

⁴⁰ Nel caso di Gruppi, l'informativa sulla gestione dei rischi - e conseguentemente gli approfondimenti del *board* - dovrebbe considerare l'organizzazione nel suo complesso e quantomeno le informazioni relative alle imprese controllate aventi rilevanza strategica.

⁴¹ L'informativa al Consiglio di Amministrazione dovrebbe infatti consentire un'immediata ed univoca individuazione, da parte dello stesso e di tutti i suoi componenti, dei rischi principali dell'organizzazione, delle relative caratteristiche (soglie di tolleranza, valutazione, ecc.) e azioni definite per il relativo contenimento. Analisi di *benchmark* e *survey* che interessano i componenti dei *board* evidenziano con una certa frequenza che l'informativa prodotta non sempre consente un'immediata individuazione dei *top risk* e delle relative risposte.

⁴² CoSO, "Board risk oversight – a progress report", 2010.

- alle casistiche di superamento dei limiti di rischio definiti (*risk appetite* e suo recepimento nelle direttive e procedure aziendali);
- alle *issues* di *risk capacity* in relazione ai rischi da fronteggiare ed ai piani definiti per il loro superamento.

Tali aspetti dovrebbero pertanto costituire esplicita previsione di flussi informativi verso il *Board*.

Le caratteristiche delle informazioni ottenute, alla base del processo di monitoraggio, *review* e successiva valutazione, è inoltre fisiologicamente legata alle caratteristiche dei ruoli e delle funzioni aziendali con specifici compiti in tema di controllo interno e gestione dei rischi (es. *Chief Audit Executive*, *Chief Risk Officer*, *Compliance Officer*, Dirigente preposto alla redazione dei documenti contabili societari, ecc.), con particolare riferimento all'adeguata articolazione - in relazione a dimensioni, complessità e profilo di rischio dell'impresa - al livello dicoordinamento nonché alle modalità di funzionamento, con particolare riguardo:

- all'utilizzo di metodologie ed approcci appropriati e coerenti, in linea con le caratteristiche dell'organizzazione ed i principali *framework* in materia di sistema di controllo interno, gestione dei rischi e *compliance*;
- alla focalizzazione delle attività di analisi e verifica sugli effettivi (e principali) rischi dell'organizzazione.

Nell'attività di *oversight*, particolare attenzione, a questo riguardo, dovrebbe essere prestata a:

- formazione e *awareness* del personale sulle tematiche di controllo interno e gestione dei rischi;
- riporti gerarchici e funzionali e dimensionamento delle strutture organizzative, di secondo e terzo livello, preposte alla gestione dei rischi e al controllo interno e - prima ancora - coerenza ed allineamento del SCIGR con il sistema di *governance* aziendale, da intendersi sia con riferimento all'attribuzione di ruoli, compiti e responsabilità, sia con riferimento all'attribuzione dei poteri;
- profilo professionale delle risorse coinvolte (specie in posizione di responsabilità), incluso il possesso di certificazioni professionali rilevanti;
- documentazione, aggiornamento e diffusione delle norme e delle procedure a supporto delle metodologie adottate per lo svolgimento delle attività;
- *benchmark* di allineamento delle prassi adottate alle *best practices* di riferimento, avendo riguardo alle caratteristiche dell'organizzazione;
- certificazioni/*assurance* indipendenti di adeguatezza delle metodologie adottate e allineamento a standard di riferimento internazionalmente riconosciuti (es. *Quality Assurance Review* delle attività di *Internal Audit*, *Third Party Assurance* sui processi di gestione dei rischi e di *compliance*);
- livello di attenzione e attività di presidio dei *key risk* avendo riguardo agli obiettivi strategici dell'organizzazione.

Ancorché l'attività di monitoraggio e *review* debba costituire elemento essenziale del processo di *risk management* da parte delle strutture aziendali di riferimento, secondo il modello di gestione dei rischi identificato, il *Board* dovrebbe dunque, in ogni caso, formarsi la propria visione sull'efficacia del Sistema di Controllo Interno e Gestione dei Rischi sulla base delle evidenze ottenute, esercitando la stessa diligenza professionale attesa dal senior management nell'assolvimento delle proprie responsabilità ed includendo nel processo di *oversight* anche l'attività di riesame e *review* svolta dalle strutture preposte⁴³.

⁴³ FRC, *Guidance on Risk Management, Internal Control and Related Financial and Business Reporting*, 2014.

2. L'esercizio di *oversight* del Consiglio di Amministrazione: il monitoraggio continuo (*on going*)

Nel processo di monitoraggio continuo da parte del Consiglio di Amministrazione in merito al SCIGR, è opportuno che il *Board* garantisca una costante supervisione sull'efficacia del processo di identificazione e valutazione dei rischi (*risk assesment*), di gestione e mitigazione degli stessi, nonché sulla tempestività di intervento in merito a eventuali aree di miglioramento identificate, analizzando nel contempo le cause delle debolezze identificate.

E' opportuno che la gestione del rischio sia, infatti, incorporata in tutte le prassi e processi dell'organizzazione, in maniera pertinente, efficace ed efficiente. Il processo di gestione dei rischi dovrebbe, cioè, essere parte integrante dei processi organizzativi e non un processo ulteriore, separato da essi. In particolare, la gestione del rischio dovrebbe essere incorporata nella gestione della politica, nella pianificazione strategica e commerciale, nel loro riesame e nei processi di gestione del cambiamento. Il piano di gestione dei rischi, anche incorporato in altri piani dell'organizzazione (es. piano strategico), dovrebbe pertanto supportare l'attuazione della politica di gestione del rischio ai vari livelli dell'organizzazione e l'incorporazione della gestione dei rischi in tutti i processi aziendali⁴⁴. Requisito necessario (ma non sufficiente) per assicurare che questo avvenga è un adeguato recepimento, nelle *policy*, direttive e procedure aziendali, dei processi, delle attività e delle valutazioni (e delle correlate responsabilità) connesse al processo di *risk management*.

Focalizzandosi sui risultati del processo, oltre che sull'adeguatezza ed efficacia del suo disegno, nelle attività di analisi e verifica di atti e documenti (anche di supporto al processo decisionale) nel corso dell'esercizio, il Consiglio dovrebbe considerare:

- se i rischi più rilevanti per l'organizzazione siano stati individuati;
- quanto siano stati valutati efficacemente i rischi;
- come tali rischi siano stati gestiti o mitigati;
- se siano state intraprese tempestivamente opportune azioni correttive per porre rimedio a *failures* e carenze⁴⁵.

A tale proposito, si può facilmente desumere che l'efficacia del processo di *risk assesment* e di gestione dei rischi è strettamente correlato alla comprensione, nell'organizzazione, del *risk appetite*⁴⁶, ossia della comprensione dell'ammontare di rischio che l'organizzazione stessa è in grado di accettare nel perseguimento dei propri obiettivi e, dunque, del livello di rischio al di sopra del quale sia necessario definire ed implementare specifiche misure per la sua mitigazione.

