associazione riconosciuta
ned community
amministratori non esecutivi e indipendenti

Il Comitato Controllo e Rischi: ruolo, funzioni e agenda per un'efficace governance

marzo 2025

In collaborazione con

KPMG

Il presente documento è stato realizzato da Nedcommunity
nell'ambito del "Reflection Group - La governance in materia di rischi e di controlli"

*Si ringrazia il **Reflection Group***
(Graziella Capellini, Rosalba Casiraghi, Diana D'Alterio,
Carolyn Dittmeier - coordinatrice, Patrizia Giangualano - coordinatrice, Leonardo Scimmi)

*e i membri del team **KPMG***
(Jennifer Altmeyer Cucolo, Aldo Cinquegrana, Antonio Mansi, Alessandra Rizzo, Nicolò Zanghi)

Indice

Premessa: evoluzione del contesto di riferimento

Il dibattito sulla corporate governance si è arricchito nel corso degli anni a livello internazionale a fronte di cambiamenti del contesto economico e sociale e di crisi finanziarie che hanno portato a ridefinire il ruolo dell'Organo di amministrazione[1] e i suoi meccanismi di funzionamento. Questo si è tradotto in nuova normativa (partendo dalle policy e direttive UE, poi riflesse nelle leggi nazionali), modifiche dei documenti di autoregolamentazione (ad esempio i Codici di Corporate Governance per le società quotate, primi tra tutti quello UK e quello italiano) e frequenti aggiornamenti nei riferimenti di leading practice internazionali (tra i principali, il framework del COSO[2], i principi internazionali stabiliti dal G20/OECD[3], gli standard definiti dall'ISO[4] e dal Financial Stability Board[5]). Ad integrazione, l'entrata in vigore del decreto legislativo 125/2024, in attuazione della Corporate Sustainability Reporting Directive (cd. CSRD), ha introdotto un progressivo rafforzamento del processo di reporting e controllo interno e il relativo coinvolgimento degli organi di amministrazione e controllo.

I seguenti tre principi chiave accomunano i riferimenti normativi e le leading practice in relazione al ruolo dell'Organo di amministrazione:

1. L'Organo di amministrazione deve promuovere la definizione di una strategia di lungo termine che tenga conto delle istanze degli azionisti e di un ampio gruppo di stakeholder, inclusa la comunità nel suo complesso.
2. Nella supervisione delle attività riferite ai rischi, l'Organo di amministrazione deve promuovere un'ampia informativa al mercato anche sui temi di sostenibilità e una gestione dei rischi ESG in ottica di lungo periodo.
3. L'Organo di amministrazione deve garantire la coerenza tra strategia, governance e cultura aziendale.

In considerazione dell'aumentata complessità, e della varietà e rilevanza dei rischi che ormai ogni organizzazione deve affrontare, Nedcommunity intende fornire un supporto ai componenti del Comitato Controllo e Rischi (di seguito anche "CCR") nella pianificazione delle attività necessarie ad ottemperare alle responsabilità poste in capo a tale Comitato attraverso una nuova versione dell'Agenda del Comitato Controllo e Rischi.

Il presente documento (aggiornato rispetto alla pubblicazione del 2021) tiene conto delle più recenti evoluzioni sia normative che di leading practice e di contesto ambientale.

Tra le prime, citiamo in particolare il Codice di Corporate Governance delle Società Quotate alla Borsa Italiana (aggiornato nel gennaio 2020) e le indicazioni della Banca Centrale Europea e della European Banking Authority[6]; mentre tra le leading practice, le varie linee guida di COSO:

- nel 2017 l'aggiornamento *Enterprise Risk Management - Integrating with strategy and performance*,
- nel 2018 il paper *Applying enterprise risk management to Environmental, Social and Governance-related risks* e
- nel 2023 la guida supplementare intitolata *Achieving Effective Internal Control of Sustainability Reporting (ICSR)*.

Il ruolo del CCR si è in parte ampliato e in parte aperto ad una maggiore trasversalità, perseguita anche attraverso l'interazione con gli altri comitati endoconsiliari.

---

1 Per Organo di amministrazione si intende (i) nel sistema tradizionale ed il sistema monistico il Consiglio di amministrazione (ii) nel sistema dualistico il Consiglio di Gestione

2 Committee of Sponsoring Organizations of the Treadway Commission o COSO (https://www.coso.org/) ha pubblicato due principali framework "Internal Control" (del 1992, aggiornato nel 2013) e l'"Enterprise Risk Management" (del 2004, aggiornato nel 2017). Inoltre, COSO pubblica paper su temi emergenti.

3 I principi di Corporate Governance dell'OECD.

4 ISO, International Organization for Standardization, ha pubblicato standard di risk management nel 2018.

5 FSB, Financial Stability Board, fornisce un riferimento ampio in continuo aggiornamento.

6 Banca Centrale Europea (BCE), *Guida sui rischi climatici e ambientali. Aspettative di vigilanza in materia di gestione dei rischi e informativa,* pubblicata il 27 novembre 2020 e Banca d'Italia "Aspettative di vigilanza sui rischi climatici e ambientali" dell'8 aprile 2022.
Gli "Orientamenti EBA" pubblicati dall'*European Banking Authority* (EBA) il 29 maggio 2020 in materia di concessione e monitoraggio dei prestiti.
Inoltre, l'EBA ha pubblicato il 2/07/21 un aggiornamento delle Linee Guida ("*Final Report on Guidelines on internal governance under Directive 2013/36/EU*") in relazione alla governance degli enti creditizi, in particolare per quanto riguarda la diversità di genere, il riciclaggio di denaro, il finanziamento rischio terroristico e la gestione dei conflitti di interesse, anche nell'ambito di finanziamenti e altre operazioni con componenti dell'Organo di amministrazione e loro parti correlate.
Banca d'Italia ha pubblicato il 29/11/2022 orientamenti sulla composizione e sul funzionamento dei consigli di amministrazione delle LSI ("*less significant institutions*", ossia le banche meno significative).

Il presente documento si articola in quattro capitoli e in una Appendice. Il primo capitolo rappresenta un'introduzione sul Sistema di Controllo Interno e Gestione dei Rischi e suoi principali framework di riferimento. Il secondo descrive il ruolo del CCR nella governance aziendale, incluso il confronto tra i compiti del CCR e dell'Organo di controllo. Il terzo riporta le principali funzioni del CCR. Il quarto riporta una proposta di massima di agenda annuale delle attività e la loro tempistica, che dovrà essere adattata ad ogni specifica realtà in considerazione della sua operatività, complessità e dimensione. Segue una Appendice, contenente la bibliografia con riferimenti per ulteriori approfondimenti.

1 Il Sistema di controllo interno e di gestione dei rischi (SCIGR)

Il Sistema di Controllo Interno e di Gestione dei Rischi (di seguito "SCIGR") è costituito "dall'insieme delle regole, procedure e strutture organizzative finalizzate ad una effettiva ed efficace identificazione, misurazione, gestione e monitoraggio dei principali rischi, al fine di contribuire al successo sostenibile della società"[7].

Il livello di maturità dei sistemi di controllo interno e di gestione dei rischi raggiunto negli ultimi anni, anche a seguito dello sviluppo delle leading practice e del tentativo di aumentare il livello di resilienza delle organizzazioni rispetto all'incertezza del contesto e alla volatilità dei mercati, ha posto l'attenzione degli standard setter sulla necessità di monitorare il livello di cultura aziendale quale elemento alla base della *good governance* e del rispetto delle regole.

In tale contesto, la cultura del rischio[8] si riferisce ai valori e agli atteggiamenti condivisi all'interno di un'organizzazione riguardo alla gestione del rischio. Una cultura del rischio efficace promuove la consapevolezza e la responsabilità a tutti i livelli dell'organizzazione e rappresenta un elemento chiave nella gestione efficace dei rischi a supporto dei processi decisionali. Le società dovrebbero sviluppare una cultura del rischio robusta ed estesa a tutta l'organizzazione, basata sulla piena comprensione e su una visione olistica dei rischi e dei processi con cui tali rischi vengono gestiti.

A livello internazionale, il COSO ha integrato il "modello delle tre linee"[9] nell'ambito dei modelli di controllo interno e di risk management (cfr. pag. 1) definendo e classificando, in funzione del grado di autonomia e indipendenza, i contributi delle varie funzioni aziendali.

Le Tre Linee del SCIGR

L'"architettura" dei controlli poggia sui **controlli di linea** (anche detti "di primo livello" o "diretti"), rivolti ad assicurare il corretto svolgimento delle operazioni. Si tratta dei controlli effettuati dalle strutture operative (ad esempio, controlli di tipo gerarchico) ovvero incorporati nelle stesse procedure oppure eseguiti nell'ambito dell'attività di back-office.

Le funzioni aziendali alle quali sono affidati i cosiddetti **controlli "di secondo livello**" svolgono compiti di monitoraggio e gestione dei tipici rischi aziendali (si pensi ai rischi operativi, finanziari, di mercato, di compliance, etc.). Tali controlli concorrono alla definizione delle metodologie di identificazione e misurazione dei rischi, verificano il rispetto dei limiti assegnati alle varie funzioni operative e monitorano nel continuo la coerenza dell'operatività delle singole aree produttive con gli obiettivi di rischio-rendimento prestabiliti nonché la conformità ai modelli di controllo codificati nelle policy e nelle procedure. In tale contesto un importante ruolo è attribuito alle funzioni di controllo cd. "di secondo livello": la funzione di Risk Management, in qualità di facilitatore dei processi di identificazione, misurazione, gestione, reporting dei rischi; la funzione di Compliance che presidia gli ambiti normativi più rilevanti ovvero quelli dai quali possono generarsi rischi per la reputazione o di tipo sanzionatorio; altre funzioni di controllo dedicate al presidio di specifici rischi quali, ad esempio, antiriciclaggio, anticorruzione, salute, sicurezza e ambiente, cybersecurity, ecc. Le funzioni di controllo di secondo livello svolgono quindi il ruolo di standard setter definendo i modelli di controllo relativi ai suddetti rischi rilevanti e monitorando sistematicamente, con un approccio risk-based, l'adeguatezza e l'effettivo funzionamento degli stessi.

Una posizione centrale viene, poi, riconosciuta alla funzione di **internal audit** (o revisione interna), investita dell'attività di controllo **"di terzo livello"**. Si tratta di un'attività, indipendente e obiettiva, di "assurance" e di consulenza, finalizzata al miglioramento dell'efficacia e dell'efficienza dell'organizzazione. Essa assiste l'organizzazione aziendale nel perseguimento dei relativi obiettivi tramite un approccio professionale sistematico, volto a generare valore aggiunto, in quanto diretto a valutare e migliorare i processi di controllo, di gestione dei rischi e di corporate governance, individuando andamenti anomali, violazioni delle procedure e della regolamentazione, nonché valutando la funzionalità del complessivo sistema dei controlli interni. In linea con i nuovi Standard professionali dell'Internal Audit globalmente riconosciuti (www.aiiaweb.it), il Purpose dell'Internal Auditing è infatti: "L'Internal Auditing rafforza la capacità

---

7 Codice di Corporate Governance di Borsa Italiana - Art. 6.

8 La BCE ha avviato una consultazione pubblica sulla bozza di "Draft guide on governance and risk culture" (luglio 2024). La Guida riflette l'attenzione della BCE verso organi di gestione diversificati ed efficaci che è una priorità di vigilanza del Meccanismo di vigilanza unico (SSM) e definisce le aspettative di vigilanza in materia di governance e cultura del rischio delle banche sottoposte a vigilanza.
Nel dettaglio, la Guida chiarisce le aspettative delle autorità di vigilanza in merito alla composizione e al funzionamento degli organi di gestione e dei comitati di gestione, definisce i ruoli e le responsabilità delle funzioni di controllo interno, sottolinea l'importanza della cultura del rischio e delinea le aspettative in merito ai quadri di propensione al rischio delle banche.

9 L'Institute of Internal Audit ha definito "The IIA's Three Lines Model" secondo cui gli organi di governo, il management, le strutture di controllo e gestione dei rischi, nonché l'Internal Audit, non sono suddivisi in ruoli rigidi. Le "linee" differenziamo le aree di responsabilità: 1) *Responsabilità* da parte dell'organo di governo nei confronti delle parti interessate per il controllo; 2) *Azioni* (inclusa la gestione del rischio) da parte della direzione per raggiungere gli obiettivi organizzativi; 3) *Assurance e consulenza* da parte dell'Internal Audit per fornire informazioni dettagliate, fiducia e incoraggiamento al miglioramento continuo.

dell'organizzazione di creare valore e di mantenerlo nel tempo, fornendo al Board e al management assurance, advisory, approfondimenti e previsioni, in modo indipendente, obiettivo e risk-based".

L'Internal Auditing è maggiormente efficace quando la funzione Internal Audit è indipendente e risponde direttamente all'Organo di amministrazione e gli Internal Auditor sono liberi da qualsiasi condizionamento e si impegnano a effettuare valutazioni obiettive.

Il quadro degli attori del sistema di controllo è completato dagli organi posti in posizione apicale nell'ambito della società.

Nel dettaglio, si tratta, di:

- l'Organo di amministrazione, che svolge un ruolo di indirizzo e di valutazione dell'adeguatezza del sistema; in particolare (i) definisce le linee di indirizzo del sistema di controllo interno e di gestione dei rischi in coerenza con le strategie della società (ii) valuta, con cadenza almeno annuale, l'adeguatezza del medesimo sistema rispetto alle caratteristiche dell'impresa e al profilo di rischio assunto, nonché la sua efficacia (iii) definisce i princìpi che riguardano il coordinamento e i flussi informativi tra i diversi soggetti coinvolti nel sistema di controllo interno e di gestione dei rischi al fine di massimizzare l'efficienza del sistema stesso, ridurre le duplicazioni di attività, cogliere eventuali omissioni e garantire un efficace svolgimento dei compiti propri delle funzioni e degli organi di controllo;
- il Comitato Controllo e Rischi (CCR), istituito all'interno dell'Organo di amministrazione e composto da soli amministratori non esecutivi in maggioranza indipendenti, con il compito di supportare le valutazioni e le decisioni dell'Organo di amministrazione relative al sistema di controllo interno e di gestione dei rischi e all'approvazione delle relazioni periodiche di carattere finanziario e di sostenibilità;
- il *Chief executive officer*, che dà esecuzione alle linee di indirizzo definite dall'Organo 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, nonché curandone l'adattamento alla dinamica delle condizioni operative e del panorama legislativo e regolamentare;
- l'Organo di controllo, che vigila sull'efficacia del sistema di controllo interno e di gestione dei rischi.

Il modello delle tre linee si realizza in modo efficace tramite l'integrazione e il coordinamento delle sue componenti. Nel Codice di Corporate Governance, il Principio XX preme sull'importanza del coordinamento tra i diversi soggetti coinvolti nel SCIGR e attribuisce all'Organo di amministrazione il compito di definire "i princìpi che riguardano il coordinamento e i flussi informativi tra i diversi soggetti coinvolti nel sistema di controllo interno e di gestione dei rischi al fine di massimizzare l'efficienza del sistema stesso, ridurre le duplicazioni di attività e garantire un efficace svolgimento dei compiti propri dell'Organo di controllo".

L'Organo di amministrazione al fine di fornire le **linee di indirizzo del SCIGR** definisce un framework normativo finalizzato a una sua disciplina integrata e coerente con i requisiti normativi applicabili (es. nel settore finanziario), con il Codice di Corporate Governance e con altre leading practice (es. COSO Framework) con l'obiettivo di:

- consolidare e strutturare in modo organico ed efficiente il ruolo delle differenti componenti del SCIGR;
- identificare i flussi informativi in materia di SCIGR e le modalità di coordinamento e collaborazione tra gli attori;
- nei gruppi aziendali, definire un modello di relazione (direzione e coordinamento) tra la società e le società controllate in materia di SCIGR.

In particolare, con riferimento ai gruppi di società, l'Organo di amministrazione della capogruppo definisce le linee di indirizzo e valuta l'adeguatezza ed efficacia del SCIGR a livello di gruppo. Pertanto, nell'ambito della propria attività di direzione e coordinamento nei confronti delle società controllate, la capogruppo emana e diffonde le linee di indirizzo e il relativo modello di attuazione a cui le società controllate devono attenersi, nell'istituzione e mantenimento del relativo SCIGR.

I NUOVI RUOLI NELL'AMBITO DELLA GOVERNANCE A FRONTE DELL'INTRODUZIONE DELLA CSRD

Con l'entrata in vigore del decreto legislativo 125/2024 la rendicontazione di sostenibilità diventa parte integrante della relazione di gestione e le aziende italiane, in funzione della loro dimensione, saranno tenute a conformarsi progressivamente a stringenti standard di sostenibilità definiti a livello europeo (European Sustainability Reporting Standard), che implicheranno la creazione o il rafforzamento di sistemi di controllo interno robusti in grado di garantire la correttezza e qualità delle informazioni di sostenibilità che acquisiscono la stessa rilevanza di quelle finanziarie.

L'Organo di amministrazione e l'Organo di controllo, nell'assumere un ruolo sempre più attivo nella supervisione di dati e processi, sono tenuti ad approfondire la propria conoscenza sui temi ESG ed eventualmente adottare procedure rilevanti anche ai fini sanzionatori.