Un'efficace attività di *oversight* del *Board* su tali tematiche, pertanto, non dovrebbe prescindere dalla valutazione dell'effettiva comprensione del *risk appetite* da parte del *management*, chiamato a tradurlo nel processo decisionale nella definizione del *risk profile* (ossia dell'identificazione e valutazione dei rischi principali dell'organizzazione e delle misure per la loro gestione), nella misurazione della *risk capacity* (ossia dell'ammontare di rischio che l'organizzazione è capace di sopportare, in ragione dei relativi impatti) e nella successiva valutazione e gestione dei rischi. In particolare, dovrebbe essere chiaro al *management* (e valutato dal *Board* attraverso interazioni con lo stesso):

⁴⁴ ISO 31000: 2010, *Gestione del rischio – Principi e linee guida*, si veda in particolare il paragrafo 4.3.

⁴⁵ FRC, *Guidance on Risk Management, Internal Control and Related Financial and Business Reporting*, 2014.

⁴⁶ Ancorché i rischi non possano essere gestiti direttamente dal *Board*, ma ne debba tuttavia essere fornito dallo stesso l'indirizzo e supervisionata la gestione (da cui ne deriva la responsabilità di *oversight*), è compito del Consiglio di Amministrazione definire il *risk appetite* e influenzarne la cultura. Assumere rischi – ad un corretto livello ed ambito – è critico per una conduzione di successo del *business*.

- quali rischi non siano accettati dall'organizzazione, avendo riguardo ai suoi valori;
- quali rischi sia necessario assumere e gestire, in relazione alla strategia definita;
- quali rischi siano considerati tollerabili dagli *stakeholder*;
- quali risorse siano necessarie per gestire tali rischi;
- quale variabilità sia ritenuta accettabile intorno al raggiungimento degli obiettivi definiti (*risk tolerance*).

A tale riguardo, nel processo di monitoraggio *on going*, il *Board* dovrebbe confrontarsi con il *management* e approfondire:

- le caratteristiche del processo di *risk assessment* finalizzato ad identificare, prioritizzare e analizzare nel continuo i rischi-chiave e di renderli allineati agli obiettivi strategici;
- l'esistenza di un processo volto ad intervenire con tempestivi aggiustamenti su *risk appetite* e *risk tolerance* al cambiamento degli obiettivi strategici e a comunicarli con efficacia a *stakeholder* interni ed esterni;
- la tempestività di aggiornamento del *risk profile* in relazione a cambiamenti strategici, di *business* e del contesto esterno;
- la capacità dell'organizzazione di valutare e gestire i rischi correnti e prospettici, in relazione ai propri indirizzi strategici.

Relativamente al monitoraggio *on going*, inoltre, le tematiche correlate al rischio dovrebbero essere tenute in particolare considerazione nelle discussioni e nelle delibere che implicino cambiamenti nella strategia nonché iniziative di investimento.

Nelle discussioni e deliberazioni, è in ogni caso opportuno che vengano tenuti in adeguata considerazione gli aspetti connessi ai costi-benefici correlati a differenti opzioni nei controlli da implementare.

Sin da tale attività di monitoraggio, è evidente che l'attenzione del Consiglio di Amministrazione dovrebbe essere orientata ad assicurare che le informazioni alla base delle decisioni da assumere siano tempestive, di adeguata qualità (incluso il giusto livello di dettaglio) e coerenti, con riferimento ad eventuali differenti fonti di provenienza.

Tra esse, dovrebbe essere previsto un tempestivo flusso informativo in merito alle circostanze in cui i limiti di tolleranza al rischio sono stati superati (presupponendo che siano stati assunti troppi rischi) o non raggiunti (presupponendo che non siano stati assunti i rischi previsti).

3. L'esercizio di *oversight* del Consiglio di Amministrazione: la *review* periodica (*annual basis*)

Oltre alle attività di monitoraggio continuo (*on going*), il Consiglio di Amministrazione dovrebbe porre in essere, con cadenza annuale, una *review* dell'efficacia complessiva del sistema, al fine di assicurare che tutti gli aspetti significativi del processo di controllo interno e di gestione dei rischi dell'organizzazione siano stati considerati e valutati e risultino adeguati.

Come già evidenziato, il *Board* dovrebbe definire il processo da adottare e le attività da svolgere per tale *review*. Dovranno essere dunque definite le modalità di utilizzo delle informazioni, le funzioni aziendali preposte al controllo e alla gestione dei rischi, l'attività istruttoria svolta dai Comitati, la documentazione a supporto dei risultati delle attività condotte, anche al fine di supportare l'informativa prodotta nel *reporting* annuale.

A tale riguardo, pur tenendo conto delle caratteristiche dell'organizzazione, dovrebbe essere incentivato ed auspicato il ricorso, da parte delle funzioni preposte, all'utilizzo di *standard*, metodologie e *framework* di organizzazione e svolgimento delle attività internazionalmente riconosciuti, favorendo se del caso – forme esterne di *assurance* indipendente e qualificata di tali requisiti.

Si rammenta tra gli altri, a questo proposito:

- con riferimento alla progettazione, analisi e valutazione del processo di gestione dei rischi, l'esistenza dello *standard* internazionale ISO 31000 in materia di "Gestione del Rischio", nonché l' "Enterprise Risk Management Framework", emesso dal CoSO;
- con riferimento alla progettazione, analisi e valutazione del sistema di controllo interno, l' "Internal Control – Integrated Framework", anch'esso emesso dal CoSO;
- con riferimento alla progettazione, analisi e valutazione dei sistemi di compliance, lo *standard* internazionale ISO 19600.