Organo di amministrazione

- È responsabile dell'approvazione della Rendicontazione di Sostenibilità inclusa nella Relazione sulla gestione del gruppo, nonché di garantire che le informazioni richieste all'art. 4 del D.Lgs. 125/2024 siano fornite in conformità a quanto previsto dal citato decreto. Nell'adempimento di tale obbligo, agisce secondo criteri di professionalità e diligenza.

Comitato Controllo e Rischi

- Supporta le decisioni dell'Organo di amministrazione in merito alle questioni di sostenibilità connesse all'esercizio dell'attività dell'impresa e alle sue dinamiche di interazione con tutti gli stakeholder, incluse le questioni di sostenibilità risultate rilevanti dalla c.d. analisi di doppia rilevanza e anche dei rischi ESG ad esse connessi.
- Supporta l'Organo di amministrazione nel monitoraggio delle procedure, nonché dei progressi compiuti nel perseguimento degli obiettivi volti a gestire i rischi, gli impatti e le opportunità rilevanti presidiati dalle Funzioni aziendali competenti.
- Esamina preliminarmente all'Organo di amministrazione la Dichiarazione sulla sostenibilità.

Organo di controllo

- Vigila sull'osservanza delle disposizioni stabilite nel D.Lgs. 125/2024 e previste in materia di redazione della Dichiarazione sulla Sostenibilità e ne riferisce nella Relazione dell'Organo di controllo all'Assemblea degli azionisti.

In particolare, in ottemperanza all'Art. 19 del D.Lgs. n. 39/2010 (in attuazione della direttiva 2006/43/CE, relativa alle revisioni legali dei conti annuali e dei conti consolidati), l'Organo di controllo è incaricato di:

- informare l'Organo di amministrazione dell'esito della revisione legale e dell'esito dell'attività di attestazione della rendicontazione di sostenibilità e trasmettere a tale organo la relazione aggiuntiva di cui all'articolo 11 del Regolamento europeo 537/2014, corredata da eventuali osservazioni;
- monitorare il processo di informativa finanziaria e della rendicontazione di sostenibilità, compresi l'utilizzo del formato elettronico, nonché presentare le raccomandazioni o le proposte volte a garantirne l'integrità e la trasparenza;
- controllare l'efficacia dei sistemi di controllo interno della qualità, di gestione del rischio dell'impresa, della revisione interna, per quanto attiene all'informativa finanziaria e alla rendicontazione di sostenibilità;
- monitorare la revisione legale del bilancio d'esercizio e del bilancio consolidato, nonché l'attività di attestazione concernente la rendicontazione di sostenibilità;
- verificare e monitorare l'indipendenza degli incaricati alla revisione legale e alla revisione di sostenibilità, in particolare per quanto concerne l'adeguatezza della prestazione di servizi diversi dalla revisione all'ente sottoposto a revisione;
- essere responsabile della procedura volta alla selezione degli incaricati alla revisione legale.

Amministratore delegato

Attesta, con apposita Relazione, che la Dichiarazione sulla sostenibilità inclusa nella Relazione sulla gestione è stata redatta conformemente agli standard di rendicontazione applicati ai sensi della Direttiva 2013/34/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, e del decreto legislativo adottato in attuazione dell'articolo 13 della legge 21 febbraio 2024, n. 15 e con le specifiche adottate a norma dell'articolo 8, paragrafo 4, del regolamento (UE) 2020/852 del Parlamento europeo e del Consiglio, del 18 giugno 2020.

Dirigente preposto

Attesta, con apposita Relazione, che la Dichiarazione sulla sostenibilità inclusa nella Relazione sulla gestione è stata redatta conformemente agli standard di rendicontazione applicati ai sensi della Direttiva 2013/34/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, e del decreto legislativo adottato in attuazione dell'articolo 13 della legge 21 febbraio 2024, n. 15 e con le specifiche adottate a norma dell'articolo 8, paragrafo 4, del regolamento (UE) 2020/852 del Parlamento europeo e del Consiglio, del 18 giugno 2020.

Team ESG o funzione di sostenibilità

- Indipendentemente dalla collocazione aziendale lasciata alla scelta dell'azienda il team ESG o la funzione di sostenibilità supporta l'Organo di amministrazione e l'Amministratore Delegato nell'individuazione dei temi di sostenibilità potenzialmente rilevanti per il Gruppo e nella definizione delle relative linee strategiche e politiche di sostenibilità, anche ai fini della definizione e aggiornamento dell'analisi di doppia rilevanza. Propone all'Amministratore Delegato e all'Organo di amministrazione la realizzazione delle iniziative rilevanti in ambito ESG e ne monitora l'implementazione anche a livello di Gruppo.
- E' periodicamente informato dei risultati inerenti il monitoraggio dei progressi compiuti nel perseguimento degli obiettivi connessi agli impatti, ai rischi e alle opportunità rilevanti, presidiati dalle singole funzioni competenti, prima di sottoporre tale informativa al Comitato Controllo e Rischi e all'Organo di amministrazione della Capogruppo.
- Predispone la Dichiarazione sulla Sostenibilità preventivamente alla presentazione al Comitato Controllo e Rischi e all'Organo di amministrazione.

1.a) I framework internazionali di riferimento

Il Codice di Corporate Governance delle Società Quotate alla Borsa Italiana[10] (gennaio 2020) – (di seguito il "Codice") è allineato con l'evoluzione delle leading practice internazionali che portano in evidenza l'importanza di un approccio integrato di analisi del rischio con la strategia e con i fattori di sostenibilità, tenendo conto di un ampio gruppo di *stakeholder*. In particolare, i modelli di leading practice internazionali aiutano a definire in modo più articolato le aspettative sul ruolo del CCR e forniscono dei riferimenti su che modelli appoggiarsi per svolgere le attività definite dai regolatori. Il Codice lascia libera scelta su quale modello di leading practice nazionale o internazionale usare, ma richiede di fare riferimento esplicito, nella Relazione sul Governo Societario, a quale scelta sia stata compiuta.

Il modello di leading practice internazionale più diffuso e longevo è quello sviluppato dalla Committee of Sponsoring Organizations of the Treadway Commission (COSO) che ha fornito due famiglie di linee guida:

- il COSO - Internal Control-Integrated Framework (cd. "COSO Framework o COSO I);
- il COSO - Enterprise Risk Management-Integrated Framework, (cd COSO ERM Framework).

COSO Frameworks

Entrambi concepiti come modelli integrati, tra le differenti componenti e rispetto agli obiettivi:

- il primo si focalizza sul Sistema di Controllo Interno (con enfasi su financial reporting, efficacia/efficienza operativa e conformità). Il COSO Framework (2013) ha costituito in questi anni il modello di riferimento più importante sia per le autorità di vigilanza (standard setter) sia per le imprese, sia per le funzioni, tra cui il dirigente preposto per l'informativa finanziaria. In particolare, il COSO Framework definisce il Sistema di Controllo Interno come "un processo messo in atto dal Consiglio di Amministrazione, dal management e da tutto il personale, volto a fornire una ragionevole garanzia sul raggiungimento dei seguenti obiettivi: efficacia ed efficienza delle attività operative;

[10] Promosso dal Comitato Corporate Governance (2020).

attendibilità delle informazioni (interne ed esterne, finanziarie e di sostenibilità); conformità alle leggi e alle norme vigenti cui l'impresa è soggetta". Il Sistema di Controllo Interno è articolato in 5 componenti di controllo (Ambiente di Controllo, Valutazione del Rischio, Attività di Controllo, Informazione e Comunicazione e Attività di Monitoraggio) e risulta efficace se, con riferimento a uno o più obiettivi, tutte e cinque le componenti esistono nel disegno e nell'implementazione del complessivo sistema aziendale e funzionano in maniera integrata nell'operatività;

- il secondo, ERM, riferito alla Gestione dei Rischi e relativo Sistema di Controllo Interno, incorpora i principi di COSO I e pone inoltre uno specifico focus sugli obiettivi strategici dell'impresa, nonché sul processo di identificazione, misurazione e valutazione dei rischi.

L'impostazione dei suddetti framework integra il ruolo del management coerentemente con i principi del modello delle tre linee di controllo, codificato a livello internazionale e riportato in numerosi *guidance paper*.

I framework del COSO possono essere implementati congiuntamente oppure applicati singolarmente riportando tali decisioni nella Relazione sul Governo Societario.

Di particolare rilevanza per l'evoluzione del ruolo del CCR sono i recenti aggiornamenti in tema di gestione del rischio. Con la pubblicazione nel 2017 del Framework *Enterprise Risk Management (ERM) - Integrating with strategy and performance,* l'ente COSO porta in evidenza l'importanza della supervisione da parte dell'Organo di amministrazione sull'attività di risk management ("board risk oversight") collegandola con la strategia e con la capacità di risposta dell'organizzazione ai rischi emergenti. I temi trattati includono: (i) l'integrazione dell'ERM con il business model e la generazione di valore; (ii) l'importanza di catturare segnali di rischio in una fase preliminare e di avere meccanismi per prendere decisioni in situazioni di grande incertezza; (iii) l'attenzione per la collaborazione e trasversalità. Inoltre, nel 2018 il paper *Applying enterprise risk management to Environmental, Social and Governance-related risks* ha ulteriormente approfondito le modalità per incorporare i fattori ESG nelle analisi di rischio, considerando anche i rischi emergenti e la necessità di creare una maggiore resilienza nelle organizzazioni e di avere adeguate strategie di comunicazione e reporting.

Tra gli altri aggiornamenti, si segnala che nel 2019 COSO ha pubblicato anche un approfondimento del modello ERM, particolarmente utile per il CCR, su come le organizzazioni si possono proteggere da attacchi cyber: *Managing cyber risk in a digital age.*

Inoltre, nel 2023 COSO ha pubblicato uno studio comprensivo di una guida supplementare intitolata *Achieving Effective Internal Control of Sustainability Reporting (ICSR)*, basata sul COSO Internal Control-Integrated Framework, che fornisce diversi spunti interessanti per le organizzazioni nel processo di adeguamento del proprio Sistema di Controllo Interno alla luce delle novità in ambito ESG. La guida ribadisce il ruolo di oversight dell'Organo di amministrazione rispetto alla definizione e all'attuazione di processi e controlli relativi alle attività aziendali e alla rendicontazione di sostenibilità.

Principi OECD

Nella stessa direzione, l'OECD individua nel documento *Principles of Corporate Governance 2023* tra le aree di notevole rilevanza da inglobare nel quadro generale di gestione dei rischi aziendali:

- i rischi correlati alle tematiche di sostenibilità (Environmental, Social and Governance);
- i temi di sicurezza digitale;
- i fattori esogeni quali crisi sanitarie, tensioni geo-politiche, interruzioni della catena di approvvigionamento;
- la gestione del rischio fiscale, in termini di gestione degli adempimenti tributari e tax compliance.

In tale ambito, l'OECD sottolinea come l'Organo di amministrazione, responsabile della definizione e supervisione di un adeguato SCIGR, dovrebbe assicurare adeguati processi di gestione dei rischi che funzionino ex ante, garantendo la prevenzione e mitigazione degli eventi negativi, ed ex post, consentendo un'adeguata gestione delle situazioni di crisi al manifestarsi di un evento negativo, preservando la continuità aziendale.

A titolo indicativo, nel riquadro sottostante vengono sintetizzati gli elementi frequenti nelle leading practice internazionali cui il CCR è invitato a tenere conto nell'esercizio del suo ruolo.

PRINCIPALI RIFERIMENTI ALLE "LEADING PRACTICE" INTERNAZIONALI[11]

Le leading practice, evolute negli ultimi anni, pongono l'attenzione su alcune caratteristiche del Comitato Controllo e Rischi: una forte indipendenza di giudizio rispetto all'operato del management - con cui instaura una dialettica costruttiva - e una particolare attenzione agli aspetti di governance, di gestione del rischio e di cultura aziendale[12].

Il Financial Reporting Council (FRC) ha pubblicato, nel gennaio 2024, una nuova versione del Codice di governo societario UK[13]. Tra le principali novità è stato definito che l'Organo di amministrazione debba stabilire e mantenere un efficace sistema di gestione dei rischi e di controllo interno ed effettuare una valutazione approfondita dei rischi emergenti e principali per determinare la soglia di rischio che l'impresa è disposta a tollerare per raggiungere obiettivi strategici a lungo termine. Il Board deve assicurare una sorveglianza continua dei sistemi di controllo interno e della gestione dei rischi e deve riesaminarne, almeno una volta all'anno, la loro efficacia. In termini di trasparenza, la relazione annuale deve contenere le seguenti informazioni:

- una descrizione dettagliata del modo in cui l'Organo di amministrazione ha monitorato ed esaminato l'efficacia dei dispositivi di controllo interno e di gestione dei rischi;
- una dichiarazione attestante l'efficacia dei controlli effettuati alla data di chiusura dell'esercizio;
- una descrizione dettagliata di tutti i controlli e le disfunzioni constatati alla data di chiusura dell'esercizio, nonché una descrizione delle misure adottate o proposte al consiglio per migliorare i dispositivi di controllo interno e di gestione dei rischi.

A tal fine, il Board designa l'Audit Committee che ha la responsabilità di occuparsi di questioni inerenti ai processi di rendicontazione finanziaria, alla gestione del rischio e al relativo controllo interno.

Stante la complessità delle organizzazioni e del portafoglio rischi, l'Audit Committee potrebbe essere affiancato da un Risk Committee per supportare il Board nella supervisione della gestione del rischio. In tal caso la complessità introduce la necessità di coordinamento e interazione tra i Comitati.

11 Si veda la bibliografia essenziale nell'Appendice 2. Si fa in particolare riferimento a COSO (2017) e FSB (2014). Si veda anche Nedcommunity (2013) e AIFIRM (2020) per una lettura e visione d'insieme.
12 Peter Drucker "Culture eats strategy for breakfast"
13 Financial Reporting Council - UK Corporate Governance Code (January 2024).

2 Il Comitato Controllo e Rischi nella governance della società

Il Codice di Corporate Governance di Borsa Italiana, in linea con le leading practice internazionali, identifica nell'Organo di amministrazione il responsabile ultimo della **strategia** della società e del gruppo ad essa facente capo, in coerenza con il perseguimento del **successo sostenibile**, indicato come primo principio.

Risk management ai fini del "Successo Sostenibile"

Il successo sostenibile è definito come "l'obiettivo che guida l'azione dell'Organo di amministrazione e che si sostanzia nella creazione di valore nel lungo termine a beneficio degli azionisti, tenendo conto degli interessi degli altri stakeholder rilevanti per la società".

La parola "sostenibile" vuole esprimere la capacità di generare valore (e quindi profitti) nel tempo, aspetto che richiede anche l'attenzione alle esigenze dei vari stakeholder: non si genera valore nel lungo periodo se non si attraggono e sviluppano i talenti adeguati, se non si cura la qualità della catena di fornitura, se non si riduce l'impatto sull'ambiente dovuto al cambiamento climatico. Il Codice di Corporate Governance richiama tutto l'Organo di amministrazione e tutti i Comitati endoconsiliari a porre il successo sostenibile come obiettivo che guida le scelte e i comportamenti. Il Codice richiede che il successo sostenibile sia il filo conduttore di tutte le attività dell'Organo di amministrazione e dei suoi Comitati, dalla strategia alle remunerazioni, al controllo e alla gestione dei rischi.

Per quanto concerne la gestione del rischio, l'Organo di amministrazione *"definisce la natura e il livello di rischio compatibile con gli obiettivi strategici della società, includendo nelle proprie valutazioni tutti gli elementi che possono assumere rilievo nell'ottica del successo sostenibile della società*[14]*"*.

Il Codice di Corporate Governance promuove un approccio strategico del ruolo del CCR: l'obiettivo principale del CCR è il supporto all'Organo di amministrazione nel processo di identificazione, valutazione e gestione dei rischi in ottica di successo sostenibile. L'analisi del Sistema di Controllo Interno e Gestione dei Rischi è uno dei mezzi per perseguire l'obiettivo di gestione del rischio.

Un altro elemento del Codice è l'attenzione per l'informativa di sostenibilità e il ruolo del CCR nelle attività a favore dell'Organo di amministrazione propedeutiche all'approvazione della relazione di sostenibilità.

Questo aspetto amplia l'agenda del CCR e richiede attenzione alle modalità di attuazione del recente Decreto Legislativo 125/2024[15] sulla reportistica di sostenibilità, in particolare in relazione al processo che porta alla formazione dei dati e alla rispondenza agli standard di rendicontazione di sostenibilità internazionali, anche quando il presidio sulla struttura e sul contenuto di tale reportistica sia affidato ad un altro Comitato.

In sintesi, il CCR nel suo ruolo di comitato consultivo, risponde all'esigenza di rafforzare la governance della società, garantendo all'Organo di amministrazione un efficace esercizio dell'attività di supervisione sulla componente esecutiva e permettendo di addivenire in modo più informato e consapevole alle deliberazioni attinenti in generale alla gestione dei rischi in ottica integrata e in relazione agli obiettivi strategici, alla valutazione del sistema di controlli interni, nonché a quelle relative all'approvazione delle relazioni periodiche finanziarie e di sostenibilità.