La *review* annuale dell'efficacia complessiva del sistema dovrebbe considerare⁴⁷, in particolare:

- l'adeguatezza del processo di definizione e diffusione del *risk appetite*, ovvero la capacità/attitudini dell'impresa ad assumere i rischi, e la sua comprensione nell'organizzazione, come in precedenza già evidenziato. Nell'approfondire tali aspetti, il *Board* dovrebbe assicurare una chiara definizione del rischio e un adeguato livello di condivisione e comprensione nell'azienda. Con riferimento alla cultura del rischio nell'organizzazione, particolare attenzione dovrebbe essere posta alle modalità attraverso cui il *senior management* promuove e trasferisce nell'organizzazione il livello di rischio desiderato ed il *commitment* alla gestione dei rischi e di controllo interno, nonché alla capacità di comprendere gli errori pregressi e di imparare dalle *lessons learned*;
- le modalità operative del processo di controllo interno e di gestione dei rischi, da intendersi come disegno, implementazione e monitoraggio del sistema, che includano le modalità di identificazione dei rischi più rilevanti per l'impresa. In tale contesto, l'attenzione del *Board* dovrebbe essere posta, tra gli altri aspetti, alle modalità di individuazione delle responsabilità in materia di *risk management*, al loro coordinamento ed alla relativa documentazione, in termini di chiarezza, adeguatezza ed efficacia. Specifica attenzione dovrebbe essere posta alla previsione di specifiche responsabilità per tutti i rischi identificati. Parimenti, un elemento da tenere in adeguata considerazione dovrebbe essere il possesso da parte del personale di adeguate conoscenze, capacità e strumenti per gestire efficacemente i rischi. La valutazione di adeguatezza del Sistema dovrebbe ugualmente tenere in considerazione le modalità attraverso cui il *senior management* monitora l'effettiva ed efficace implementazione del processo di *risk management*;

⁴⁷ FRC, *Guidance on Risk Management, Internal Control and Related Financial and Business Reporting*, 2014.

- l'integrazione del processo di *risk management* e di gestione dei rischi con la strategia ed il *business model* dell'organizzazione, oltre che la coerenza con il sistema di *governance*;
- a coerenza del sistema di rewarding ed incentivazione con il sistema di gestione dei rischi ed in particolare con il profilo di rischio aziendale;
- i cambiamenti nella natura, nella probabilità di accadimento e negli impatti dei rischi principali (cambiamenti nel profilo di rischio) e la capacità dell'azienda di rispondere e reagire ai cambiamenti nel proprio *business* e ambiente interno ed esterno, inclusa quella di saper adattare tempestivamente e con efficacia le proprie risposte al rischio a tali cambiamenti ("*risk resilience*");
- la capacità del *management* e del sistema di individuare con tempestività ed efficacia i rischi emergenti e le opportunità derivanti dai mutamenti nello scenario di riferimento;
- la lettura combinata dei potenziali effetti degli accadimenti rilevanti, in termini di adeguata considerazione delle correlazioni tra i differenti rischi;
- l'esistenza di robusti piani di rimedio in caso di crisi e la valutazione di adeguatezza del relativo funzionamento;
- l'esistenza e l'efficace funzionamento di adeguati canali di comunicazione e segnalazione, anche con riferimento a terze parti, di elementi di rischio specifico, inclusa la presunta o accertata violazione di leggi e regolamenti, nonché eventuali comportamenti scorretti;
- la portata, la frequenza e la qualità della comunicazione dei risultati delle attività di monitoraggio da parte del *management* nonché degli altri attori del SCIGR verso il *Board*, che consenta di ottenere una valutazione aggregata e complessiva dello stato dei controlli nell'impresa e l'efficacia con cui i rischi sono gestiti o mitigati;
- le criticità emerse e fronteggiate nell'anno ed emerse nel processo di reporting, in particolare l'incidenza di debolezze o carenze significative e la portata che hanno avuto o potrebbero avere in un impatto imprevisto;
- l'effettiva capacità del processo di *risk management* e di controllo interno di contribuire all'adeguatezza dell'informativa sul *financial reporting*;
- l'efficacia del *reporting* verso l'esterno, incluse le informazioni relative alle caratteristiche dell'attività di *oversight* del Consiglio e alle modalità di gestione dei rischi ed ai principali rischi che interessano l'impresa ed il suo contesto.

Le risultanze delle attività di monitoraggio, *on going* ma soprattutto periodiche, dovrebbero *in primis* costituire uno dei principali *input* per la valutazione di adeguatezza del SCIGR, affrontata dettagliatamente nel Capitolo successivo, e dovrebbero altresì essere considerate per valorizzare la capacità dell'azienda di affrontare e gestire i rischi.

Ove rappresentati in maniera appropriata, anche nel reporting esterno, la capacità dell'azienda di reagire ai cambiamenti ed il collegamento tra *business model*, strategie, opportunità e modalità di gestione dei rischi possono, infatti, influenzare in maniera significativa la percezione esterna della qualità del management e del *Board* e contribuire alla conservazione del valore aziendale, con impatti positivi sul costo del capitale.

È provato che la disponibilità di informazioni chiare e concise abbia una diretta ripercussione sul livello di fiducia degli analisti e degli operatori del credito e, in ultima istanza, sulla capacità dell'azienda di raccogliere capitale nel tempo. A questo riguardo, è stato evidenziato che esiste talora un *gap* piuttosto significativo tra le aspettative di comprensione dei rischi del *business model* (e delle relative salvaguardie) e la rappresentazione verso l'esterno che ne offre l'azienda.

Un *reporting* esterno sui rischi è considerato efficace se è di tipo specifico, collegato alle strategie e se riesce a rappresentare la visione dell'azienda in merito alle misure di mitigazione del rischio.

Rappresentare adeguatamente le *performance* aziendali, incluse le modalità di gestione dei rischi, è una parte importante delle responsabilità del *Board* e rappresenta, prima che un obbligo di *compliance*, un'opportunità per valorizzare l'azienda.

CAPITOLO V

LA RELAZIONE SUL GOVERNO SOCIETARIO E LA VALUTAZIONE DA PARTE DEL CONSIGLIO DI AMMINISTRAZIONE SULL'ADEGUATEZZA DEL SISTEMA DI CONTROLLO INTERNO E DI GESTIONE DEI RISCHI.

1. Gli adempimenti del Consiglio di Amministrazione nella valutazione di adeguatezza del Sistema di Controllo Interno e di Gestione dei Rischi - 2. I ruoli, le responsabilità ed i flussi informativi a supporto della valutazione del Consiglio di Amministrazione - 3. Il processo di valutazione - 4. Valutazione di eventuali carenze e approcci per la valutazione del Sistema di Controllo Interno e di Gestione dei Rischi

1. Gli adempimenti del Consiglio di Amministrazione nella valutazione di adeguatezza del Sistema di Controllo Interno e di Gestione dei Rischi

Come già precedentemente evidenziato, il Legislatore italiano ha introdotto, nella sezione delle società per azioni, all'interno dell'art. 2381, comma 3 cod. civ., tra i compiti del Consiglio di Amministrazione, "la valutazione dell'adeguatezza dell'assetto organizzativo, amministrativo e contabile della Società". La norma ha posto a carico del Consiglio di Amministrazione la valutazione dell'adeguatezza degli assetti interni dell'impresa (organizzativo, amministrativo e contabile) sulla base delle informazioni ricevute da tutti gli attori del SCIGR.

Il Codice di Autodisciplina nella sua prima versione del 1999 anticipava quanto poi richiesto dall'art. 2381, comma 3 cod. civ.. La valutazione degli assetti organizzativi e amministrativi della Società e del Gruppo da parte del Consiglio presupponeva indirettamente che gli organi delegati dovessero predisporre tali assetti. Detto compito è stato successivamente ripreso nel comma 5 dell'art. 2381 cod. civ. con l'espresso affidamento agli organi delegati della "cura dell'assetto organizzativo, amministrativo e contabile". L'attuale versione del Codice di Autodisciplina del 2015 prevede che il Consiglio di Amministrazione valuti "l'adeguatezza dell'assetto organizzativo, amministrativo e contabile dell'emittente nonché quello delle controllate aventi rilevanza strategica, con particolare riferimento al sistema di controllo interno e di gestione dei rischi".

In relazione a quanto sopra, si rende necessaria una riflessione sul contenuto della valutazione del Consiglio di Amministrazione, ossia se il Codice di Autodisciplina, quando richiama specificatamente il SCIGR con l'espressione "con particolare riferimento", intenda includerlo nella valutazione di adeguatezza dell'assetto organizzativo, amministrativo e contabile della società richiesta dal Codice Civile.

Il Codice di Autodisciplina integra il perimetro della valutazione rispetto a quanto indicato dal comma 3 dell'art. 2381. Se, da un lato, infatti il Codice Civile fa riferimento alla Società, dall'altro, il Codice di Autodisciplina richiede che la valutazione sia effettuata sull'emittente e sulle controllate aventi rilevanza strategica, specificando all'interno del Commento al Criterio applicativo I.C.1 che: "tale rilevanza può essere valutata con riferimento a criteri non solo dimensionali, cui dare conto nella relazione sul governo societario". Tuttavia, come già anticipato nel Capitolo I, la valutazione è lasciata all'Emittente che può utilizzare criteri sia qualitativi (es. rilevanza del business della società controllata rispetto agli obiettivi strategici del Gruppo) che quantitativi (es. ricavi, EBITDA, utile ante imposte, *transfer price*), di cui dovrà però dare indicazione e giustificazione nella relazione sul governo societario.

La valutazione del Sistema di Controllo Interno e di Gestione dei Rischi introdotta nel Criterio applicativo I.C.1 è ripresa ed integrata all'art. 7 del Codice di Autodisciplina, dedicato al SCIGR secondo cui il Consiglio di Amministrazione "valuta, con cadenza almeno annuale, l'adeguatezza del

sistema di controllo interno e di gestione dei rischi rispetto alle caratteristiche dell'impresa e al profilo di rischio assunto, nonché la sua efficacia"⁴⁸.

Il Codice esplicita quindi in merito al SCIGR, così come definito precedentemente, il termine di raffronto per la valutazione da parte del Consiglio: le caratteristiche dell'impresa (similmente a quanto definito con "la natura e le dimensioni dell'impresa" all'art. 2381, comma 5 cod. civ.) e il profilo di rischio assunto.

Al riguardo si ricorda che, nella ripartizione dei ruoli in merito al Sistema di Controllo Interno e Gestione dei Rischi, il Codice di Autodisciplina affida al Consiglio il compito di definire le linee di indirizzo del SCIGR⁴⁹. Le linee di indirizzo sono definite tenuto conto del profilo di rischio, determinato da parte del Consiglio stesso coerentemente con gli obiettivi strategici dell'impresa. Spetta pertanto al Consiglio di Amministrazione definire il profilo di rischio dell'organizzazione e spetta ad esso valutarne la coerenza con la strategia. Il Sistema di Controllo Interno e di Gestione dei Rischi è il mezzo per verificare che il profilo di rischio sia allineato agli obiettivi prefissati. La valutazione del SCIGR è quindi funzione della valutazione delle caratteristiche dell'impresa e del profilo di rischio assunto.

Il Codice di Autodisciplina introduce, inoltre, in aggiunta rispetto a quanto definito dal Codice Civile in merito alla valutazione dell'assetto organizzativo amministrativo e contabile, i riferimenti alla periodicità con la quale il Consiglio deve effettuare la propria valutazione (almeno annualmente) ed il documento nel quale l'Emittente può includere tali informazioni, la Relazione sul Governo Societario e gli Assetti Proprietari.

A tal proposito il *Format per la Relazione sul Governo Societario e gli Assetti Proprietari* (d'ora in avanti anche il *Format*), redatto da Borsa Italiana, che recepisce tutte le raccomandazioni del Codice di Autodisciplina, nella sezione dedicata al ruolo del Consiglio di Amministrazione, richiede di indicare nella relazione di *governance* se il Consiglio ha valutato, nel corso dell'esercizio, l'adeguatezza dell'assetto organizzativo, amministrativo e contabile con particolare riferimento al sistema di controllo interno e di gestione dei rischi⁵⁰; nella sezione dedicata al Sistema di Controllo Interno e di Gestione dei Rischi, è richiesto agli emittenti di indicare se il Consiglio ha valutato l'adeguatezza del SCIGR, nonché di descrivere, "in relazione al processo di informativa finanziaria (anche consolidata, ove applicabile) le principali caratteristiche dei sistemi di gestione dei rischi e controllo interno esistenti (ex art. 123-bis, comma 2, lett. b) del TUF)"⁵¹.

Al fine di esprimere tali valutazioni il Consiglio delibera in merito al perimetro delle società aventi rilevanza strategica e al profilo di rischio assunto. Tali delibere, unitamente alle linee di indirizzo strategico, ai piani industriali, al modello di *business*, alla struttura dei poteri, all'assetto societario, alle linee guida per l'assetto organizzativo, amministrativo e contabile e alle linee di indirizzo del sistema di controllo interno e di gestione dei rischi, definiti dal Consiglio di Amministrazione, delineano il più ampio modello di *governance* della Società.

⁴⁸ Codice di Autodisciplina, Criterio applicativo 7.C.1., lett. b).

⁴⁹ Codice di Autodisciplina, Criterio applicativo 7.C.1., lett. a): "Il Consiglio di Amministrazione, previo parere del comitato controllo e rischi [...] a) definisce le linee di indirizzo del sistema di controllo interno e di gestione dei rischi, in modo che i principali rischi afferenti all'emittente e alle sue controllate risultino correttamente identificati, nonché adeguatamente misurati, gestiti e monitorati, determinando inoltre il grado di compatibilità di tali rischi con una gestione dell'impresa coerente con gli obiettivi strategici individuati."

⁵⁰ *Format per la Relazione sul Governo Societario e gli Assetti Proprietari* - 4.3. Ruolo del Consiglio di Amministrazione: "Indicare se il Consiglio ha valutato l'adeguatezza dell'assetto organizzativo, amministrativo e contabile dell'Emittente e delle società controllate aventi rilevanza strategica predisposto dagli amministratori delegati, con particolare riferimento al sistema di controllo interno e di gestione dei rischi. In caso affermativo, illustrare brevemente l'iter di valutazione seguito".