Il CCR deve sempre essere consapevole del proprio ruolo all'interno del sistema di governance e monitorare l'evoluzione e le raccomandazioni espresse dalle istituzioni coinvolte nell'analisi del governo societario, prime tra tutte il Comitato per la Corporate Governance[16] il cui presidente annualmente porta all'attenzione delle società emittenti aspetti di miglioramento. Inoltre, il CCR terrà conto dell'attività di altri Comitati a cui sono attribuiti eventuali compiti inerenti alla Sostenibilità. Si coordinerà in modo opportuno con il Comitato dedicato alla Remunerazione al fine di assicurare che i sistemi di remunerazione nel contesto aziendale specifico non impattino negativamente sull'ambiente di controllo e, in particolare, non incentivino un'eccessiva presa di rischio oltre il livello predefinito di risk appetite.

---

14 Raccomandazione 1 c) del Codice.

15 Il Decreto Legislativo 6 settembre 2024, n. 125, pubblicato Il 10 settembre 2024 in Gazzetta Ufficiale, recepisce la Corporate Sustainability Reporting Directive (CSRD), in vigore dal 5 gennaio 2023 in sostituzione della precedente "Non Financial Reporting Directive – NFRD" (Direttiva 2014/95/UE).

16 La relazione annuale del Comitato per la Corporate Governance analizza le modalità di adesione al Codice da parte delle società quotate e offre importanti spunti per il Comitato Controllo e Rischi. Inoltre, indicazioni di leading practice vengono dai singoli componenti del Comitato per la Corporate Governance – Borsa Italiana S.p.A, ABI, ANIA, Assonime, Confindustria, Assogestioni.

2.a) I sistemi di governo societario (tradizionale, monistico e dualistico) e la configurazione del CCR

In tema di amministrazione e controllo di società sono previsti tre diversi sistemi di governo societario, fra i quali i soci possono scegliere, la cui previsione è di regola indicata nello statuto:

- il sistema tradizionale di amministrazione e controllo è caratterizzato dalla presenza di un organo di gestione (amministratore unico o consiglio di amministrazione) e un Organo di controllo che si identifica con il "Collegio sindacale";
- il modello cd. "dualistico" (di origini tedesche) si contraddistingue perché la gestione societaria è interamente rimessa all'Organo di gestione, mentre il controllo è affidato al Consiglio di sorveglianza;
- il modello, cd. "monistico" (di origine anglosassone) è caratterizzato dalla sola presenza del Consiglio di Amministrazione che istituisce al suo interno un Comitato per il controllo.

Tradizionale

Nel sistema tradizionale, l'Assemblea dei Soci nomina l'Organo di amministrazione nella forma di Amministratore Unico oppure di Consiglio di Amministrazione (CdA), il Collegio Sindacale e, con il parere del Collegio Sindacale, il soggetto incaricato della revisione legale dei conti (controllo contabile). La gestione dell'impresa spetta in via esclusiva agli amministratori, che compiono le operazioni necessarie per l'attuazione dell'oggetto sociale, deliberando su tutti gli argomenti che non siano per legge riservati alla competenza dell'assemblea, nel rispetto, in ogni caso, delle eventuali autorizzazioni che da parte di quest'ultima fossero eventualmente richieste dallo statuto per il compimento dei loro atti[17]. L'Organo di amministrazione può allora compiere non solo le attività che costituiscono in sé espressione dell'oggetto sociale[18], ma anche attività necessarie alla sua attuazione. Il Collegio Sindacale, Organo di controllo proprio del sistema tradizionale, assume funzioni sostanzialmente limitate al controllo dell'amministrazione. Spetta infatti ad un revisore contabile esterno, o ad una società di revisione, il controllo contabile della Società. Il Collegio Sindacale ha il compito di "vigilare"[19] sull'attività gestoria nel suo complesso, in particolare sull'osservanza della legge e dello statuto, da parte degli amministratori nel porre in essere i fatti di gestione (c.d. controllo di legalità) e sul rispetto dei principi di corretta amministrazione, con particolare riferimento: all'adeguatezza dell'assetto organizzativo, amministrativo e contabile adottato dalla società e al concreto funzionamento di detto assetto (controllo di correttezza gestionale).

Dualistico

Il sistema dualistico, tradizionalmente adottato in Germania (e per questo detto anche "modello renano") prevede che la governance delle S.p.A sia affidata ad un Consiglio di Sorveglianza (CdS) e ad un Consiglio di Gestione (CdG). Tale sistema prevede che l'Assemblea dei Soci nomini il Consiglio di Sorveglianza mentre al Consiglio di Sorveglianza è demandata la nomina del Consiglio di Gestione. L'Assemblea dei Soci nomina anche il soggetto incaricato del controllo contabile. La disciplina del Consiglio di Gestione corrisponde in gran parte a quella del CdA del sistema tradizionale.

Monistico

Il sistema monistico, di matrice statunitense (detto anche "modello angloamericano"), prevede che la governance delle S.p.A. venga affidata al Consiglio di Amministrazione e ad un Comitato per il Controllo sulla Gestione, costituito al suo interno. Il sistema monistico prevede che l'Assemblea dei Soci nomini il Consiglio di Amministrazione e che quest'ultimo nomini successivamente il Comitato per il Controllo sulla Gestione. L'Assemblea dei Soci nomina, infine, il soggetto incaricato del controllo contabile. Tale sistema è caratterizzato dal fatto di non avere un organo di controllo separato dall'organo di gestione, ma costituito al suo interno. Rispetto al sistema tradizionale al Comitato per il controllo sono attribuite sostanzialmente le medesime funzioni attribuite al Collegio Sindacale[20].

A seconda della scelta del sistema di amministrazione e di controllo, rispetto alla quale il Codice di Corporate Governance risulta neutrale, controllo contabile e controllo gestionale vengono modulati diversamente. Il controllo contabile riguarda la regolarità delle scritture e dei documenti attinenti alla registrazione e documentazione delle operazioni di gestione (corrispondenza del bilancio alle risultanze contabili); il controllo sulla gestione consiste, invece, nella verifica dell'osservanza dei principi di corretta amministrazione da parte degli amministratori. Il controllo gestionale può essere fatto dal Collegio sindacale, dal Consiglio di sorveglianza o dal Comitato per il Controllo sulla Gestione, a seconda del modello di governo adottato dalla società.

17 Cfr. art. 2364, n.5 c.c.
18 Cfr. art. 2328 2° comma n.3 c.c.
19 Ex art. 2403 c.c.
20 Cfr. art. 2409-octiesdecies c.c.

Nelle società che adottano il modello societario monistico o dualistico, le funzioni del Comitato Controllo e Rischi del modello tradizionale *("supportare le valutazioni e le decisioni dell'Organo di amministrazione relative al sistema di controllo interno e di gestione dei rischi e all'approvazione delle relazioni periodiche finanziarie e di sostenibilità"*) possono essere attribuite all'Organo di controllo[21].

2.b) Composizione e regolamento del CCR

In virtù della tipologia di responsabilità, il CCR deve avere determinati **requisiti di indipendenza** e **competenza**:

"Il comitato controllo e rischi è composto da soli amministratori non esecutivi, in maggioranza indipendenti ed è presieduto da un amministratore indipendente.

Il comitato possiede nel suo complesso un'adeguata competenza nel settore di attività in cui opera la società, funzionale a valutare i relativi rischi; almeno un componente del comitato possiede un'adeguata conoscenza ed esperienza in materia contabile e finanziaria o di gestione dei rischi"[22].

Come regolamentare il CCR

Al fine di una migliore organizzazione dei lavori, il CCR definisce un proprio **regolamento**, approvato dall'Organo di amministrazione, in cui sono esplicitati la composizione, i compiti e le modalità di gestione delle riunioni (ruolo del segretario, modalità di convocazione e condivisione documenti). Nel regolamento vengono inoltre definite le modalità di interazione sinergica con gli altri organi coinvolti nel controllo societario e con altri comitati endoconsiliari quali ad esempio, Operazioni Parti Correlate, Remunerazione e Governance. Per quanto riguarda il confronto con l'attività dell'Organo di controllo, che offre spunti di sinergia, si rimanda al par. "2.d Confronto tra CCR e Organo di controllo".

Il CCR identifica i flussi informativi che devono essere allo stesso indirizzati (oggetto, frequenza, contenuto, ecc.), ferma restando la possibilità di accedere, senza restrizioni, ad eventuali informazioni aziendali integrative rilevanti. Il CCR inoltre decide se invitare il CEO e/o il Presidente della Società quando il loro contributo può essere utile ad una più consapevole istruttoria da parte del Comitato su alcuni aspetti di controllo o gestione dei rischi.[23] È opportuno un intervento del CEO in CCR almeno una volta all'anno in occasione della valutazione da parte del CCR dell'adeguatezza del SCIGR, in virtù del ruolo del CEO definito dal Codice[24]. La presenza del CEO potrebbe essere valutata anche nel contesto dell'istruttoria del CCR in ambito dell'analisi dei rischi, in particolare quelli collegati al piano strategico.