⁵¹ *Format per la Relazione sul Governo Societario e gli Assetti Proprietari*: "Descrivere le principali caratteristiche del sistema di controllo interno e di gestione dei rischi (Criterio applicativo 7.C.1., lett. d). In relazione al processo di informativa finanziaria (anche consolidata, ove applicabile) descrivere le principali caratteristiche dei sistemi di gestione dei rischi e controllo interno esistenti (ex art.123-bis, comma 2, lettera b), TUF), sviluppando le informazioni richieste nell'Allegato 1."

2. I ruoli, le responsabilità ed i flussi informativi a supporto della valutazione del Consiglio di Amministrazione

La valutazione da parte del Consiglio di Amministrazione del SCIGR è supportata da diversi soggetti all'interno dell'organizzazione, ciascuno con definite competenze e responsabilità. Come già evidenziato nel Capitolo II, il Codice di Autodisciplina, nonché ulteriori fonti normative primarie⁵², individuano quali soggetti coinvolti nel SCIGR oltre al Consiglio di Amministrazione, il Comitato Controllo e Rischi, il Collegio Sindacale, il Dirigente Preposto alla redazione dei documenti contabili societari, uno o più Amministratori incaricati di presidiare il Sistema di Controllo Interno e di Gestione dei Rischi, il Responsabile *Internal Audit*, e altri ruoli e funzioni aziendali con specifici compiti in tema di controllo interno e gestione dei rischi (tra essi, il *Chief Risk Officer*, la funzione legale e *Compliance*⁵³, il responsabile del sistema di gestione della qualità, ed altri).

Resta inteso che, sebbene il Codice presupponga il coordinamento e l'interdipendenza dei diversi soggetti coinvolti nel SCIGR, rimane in capo alla Capogruppo l'onere di definire le modalità di tale coordinamento, i ruoli e le responsabilità di ciascun soggetto, nonché i principali flussi informativi a supporto del processo di valutazione periodica di adeguatezza del SCIGR, effettuata dal Consiglio di Amministrazione che, a tal fine, definisce in prima istanza le linee di indirizzo del sistema dei controlli.

La buona pratica prevista da Banca d'Italia per il settore finanziario a tal proposito, all'interno delle linee applicative dei flussi informativi nella disposizione del 2008 in materia di organizzazione e governo societario, richiede che le banche con appositi regolamenti disciplinino "le tempistiche, le forme e i contenuti della documentazione", "i soggetti tenuti ad inviare [...] flussi informativi agli organi aziendali, prevedendo in particolare che i responsabili di funzioni di controllo [...] devono riferire direttamente agli organi di controllo, di gestione e di supervisione strategica", "il contenuto minimo dei flussi informativi, includendo, tra l'altro, il livello e l'andamento dell'esposizione della banca a tutte le tipologie di rischio rilevanti [...] gli eventuali scostamenti rispetto alle politiche approvate dall'organo di supervisione strategica"⁵⁴.

Il Consiglio di Amministrazione, al fine di esprimere la propria valutazione di adeguatezza del SCIGR e dell'assetto organizzativo amministrativo e contabile, istituisce un Comitato Controllo e Rischi, con il compito di supportare con un'adeguata attività istruttoria le valutazioni del Consiglio di Amministrazione, assistendo lo stesso e fornendo specifici pareri non solo sull'adeguatezza del SCIGR ma anche sulla definizione delle linee guida del sistema.

⁵² Si vedano il TUF e il Codice Civile.

⁵³ Codice di Autodisciplina, Commento all'art.7 - Sistema di controllo interno e di gestione dei rischi: "Un ruolo di particolare rilevanza nell'ambito del sistema di controllo interno e di gestione dei rischi è normalmente ricoperto dalle funzioni legali e di compliance, con particolare riferimento al presidio del rischio legale e di non conformità, ivi incluso anche il rischio della commissione di illeciti penali a danno o nell'interesse dell'azienda."

⁵⁴ Disposizioni di vigilanza in materia di organizzazione e governo societario delle banche del 4 marzo 2008, par. 5. Flussi informativi che nelle Linee applicative indica:

"Con appositi regolamenti devono essere disciplinati almeno i seguenti aspetti:

- a) tempistica, forme e contenuti della documentazione da trasmettere ai singoli componenti degli organi necessaria ai fini dell'adozione delle delibere sulle materie all'ordine del giorno; i regolamenti dovranno definire anche i compiti e i doveri attribuiti ai presidenti degli organi stessi, in punto di: formazione dell'ordine del giorno; informazione preventiva ai componenti degli organi in relazione agli argomenti all'ordine del giorno; documentazione e verbalizzazione del processo decisionale; disponibilità *ex post* di detta documentazione; trasmissione delle delibere all'Autorità di vigilanza, quando previsto dalla normativa;
- b) individuazione dei soggetti tenuti a inviare, su base regolare, flussi informativi agli organi aziendali, prevedendo in particolare che i responsabili delle funzioni di controllo nell'ambito della struttura organizzativa della banca devono riferire direttamente agli organi di controllo, di gestione e di supervisione strategica;
- c) determinazione del contenuto minimo dei flussi informativi, includendo, tra l'altro, il livello e l'andamento dell'esposizione della banca a tutte le tipologie di rischio rilevanti (creditizi, di mercato, operativi, reputazionali, etc.), gli eventuali scostamenti rispetto alle politiche approvate dall'organo di supervisione strategica, tipologie di operazioni innovative e i rispettivi rischi."

L'attività istruttoria del Comitato Controllo e Rischi è funzione anche delle attività di controllo e delle relative valutazioni espresse dagli altri soggetti coinvolti nel sistema, svolgendo un ruolo di collettore dei flussi informativi provenienti dai tre livelli di controllo. L'attività di analisi della corretta progettazione e realizzazione del SCIGR viene infatti eseguita da parte del Comitato attraverso incontri dedicati con i soggetti preposti al controllo, al fine di comprendere e valutare i presidi di gestione dei rischi posti in essere, e attraverso l'analisi delle relazioni periodiche emesse in particolare da parte del Dirigente Preposto, dell'Organismo di Vigilanza e del Responsabile Internal Audit nonché da parte della Società di Revisione.

Il Dirigente Preposto, ai sensi dell'art. 154-*bis* del TUF, rilascia una dichiarazione, accompagnata agli atti e alle comunicazioni al mercato delle Società, nella quale attesta, tra le altre, l'adeguatezza e l'effettiva applicazione delle procedure amministrativo contabili summenzionate, oltretutto la corrispondenza dei documenti alle risultanze dei libri e delle scritture contabili e la loro idoneità a fornire una rappresentazione corretta e veritiera della situazione patrimoniale, economica e finanziaria. Nell'analisi svolta individua eventuali azioni correttive e piani di miglioramento da sottoporre alla valutazione del Consiglio.

L'Organismo di Vigilanza, identificabile anch'esso al secondo livello di controllo, in quanto organo a cui è affidato il compito di vigilare sull'osservanza ed il funzionamento del Modello di Organizzazione Gestione e Controllo *ex* D.Lgs. 231/01⁵⁵, predisponde periodicamente una relazione in riferimento alle attività svolte, al funzionamento e all'osservanza del modello, ad eventuali aspetti critici emersi nonché alla necessità di effettuare particolari interventi.

Qualora la società abbia istituito il *Chief Risk Officer*, deputato al presidio dei rischi in un'ottica integrata ed organica, il Consiglio di Amministrazione sarà destinatario di un'ulteriore relazione da parte di tale soggetto. Il *Chief Risk Officer* periodicamente predisponde una relazione in cui sono riportate le risultanze dell'attività di *risk assessment* evidenziando i rischi maggiormente rilevanti in termini di probabilità e impatto, i piani di trattamento dei rischi, l'analisi delle cause nonché gli elementi di mitigazione.

I soggetti con specifici ruoli nel monitoraggio dei rischi aziendali effettuano specifiche valutazioni dei rischi (*risk assessment*) e sono chiamati periodicamente, da parte del Comitato Controllo e Rischi a presentare i risultati di tali attività.

Il Responsabile *Internal Audit*, quale soggetto incaricato del controllo di terzo livello "verifica, sia in via continuativa sia in relazione a specifiche necessità e nel rispetto degli standard internazionali, l'operatività e l'idoneità del sistema di controllo interno e di gestione dei rischi, attraverso un piano di audit, approvato dal Consiglio di Amministrazione"⁵⁶. Il Responsabile *Internal Audit*, inoltre, predispose relazioni periodiche sulle attività di verifica svolte, le relative risultanze e le azioni intraprese per il loro contenimento. Le relazioni periodiche contengono, infine, "una valutazione sull'idoneità del sistema di controllo interno e di gestione dei rischi"⁵⁷. La valutazione periodica del SCIGR è effettuata prendendo in considerazione le risultanze delle attività svolte da parte delle altre

⁵⁵ Il decreto ha introdotto un regime di responsabilità amministrativa a carico della società per alcune fattispecie di reati commesse da amministratori, dirigenti o dipendenti nell'interesse o a vantaggio delle società stesse.

⁵⁶ Codice Autodisciplina, Criterio applicativo 7.C.5., lett. a): "Il responsabile della funzione di *internal audit*: a) verifica, sia in via continuativa sia in relazione a specifiche necessità e nel rispetto degli standard internazionali, l'operatività e l'idoneità del sistema di controllo interno e di gestione dei rischi, attraverso un piano di *audit*, approvato dal Consiglio di Amministrazione, basato su un processo strutturato di analisi e prioritizzazione dei principali rischi".

⁵⁷ Codice Autodisciplina, Criterio applicativo 7.C.5., lett. d): "Il responsabile della funzione di *internal audit*: [...] d) predispose relazioni periodiche contenenti adeguate informazioni sulla propria attività, sulle modalità con cui viene condotta la gestione dei rischi nonché sul rispetto dei piani definiti per il loro contenimento. Le relazioni periodiche contengono una valutazione sull'idoneità del sistema di controllo interno e di gestione dei rischi".

funzioni di controllo di primo e secondo livello su specifici aspetti del sistema, le cui risultanze sono trasmesse agli organi di *governance*⁵⁸. È inoltre richiesto all'*Internal Audit* di effettuare verifiche sull'affidabilità dei sistemi informativi utilizzati dalla Società, inclusi i sistemi di rilevazione contabile⁵⁹, affinché la Società possa assicurare l'affidabilità di tali sistemi in particolar modo nella rilevazione dei dati amministrativo contabili.

3. Il processo di valutazione

Il processo di informativa, così come descritto al paragrafo precedente, costituisce perciò la base di riferimento per l'espressione del giudizio di adeguatezza dell'assetto organizzativo, amministrativo e contabile della Società da parte del Consiglio di Amministrazione, anche per il tramite del Comitato Controllo e Rischi. Le valutazioni espresse dal Consiglio di Amministrazione richiedono il supporto di un processo codificato e strutturato, corroborato da un sistema articolato di flussi informativi al fine di garantire il coinvolgimento tempestivo di tutti gli attori del controllo interno.

I soggetti coinvolti riportano non solo un giudizio sintetico del Sistema di Controllo Interno di riferimento ma anche l'informativa di eventuali carenze emerse, fornendo una valutazione in merito alla rilevanza delle stesse, all'impatto sull'azienda nonché alle azioni di mitigazione da implementare.

Il Consiglio di Amministrazione effettua le proprie valutazioni secondo modalità ed approcci differenti a seconda della struttura e delle caratteristiche del Consiglio stesso nonché delle regole che ha definito, sulla base dei flussi informativi e di reporting sovra esposti, filtrati anche attraverso una attività istruttoria del CCR. In particolare, il CCR riceve i flussi informativi da parte delle funzioni di *compliance* e *governance* (es. relazione del Dirigente Preposto, relazione dell'Organismo di Vigilanza, ecc.), incaricate dei controlli di II livello, nonché la valutazione di idoneità e adeguatezza sul SCIGR da parte del Responsabile *Internal Audit*, incaricato del terzo livello di controllo.

Il Consiglio, demandato a fornire un giudizio sul SCIGR, valuterà autonomamente sulla base di un processo di valutazione definito, se le carenze riscontrate siano da ritenersi significative e di entità tale da inficiare l'adeguatezza del Sistema di Controllo Interno e di Gestione dei Rischi nel suo complesso. I risultati della valutazione del Consiglio sono riportati nella Relazione sulla *Governance* in un giudizio di adeguatezza o non adeguatezza del SCIGR, positivo o negativo.

Le migliori prassi internazionali in materia di sistema di controllo interno, prevedono che, in sede di valutazione, qualora il Consiglio ritenga che il giudizio di adeguatezza del Sistema di Controllo Interno sia non adeguato, indichi nella relazione sulla *governance* almeno i seguenti aspetti:

- le debolezze riscontrate;
- le azioni di mitigazione che saranno apportate;
- i criteri quali/quantitativi utilizzati;
- il processo di valutazione effettuato.

⁵⁸ Codice Autodisciplina, Criterio applicativo, 7.C.5., lett. f): "Il responsabile della funzione di *internal audit*: [...] f) trasmette le relazioni [...] ai presidenti del Collegio Sindacale, del Comitato Controllo e Rischi e del Consiglio di Amministrazione nonché all'Amministratore Incaricato del Sistema di Controllo Interno e di gestione dei Rischi".