Infine, il CCR può avvalersi di consulenti esterni, con le modalità previste dal Regolamento, qualora ritenga opportuno approfondire certi temi o ricevere un'opinione indipendente. A questo fine il Regolamento deve prevedere che il CCR abbia a disposizione un proprio budget.

Per l'organizzazione dei compiti del CCR, è buona ed opportuna pratica la predisposizione di un **piano annuale** che preveda una distribuzione delle attività nel corso dell'anno in funzione degli eventi societari di rilievo (quali ad esempio: approvazione reportistica finanziaria e di sostenibilità; approvazione Relazione sul Governo Societario, discussione piano strategico). La tempistica delle riunioni è molto importante in quanto consente di avere un'utile interazione con il management e gli organi coinvolti nel controllo e di contribuire nei momenti critici della vita societaria **ponendo le domande giuste al momento giusto**. Nel capitolo 4 si fornisce una proposta di massima di un'agenda annuale del CCR che copre i vari ambiti di responsabilità.

Rolling Agenda del CCR

2.c) I Flussi verso l'Organo di amministrazione e con gli altri comitati endo-consiliari

Uno degli elementi più significativi alla base della governance aziendale è senz'altro rappresentato dallo scambio di informazioni: l'Organo amministrativo deve, infatti, poter disporre di un flusso informativo costante ed essere, a propria volta, in grado di elaborare prontamente gli elementi informativi necessari a guidare in senso evolutivo la dinamica dell'impresa. La trasparenza informativa sui fatti della gestione aziendale ha acquisito una tale incisività valoriale nell'ambito della corporate governance da imporre alle società quotate di dotarsi di strutture capaci di facilitare la circolazione e la fruibilità delle informazioni rilevanti.

---

21 Cfr. raccomandazione 32, c) Codice di Corporate Governance.

22 Raccomandazione 35 del Codice di Corporate Governance. I requisiti sono raccomandati anche dalla "Financial Reporting Council's Guidance on Audit Committees".

23 In diverse società, viene esteso un invito permanente come osservatore al Presidente (qualora indipendente), anche nell'ottica di adempiere al suo ruolo nella governance.

24 Raccomandazione 34 B: "*Il CEO dà esecuzione alle linee di indirizzo definite dall'Organo 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, nonché curandone l'adattamento alla dinamica delle condizioni operative e del panorama legislativo e regolamentare*".

I pareri del CCR

In particolare, il Comitato Controllo e Rischi, in virtù del proprio ruolo di supporto all'Organo di amministrazione con funzione di supervisione strategica in materia di rischi e sistema di controlli interni, esprime pareri su:

- definizione e approvazione degli indirizzi strategici e delle politiche di governo dei rischi e specifici aspetti inerenti alla identificazione dei principali rischi aziendali per assicurare che siano accuratamente valutati anche i rischi e i profili connessi a fattori ESG al fine di favorire il successo sostenibile della società;
- attuazione del piano industriale con riferimento al profilo di rischio aziendale compatibile con gli obiettivi strategici;
- proposta di nomina/revoca del Responsabile Internal Audit, nonché sull'adeguatezza delle risorse assegnate a quest'ultimo per l'espletamento delle proprie responsabilità;
- programmi di attività (compreso il piano di audit) e le relazioni periodiche della funzione Internal Audit indirizzate al Consiglio di Amministrazione;
- rispetto delle "condizioni essenziali" per consentire la piena efficacia della funzione Internal Audit[25];
- corretto utilizzo dei principi contabili per la redazione dei bilanci d'esercizio e consolidato (valutandone anche l'omogeneità), e a tal fine si coordina con il dirigente preposto alla redazione dei documenti contabili e con l'Organo di controllo;
- idoneità dell'informazione periodica, finanziaria e di sostenibilità, a rappresentare correttamente il modello di business, le strategie della società, l'impatto della sua attività e le performance conseguite e contenuto dell'informazione periodica di sostenibilità rilevante ai fini del sistema di controllo interno e di gestione dei rischi.

La centralità del rischio nell'esecuzione delle funzioni del CCR consente allo stesso di essere informato su materie trasversali rispetto agli ambiti di azione propri di altri Comitati, ad esempio tematiche organizzative, di remunerazione, sostenibilità.

Sinergie con altri Comitati

A tal proposito, il CCR potrebbe confrontarsi con altri comitati endoconsiliari (ad esempio Comitato Nomine, Comitato Remunerazioni, Comitato Parti Correlate, Comitato Sostenibilità) in merito agli aspetti relativi all'organizzazione (es. piani di successione, politica di remunerazione) e rilevanti ai fini della complessiva valutazione circa l'adeguatezza del SCIGR oppure rispetto a questioni relative alle operazioni con Parti Correlate oppure ai fini di esame dei principali rischi di natura ESG e Climate Change nonché i relativi piani di azione finalizzati alla loro mitigazione. A titolo esemplificativo il CCR, attraverso idonei scambi di informazione con il Comitato Remunerazione, può aumentare la sua consapevolezza in merito all'importanza della politica di bonus e incentivazione in base al raggiungimento degli obiettivi sfidanti del budget e quindi richiedere maggiori approfondimenti sull'ambiente interno e di controllo in ambito.

La costituzione e l'azione coordinata di Comitati endoconsiliari con funzioni consultive, può supportare il Board e rafforzare l'assetto di corporate governance della società. Il mandato, la composizione e il funzionamento degli eventuali Comitati devono essere definiti dal Board che mantiene la responsabilità collegiale delle decisioni assunte a livello aziendale[26].

2.d) Confronto tra CCR e Organo di controllo

Un **confronto tra i compiti attribuiti al CCR[27] e quelli attribuiti all'Organo di controllo**[28] potrebbe agevolare un maggiore coordinamento delle rispettive attività.

---

25 Rif Global Internal Audit Standards (2024), https://www.aiiaweb.it/system/files/2024-08/240730_GIAS_ITA_def_1.pdf.

26 Principi di Corporate Governance del G20/OECD - Cap. V, par. E The responsibilities of the board (2023).

27 Nelle società che adottano il modello societario "one-tier" o "two-tier", le funzioni del CCR possono essere attribuite all'Organo di controllo (Cfr. raccomandazione 32, c) Codice di Corporate Governance).

28 L'Organo di controllo o "Comitato per il controllo interno e la revisione contabile" si identifica con:
a) il collegio sindacale;
b) il consiglio di sorveglianza negli enti che adottano il sistema di amministrazione e controllo dualistico, a condizione che ad esso non siano attribuite le funzioni di cui all'articolo 2409-terdecies, primo comma, lettera f- bis), del codice civile, ovvero un comitato costituito al suo interno. In tal caso, il comitato è sentito dal consiglio di sorveglianza in merito alla raccomandazione di cui all'articolo 16, comma 2, del Regolamento europeo. Almeno uno dei componenti del medesimo comitato deve essere scelto tra gli iscritti nel Registro;
c) il comitato per il controllo sulla gestione negli enti che adottano il sistema di amministrazione e controllo monistico.

La disciplina dell'Organo di controllo delle società quotate risulta composta dalla combinazione di differenti fonti normative: le disposizioni contenute nel D.Lgs. 24 febbraio 1998, n. 58 (TUF) devono coordinarsi con quelle del codice civile e con le numerose regole e istruzioni emanate dalla Consob e dalle autorità di vigilanza in specifici settori di attività, così come dalle Norme di comportamento pubblicate dal Consiglio Nazionale dei Dottori Commercialisti ed Esperti Contabili[29] nonché le importanti indicazioni fornite dal Codice di Corporate Governance in relazione al funzionamento del sistema di controllo interno e di gestione del rischio.

Il riconoscimento del ruolo dell'Organo di controllo quale presidio avanzato di un più corretto ed efficiente governo societario trova una consacrazione nel Codice di Corporate Governance che assegna espressamente a tale organo il ruolo di vigilanza sull'efficacia del sistema di controllo interno e di gestione dei rischi.

La vigilanza svolta dall'Organo di controllo si realizza sul rispetto dei principi di corretta amministrazione, sull'adeguatezza dell'assetto organizzativo, del sistema di controllo interno e gestione dei rischi, del sistema amministrativo-contabile, sull'attuazione delle regole di governo societario, sull'informativa di sostenibilità e sull'adeguatezza delle procedure per la regolamentazione delle operazioni con parti correlate.

Il ruolo di vigilanza sulla conformità alle norme, allo statuto, alle procedure interne differenzia l'Organo di controllo dal CCR, il quale svolge essenzialmente un ruolo di supporto all'Organo amministrativo nella valutazione - anche di merito - sull'adeguatezza degli assetti e sull'andamento della gestione. Pur rilevando il ruolo distinto del Comitato che partecipa alla funzione gestoria, seppure con un ruolo di "garanzia", diretto al miglior funzionamento del sistema di controllo interno, al principio di coordinamento e alla mitigazione di possibili duplicazioni), il Codice prevede la partecipazione necessaria alle riunioni del CCR del Presidente dell'Organo di controllo (o di altro suo componente all'uopo designato) e la partecipazione (sebbene facoltativa) degli altri componenti dell'Organo di controllo[30].