⁵⁹ Codice Autodisciplina, Criterio applicativo, 7.C.5., lett. g): "Il responsabile della funzione di *internal audit*: [...] g) verifica, nell'ambito del piano di audit, l'affidabilità dei sistemi informativi inclusi i sistemi di rilevazione contabile".

4. Valutazione di eventuali carenze e approcci per la valutazione del Sistema di Controllo Interno e di Gestione dei Rischi

Nel panorama dei codici di *corporate governance* internazionali non è stato ad oggi identificato un *framework* di riferimento per la valutazione del SCIGR da parte del Consiglio di Amministrazione e per la valutazione delle carenze, qualora emerse.

Si riportano di seguito alcuni standard internazionali, con riferimento al sistema di controllo, che possono essere utili nel processo di valutazione.

Secondo il principio di revisione internazionale ISA Italia 265 (comunicazione delle carenze nel controllo interno ai responsabili delle attività di *governance* ed alla direzione), una carenza esiste quando:

- un controllo è configurato, messo in atto ovvero opera in modo tale da non consentire la prevenzione, o l'individuazione e la correzione, in modo tempestivo, di errori nel bilancio; ovvero
- non esiste un controllo necessario per prevenire, ovvero per individuare e correggere, in modo tempestivo, errori nel bilancio.

I principi di revisione internazionali ISA Italia (*International Standard on Auditing*) 265 e 315 possono essere utili da considerare nella valutazione del SCIGR, definendo, nell'ambito delle carenze individuate dal revisore, quali debbano essere comunicate ai responsabili delle attività di *governance* e alla direzione. In particolare, secondo tali principi, dovranno essere tempestivamente comunicate ai responsabili delle attività di *governance* le carenze significative individuate, e le stesse dovranno essere comunicate anche alla direzione "a meno che, nelle circostanze, risulti inappropriato comunicarle direttamente alla direzione"; dovranno essere comunicate, inoltre, alla direzione altre carenze individuate che "secondo il giudizio professionale siano sufficientemente importanti da meritare di essere portate all'attenzione della direzione".

Il *Public Company Accounting Oversight Board (PCAOB)*⁶⁰ all'interno del documento *Auditing Standard No. 5* individua un range di carenze riscontrabili nella valutazione del sistema di controllo da prendere in considerazione (*deficiencies, significant deficiencies e material weakness*)⁶¹, in funzione del loro impatto sull'attendibilità dei risultati esposti nell'informativa finanziaria.

⁶⁰ Il PCAOB è una organizzazione non-profit creata a seguito dell'emanazione del Sarbanes-Oxley Act nel 2002 negli U.S.A., al fine di sovrintendere alle attività di audit delle imprese pubbliche e di altri emittenti al fine di tutelare gli interessi degli investitori e promuovere l'interesse pubblico nella preparazione di report informativi, accurati e indipendenti di audit.

⁶¹ PCAOB, *Auditing Standard No. 5*: "A deficiency in internal control over financial reporting exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.

- A deficiency in design exists when (a) a control necessary to meet the control objective is missing or (b) an existing control is not properly designed so that, even if the control operates as designed, the control objective would not be met.

- A deficiency in operation exists when a properly designed control does not operate as designed, or when the person performing the control does not possess the necessary authority or competence to perform the control effectively."

"A material weakness is a deficiency, or a combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the company's annual or interim financial statements will not be prevented or detected on a timely basis."

"A significant deficiency is a deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness, yet important enough to merit attention by those responsible for oversight of the company's financial reporting."

Nel caso in cui la società identifichi una *material weakness* è opportuno che sia data informazione al mercato in merito alla natura della carenza, agli effetti sul bilancio nonché alle azioni correttive che la società ha avviato.

Uno dei più recenti approcci per la valutazione del SCIGR è quello sviluppato dal CoSO nella recente pubblicazione del 2013, *Internal Control – Integrated Framework*. Il modello individua, sulla base delle cinque componenti di analisi del sistema di controllo interno, 17 principi da prendere in considerazione per la progettazione, implementazione, gestione e valutazione dei sistemi di controllo⁶² ed una serie di strumenti di supporto (c.d. *point of focus*) al fine di garantire la corretta e completa attuazione dei principi. L'approccio si basa sul concetto che il Sistema, per essere efficace, deve garantire il funzionamento, in maniera integrata, di ciascuna componente e dei relativi principi. L'approccio sviluppa inoltre un insieme di strumenti guida per l'applicazione, il disegno e la valutazione dell'efficacia del sistema. Pertanto, in caso di "*major deficiency*", la società non potrà concludere positivamente in merito all'adeguatezza del Sistema di Controllo Interno.

In alternativa all'approccio sviluppato da CoSO, che risulta incentrato sulla presenza e sul funzionamento dei suddetti principi, è possibile fare riferimento ad un approccio, cosiddetto "*Maturity Model Approach*", che, oltre a valutare la presenza dei principi, fornisce una valutazione del livello di maturità del processo di gestione dei rischi da parte dell'organizzazione. La valutazione del livello di maturità del Sistema è funzionale al Consiglio di Amministrazione per valutare se il Sistema soddisfa le esigenze previste e per valutare se è necessario implementare eventuali azioni correttive al fine di raggiungere il livello desiderato. Secondo tale approccio sono stati sviluppati più modelli da parte di diverse organizzazioni, e sono state identificate differenti componenti a supporto della valutazione. Le scale di maturità costituiscono comunque lo strumento di riferimento per la valutazione.

⁶² Pur essendo focalizzato sul sistema di controllo interno e non sul SCIGR, tale *framework* potrebbe rappresentare uno spunto interessante per la strutturazione di uno strumento di valutazione dell'adeguatezza del SCIGR.