Nell'**Appendice 1** sono dettagliate, per ambito di responsabilità, le funzioni del CCR e dell'Organo di controllo, facendo anche riferimento alla normativa specifica. In linea di massima:

Appendice 1
Il Confronto

- l'Organo di controllo effettua un controllo di maggiore approfondimento in relazione ai processi relativi al lavoro e agli esiti della società di revisione, in base alle responsabilità di legge attribuiti a tale organo;
- il CCR prende atto dei pareri e delle osservazioni dell'Organo di controllo;
- l'Organo di controllo effettua una vigilanza sul funzionamento del CCR come pure dell'Organo di amministrazione e degli altri comitati;
- l'Organo di controllo acquisisce elementi dal CCR che contribuiscono allo svolgimento del proprio ruolo e responsabilità.

Un ottimale coordinamento tra questi due organi favorisce la corretta circolazione delle informazioni endoconsiliari e consente di migliorare l'efficienza del complessivo sistema dei controlli interni.

Di fatto in molte società quotate si è diffusa la prassi di tenere riunioni congiunte tra CCR e Organo di controllo, con l'obiettivo di semplificare ed efficientare il flusso informativo e il coordinamento[31].

Questo coordinamento è reso ancora più esplicito per gli istituti bancari.

2.e) Composizione e funzionamento del CCR in ambito finanziario

Per gli istituti finanziari, sono previsti requisiti più dettagliati relativi al CCR e alle sue funzioni, in coerenza con i principi e le linee guida emanati dalle autorità di vigilanza internazionali in materia di internal governance, a seguito delle crisi finanziarie che hanno coinvolto alcuni istituti in diversi Paesi.

---

29 CNDCEC - Norme di comportamento del collegio sindacale di società quotate (21 dicembre 2023).

30 La raccomandazione 37 del Codice di Corporate Governance cita: "L'Organo di controllo e il Comitato Controllo e Rischi si scambiano tempestivamente le informazioni rilevanti per l'espletamento dei rispettivi compiti. Il presidente dell'Organo di controllo, o altro componente da lui designato, partecipano ai lavori del comitato controllo e rischi".

31 A tale scopo i Presidenti del CCR e dell'Organo di controllo concordano in anticipo l'ordine del giorno e le date degli incontri congiunti e il Segretario del CCR mette a disposizione la documentazione relativa al CCR contestualmente a tutti i componenti del CCR e dell'Organo di controllo.

Settore bancario e creditizio

Con riferimento al settore bancario e creditizio, le prerogative e funzioni del CCR relative al controllo dei rischi sono disciplinate da specifiche disposizioni in materia di controlli interni emanate ai sensi dell'articolo 53 del testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo 1° settembre 1993, n. 385 (Testo Unico Bancario, TUB)[32].

La composizione, il mandato, i poteri (consultivi, istruttori, propositivi), le risorse disponibili e i regolamenti interni dei comitati sono chiaramente definiti; l'istituzione dei comitati non deve comportare una limitazione dei poteri decisionali e della responsabilità degli organi aziendali al cui interno essi sono costituiti.

Ciascun comitato è composto, di regola, da 3-5 componenti, tutti non esecutivi e in maggioranza indipendenti; ove sia presente un consigliere eletto dalle minoranze, esso fa parte di almeno un comitato. I comitati devono distinguersi tra loro per almeno un componente. I lavori di ciascun comitato sono coordinati da un presidente scelto tra i componenti indipendenti.

Il presidente del comitato non può coincidere con il presidente dell'Organo con funzione di supervisione strategica o con il presidente di altri comitati.

I componenti del comitato devono possedere conoscenze, competenze ed esperienze tali da poter comprendere appieno e monitorare le strategie e gli orientamenti al rischio della banca. Il comitato deve potersi avvalere di esperti esterni e - ove necessario - interloquire direttamente con le funzioni di revisione interna, controllo dei rischi e conformità alle norme.

Il CCR svolge funzioni di supporto all'organo con funzione di supervisione strategica in materia di rischi e sistema di controlli interni.

In tale ambito, particolare attenzione deve essere riposta dal CCR per tutte quelle attività strumentali e necessarie affinché l'organo con funzione di supervisione strategica possa addivenire ad una corretta ed efficace determinazione del *Risk Appetite Framework* (o "RAF") – strumento richiesto per le banche - e delle politiche di governo dei rischi.

Normativa EBA

L'EBA ha pubblicato il 02/07/2021 un aggiornamento delle Linee Guida[33] in relazione alla governance degli enti creditizi, in particolare per quanto riguarda la diversità di genere, il riciclaggio di denaro, il finanziamento rischio terroristico e la gestione dei conflitti di interesse, anche nell'ambito di finanziamenti e altre operazioni con componenti dell'Organo di amministrazione e loro parti correlate, nelle quali sono rappresentate le caratteristiche e le attribuzioni del CCR a supporto dell'Organo di amministrazione e dell'Organo di gestione.

In particolare, il CCR dovrebbe:

- fornire consulenza e assistenza all'Organo di amministrazione relativamente al monitoraggio della strategia in materia di rischio e della propensione al rischio, sia correnti che future (tenendo in considerazione tutte le tipologie di rischi, per garantire che siano in linea con la strategia aziendale, gli obiettivi, la cultura societaria e i valori dell'ente), nonché nel sorvegliare l'attuazione della strategia in materia di rischio e i limiti corrispondenti stabiliti;
- sorvegliare l'attuazione delle strategie per la gestione del capitale e della liquidità – nonché per tutti gli altri rischi pertinenti, quali i rischi di mercato, di credito, operativi (inclusi i rischi legali e informatici) e i rischi reputazionali, al fine di valutare la loro idoneità rispetto alla strategia in materia di rischio e alla propensione al rischio approvate – e l'allineamento tra tutti i prodotti e i servizi finanziari rilevanti offerti ai clienti, il modello di business e la strategia in materia di rischio;
- fornire all'Organo di amministrazione le raccomandazioni sugli adeguamenti necessari alla strategia in materia di rischio risultanti, fra le altre cose, da modifiche al modello di business, sviluppi di mercato o raccomandazioni formulate dalla funzione di gestione dei rischi, nonché pareri sulla nomina di consulenti esterni da impiegare per ottenere pareri o assistenza;
- riesaminare alcuni possibili scenari (inclusi gli scenari di stress) per valutare in che modo il profilo di rischio dell'ente reagirebbe a eventi esterni e interni, nonché valutare le raccomandazioni dell'Internal Audit e/o dei revisori esterni e assicurare che siano svolte adeguate attività di follow-up volte ad accertare che sia stato dato seguito all'attuazione appropriata dei relativi piani di rimedio.

[32] Si cita in particolare la Circolare Banca d'Italia 285 del 17 dicembre 2013 "Disposizioni di Vigilanza per le Banche" e s.m.i.
[33] "Final Report on Guidelines on internal governance under Directive 2013/36/EU".

Il CCR dovrebbe collaborare con gli altri comitati le cui attività possano ripercuotersi sulla strategia in materia di rischio (ad es. il Comitato per il Controllo Interno e il Comitato Remunerazioni come già accennato) e comunicare regolarmente con le funzioni di controllo interno, in particolare con la funzione Risk Management.

Banca d'Italia

Inoltre, la Banca d'Italia ha pubblicato il 29/11/2022 dei propri orientamenti sulla composizione e sul funzionamento dei consigli di amministrazione delle LSI ("*less significant institutions*", ossia le banche meno significative), a seguito di un'indagine trasversale sugli assetti di governo societario che l'Autorità di Vigilanza ha condotto nel 2020 su composizione e funzionamento dei board.

Con riferimento al ruolo del CCR, che svolge una funzione cruciale nel supportare l'azione dell'organo con funzione di supervisione strategica (e.g. facilitando la comprensione da parte del CdA delle informazioni trasmesse dalle funzioni di controllo, favorendo l'assunzione di decisioni consapevoli in materia di gestione di rischi e sistema di controlli interni, etc.), è emerso che un'organizzazione efficiente e una pianificazione adeguata dei lavori di tale Comitato e del suo confronto con l'Organo di amministrazione contribuiscono in misura significativa a migliorare la gestione dei rischi.