BIBLIOGRAFIA

- Beasley M., *Board and Audit Committee Involvement in Risk Management Oversight*, AICPA (American Institute of Certified Public Accountant's), 2010.
- Beasley M., Branson B. and Hancock B., *2015 Report on the current state of enterprise risk oversight*, AICPA, 2015.
- Borsa Italiana S.p.A., *Format per la relazione sul governo societario e gli assetti proprietari*, 2015.
- Borsa Italiana S.p.A., Comitato per la Corporate Governance, *Codice di Autodisciplina*, 2015.
- Caldwell J.E., *A framework for Board oversight of enterprise risk*, Canadian Institute of Chartered Accountants, 2012.
- Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili (CNDCEC), Norme di comportamento del Collegio Sindacale di Società quotate, del 15 Aprile 2015.
- Comitato per la Corporate Governance, *Codice di autodisciplina*, 2015.
- Committee of Sponsoring Organizations of the Treadway Commission (CoSO), *Board risk oversight – a progress report*, 2010.
- Committee of Sponsoring Organizations of the Treadway Commission (CoSO), *Effective Enterprise Risk Oversight - The Role of the Board of Directors*, 2009.
- Committee of Sponsoring Organizations of the Treadway Commission (CoSO), *Internal Control-Integrated Framework*, 2013.
- Committee of Sponsoring Organizations of the Treadway Commission (CoSO), *Enterprise Risk Management-Integrated Framework*, 2004.
- Financial Reporting Council (FRC), *Boards and Risk: A summary of discussions with companies, investors and advisers*, 2011.
- Financial Reporting Council (FRC), *Guidance on Audit Committees*, 2012.
- Financial Reporting Council (FRC), *Guidance on Board effectiveness*, 2011.
- Financial Reporting Council (FRC), *Guidance on Risk Management, Internal Control and Related Financial and Business Reporting*, 2014.
- Financial Reporting Council (FRC), *The UK Corporate Governance Code*, 2014.
- Gupta P.P., and Leech T.J., *Risk Oversight: Evolving Expectations for Boards*, EDPACS, 2014.
- Kaplan R.S. e Mikes A., *Managing Risks: A New Framework*, Harvard Business Review, 06.2012.
- International Corporate Governance Network (ICGN), *ICGN Corporate Risk Oversight Guidelines: The Role of the Board and Institutional Shareholders*, 2011.
- Leech T., *Board Oversight of Management's Risk Appetite and Tolerance*, EDPACS, 2012.

BIBLIOGRAFIA

Lipton M., Rosenblum S.A. and Cain K.L., *Risk Management and the Board of Directors—An Update for 2012*, The Harvard Law School Forum on Corporate Governance and Financial Regulation, 2012.

National Association of Corporate Directors (NACD), *Advisory Council on Risk Oversight*, 2014.

National Association of Corporate Directors (NACD), *Governance Challenges: 2013 and Beyond*, 2013.

National Association of Corporate Directors (NACD), *Risk Governance: Balancing Risk and Reward*, 2009.

Organisation for Economic Co-operation and Development (OECD), *Methodology for assessing the implementation of the OECD principles on corporate governance*, 2007.

Organisation for Economic Co-operation and Development (OECD), *G20/OECD Principles of Corporate Governance*, 2015.

Rumsfeld D., *Known and Unknown*, Penguin Group, 2011.

Il presente Quaderno è stato realizzato dal Gruppo di Ricerca Governance, e in particolare hanno collaborato:

Stefano Fortunato	(KPMG)
Adele Lorenzoni	(Assirevi)
Raffaele Fontana	(Deloitte & Touche)
Fabrizio Marcucci	(Deloitte & Touche)
Nicolò Zanghi	(KPMG)
Cinzia Damiano	(PricewaterhouseCoopers)
Alfredo Gallistru	(PricewaterhouseCoopers)
Ginevra De Romanis	(Reconta Ernst & Young)
Alberto Girardi	(Reconta Ernst & Young)

e con la collaborazione degli avvocati Aldo Sacchi, Nicoletta Mazzali, Lorenzo Danese dello Studio Legale Galbiati, Sacchi e Associati.

ORGANI SOCIALI ASSIREVI

ASSEMBLEA DELLE ASSOCIATE

AGKNSERCA S.n.c.; Axis S.r.l.; Baker Tilly Revisa S.p.A.; BDO S.p.A.; BDO Italia S.p.A.; Deloitte & Touche S.p.A.; KPMG S.p.A.; PKF Italia S.p.A.; PricewaterhouseCoopers S.p.A.; Prorevi Auditing S.r.l.; Reconta Ernst & Young S.p.A.; RIA Grant Thornton S.p.A.; Trevor S.r.l.; UHY Bompani S.r.l..

COMPONENTI DEL CONSIGLIO DIRETTIVO

CONSIGLIERE	VICE CONSIGLIERE	ASSOCIATA
Mario Boella (P)		
Davide Trincherò	Giacomo Bianchi	Baker Tilly Revisa S.p.A.
Simone Del Bianco (VP e T)	Rosanna Vicari	BDO Italia S.p.A.
Stefano Dell'Orto	Fabio Pompei	Deloitte & Touche S.p.A.
Luca Ferranti	Angelo Pascali	KPMG S.p.A.
Umberto Giacometti	Fioranna Negri	PKF Italia S.p.A.
Andrea Toselli	Maurizio Lonati	PricewaterhouseCoopers S.p.A.
Simone Scettri (VP)	Massimo Antonelli	Reconta Ernst & Young S.p.A.
Luca Saccani	Giancarlo Pizzocaro	RIA Grant Thornton S.p.A.
Severino Sartori	Paolo Foss	Trevor S.r.l.
Enrico Minetti	Andrea Fantechi	UHY Bompani S.r.l.

(P) Presidente
(VP) Vice Presidente
(T) Tesoriere

Direttore Responsabile: Mario Boella
Autorizzazione Tribunale di Milano n° 269 del 24 aprile 2008

ASSIREVI

ASSIREVI – Associazione Italiana Revisori Contabili – è un'associazione privata senza scopo di lucro fondata nel 1980. L'Associazione è iscritta nel Registro delle persone giuridiche della Prefettura di Milano con il n.1261.

Possono aderire all'Associazione le società di revisione operanti in Italia iscritte al Registro di cui all'art. 6 e ss. D.Lgs. 39/2010 e relative disposizioni attuative.

Assirevi riunisce oggi 14 società di revisione, che costituiscono attualmente la maggior parte delle società che svolgono la revisione degli Enti di Interesse Pubblico. Attualmente i professionisti che operano nell'ambito dell'attività di revisione svolta dalle Associate sono circa 6.000, con una presenza distribuita su tutto il territorio nazionale.

Assirevi promuove e realizza l'analisi scientifica di supporto all'adozione dei principi di revisione (norme etico professionali, norme tecniche di svolgimento della revisione contabile e norme di stesura della relazione di revisione), nonché lo studio dell'evoluzione della legislazione e della regolamentazione. Inoltre, è impegnata nella risoluzione di problematiche professionali, giuridiche e fiscali di comune interesse delle Associate.

In tale contesto, collabora con le Istituzioni e le Autorità Pubbliche, con gli organismi professionali, e con altri organismi ed enti nella determinazione e nell'aggiornamento dei principi di revisione e dei principi contabili e nella loro diffusione.

Promuove la diffusione della conoscenza degli studi sviluppati presso le Associate attraverso diversi strumenti, tra i quali principalmente iniziative di formazione, aggiornamento e informazione su norme, leggi, decreti, regolamenti e ogni altra notizia necessaria all'attività di revisione.

Inoltre, Assirevi sostiene e realizza iniziative, studi e pubblicazioni che favoriscano la maggiore conoscenza e diffusione dell'attività di revisione contabile.

*finito di stampare
nel mese di febbraio 2016*

3LB srl
Osnago (Lc)