In particolare, la Banca d'Italia suggerisce come buona prassi che il CCR:

- si riunisca con regolarità e con sufficiente anticipo rispetto alle riunioni dell'Organo di amministrazione, eventualmente coinvolgendo i responsabili delle funzioni di controllo (quando ritenuto opportuno per il proficuo svolgimento delle riunioni);
- valuti l'opportunità di predisporre report che diano chiara evidenza dell'impatto sulla situazione della banca delle proposte in discussione, al fine di supportare in modo efficace l'adeguata comprensione dei profili di rischio da parte dell'Organo di amministrazione;
- riceva e/o trasmetta l'eventuale documentazione in tempo utile prima della riunione dell'Organo di amministrazione, così da consentire un'analisi compiuta da parte dei consiglieri.

Normativa bancaria sulla Sostenibilità

Tra i riferimenti normativi e regolamentari di maggiore rilevanza per il sistema bancario, che ricomprendono una specifica attenzione in tema di rischi, sostenibilità e fattori ESG e su cui il CCR deve indirizzare la propria attività, sono da ricomprendere gli "Orientamenti in materia di concessione e monitoraggio dei prestiti" pubblicati dall'European Banking Autority (EBA) il 29 maggio 2020 (gli "Orientamenti EBA")[34] e la "Guida sui rischi climatici e ambientali" per le banche pubblicata dalla Banca Centrale Europea (BCE)[35], nella quale, al par. 5.2 ("Propensione al rischio") si legge testualmente: «*Gli enti dovrebbero disporre di un quadro di riferimento per la determinazione della propensione al rischio (risk appetite framework, RAF), sottoposto a regolare riesame, che tenga conto di tutti i rischi rilevanti a cui sono esposti in un'ottica prospettica, in linea con l'orizzonte di pianificazione strategica. L'integrazione dei rischi climatici e ambientali nel RAF accresce la resilienza degli enti in relazione ad essi e migliora la loro capacità di gestirli, ad esempio attraverso la definizione di massimali di credito per settori e aree geografiche altamente esposti*».

La Banca d'Italia, in linea con tale iniziativa della BCE, ha elaborato nel 2022 un insieme di aspettative di vigilanza sull'integrazione dei rischi climatici e ambientali nelle strategie aziendali, nei sistemi di governo, controllo e gestione dei rischi e nella informativa al mercato degli intermediari vigilati[36]. A tal riguardo, la Banca d'Italia si attende che l'Organo di amministrazione assicuri che "*la funzione di Risk Management incorpori i fattori climatici e ambientali nella valutazione dell'esposizione ai vari rischi e nel loro monitoraggio, elaborando report esaustivi sul tipo e sul livello di materialità dei rischi climatici e ambientali a cui sono esposti l'intermediario e i portafogli, individuali e collettivi, che questo eventualmente gestisce per conto di terzi*".

Infatti, la funzione di Risk Management è responsabile della corretta attuazione del processo di gestione dei rischi, volto a identificare, misurare, prevenire e attenuare tutti i rischi assunti o assumibili dall'intermediario. In tale ambito, anche se i rischi climatici e ambientali hanno natura ben definita, la loro materializzazione determina impatti sui rischi prudenziali tradizionali (in particolare, credito, mercato, operativo e di liquidità). La gestione dei rischi climatici implica alcuni elementi di complessità, derivanti, da un lato, da un elevato grado di incertezza sull'entità degli effetti dei cambiamenti climatici – in dipendenza delle politiche, delle possibili azioni di adattamento e dei possibili canali di trasmissione – e, dall'altro lato, dalla necessità di adottare orizzonti temporali di valutazione più lunghi. La Banca d'Italia

---

[34] Gli "Orientamenti EBA" pubblicati dall'*European Banking Autority* (EBA) il 29 maggio 2020, emanati in applicazione dell'articolo 16 del Regolamento (UE) n. 1093/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010 che ha istituito l'EBA, devono essere applicati a partire dal 30 giugno 2021.

[35] Banca Centrale Europea (BCE), *Guida sui rischi climatici e ambientali. Aspettative di vigilanza in materia di gestione dei rischi e informativa,* pubblicata il 27 novembre 2020.

[36] Banca d'Italia "Aspettative di vigilanza sui rischi climatici e ambientali" dell'8 aprile 2022.

si aspetta, quindi, che gli intermediari effettuino una mappatura degli eventi che potrebbero manifestarsi per effetto dei rischi climatici e ambientali (fisici e di transizione) e integrino, di conseguenza, il sistema di gestione dei rischi, identificando i rischi che ne risulterebbero potenzialmente influenzati e le relative implicazioni di natura prudenziale.

Si ricorda che nel decreto Ministero dell'Economia e delle Finanze n. 169, del 23 novembre 2020[37] la funzione di controllo dei rischi è ricompresa tra le «principali funzioni aziendali» e sono individuati specifici criteri di competenza per gli amministratori circa la gestione dei rischi (individuazione, valutazione, monitoraggio, controllo e mitigazione delle principali tipologie di rischio di una banca, incluse le responsabilità dell'esponente in tali processi).

Inoltre, l'Autorità Bancaria Europea ha avviato una consultazione pubblica[38] sulle sue recenti direttive per la gestione dei rischi legati all'ambiente, alla società e alla governance, evidenziando l'importanza per le banche di valutare tali rischi nell'ambito dei loro processi decisionali. Con le nuove linee guida, l'EBA definisce più precisamente i requisiti, in vigore entro la metà del 2025, che le banche devono soddisfare per identificare, misurare, gestire e monitorare i rischi ESG. Questo, naturalmente, al fine di garantire la sicurezza e la stabilità delle istituzioni nel breve, medio e lungo termine in conformità con la Capital Requirement Directive (CRD6).

Il Settore Assicurativo

Con riferimento al settore assicurativo, si prevedono disposizioni similari nell'attuazione dell'art. 29-bis del Codice delle Assicurazioni Private che indica che l'Organo di amministrazione ha la responsabilità ultima dell'osservanza delle norme applicabili. In particolare, in attuazione di tale previsione della Direttiva comunitaria Solvency 2 (2009/138/UE), l'articolo 6 del Regolamento IVASS n. 38, prevede che per l'espletamento dei compiti relativi al sistema di controllo interno e gestione dei rischi, l'Organo amministrativo costituisca, ove appropriato in relazione alla natura, portata e complessità dell'attività dell'impresa e dei rischi inerenti, un Comitato per il controllo interno e i rischi (CCR).

Tale Comitato è composto da amministratori non esecutivi, in maggioranza indipendenti. L' Organo di amministrazione definisce la composizione, i compiti e le modalità di funzionamento del CCR (inclusi i flussi informativi tra i comitati endo-consiliari, tra questi e l'Organo amministrativo e con le funzioni fondamentali). Annualmente, viene effettuata una auto-valutazione sulla dimensione, sulla composizione e sull'efficace funzionamento dell'Organo di amministrazione nel suo complesso, nonché dei suoi comitati, esprimendo orientamenti sulle figure professionali la cui presenza sia ritenuta opportuna e proponendo eventuali azioni correttive.

La normativa indica che al CCR sono affidate funzioni consultive e propositive ed il compito di svolgere indagini conoscitive. In particolare, il CCR assiste l'Organo di amministrazione nella determinazione delle linee di indirizzo del sistema di controllo interno e gestione dei rischi, nella verifica periodica della sua adeguatezza e del suo effettivo funzionamento, e nell'identificazione e gestione dei principali rischi aziendali. Per poter assolvere ai propri compiti il CCR deve garantire adeguati scambi informativi con le funzioni fondamentali (funzione risk management, funzione di conformità, funzione attuariale, funzione internal audit).

Si evidenzia che l'istituzione del CCR non solleva l'Organo di amministrazione dalle proprie responsabilità. Infatti, come richiamato dagli "Orientamenti sul sistema di governance"[39] di EIOPA (Autorità europea per la vigilanza del settore), l'Organo di amministrazione dovrebbe avere un'idonea interazione con tutti i comitati che istituisce, chiedendo informazioni in maniera proattiva e, se del caso, mettendo in discussione le informazioni ricevute.

La normativa nazionale (cfr. Lettera al mercato IVASS del 5 Luglio 2018), prevede indicazioni di proporzionalità nel disegno della governance aziendale. In particolare, sulla base di criteri dimensionali e di complessità delle imprese, si prevedono tre regimi differenziati rispetto alla costituzione del CCR:

- regime rafforzato e regime ordinario: costituzione obbligatoria del CCR, in quanto presidio indispensabile per una efficace comprensione e monitoraggio dei rischi, cui è o potrebbe essere esposta l'impresa, da parte dell'Organo di amministrazione che detiene la responsabilità ultima del sistema di gestione dei rischi. L'impresa di cui all'articolo 210-ter, comma 2, del Codice delle Assicurazioni Private è esonerata dalla costituzione del CCR se tale funzione è svolta dal CCR di gruppo costituito presso l'ultima società controllante italiana, qualora lo stesso sia idoneo a presidiare adeguatamente il profilo di rischio specifico della controllata. In questo caso l'impresa controllata potrà avvalersi della facoltà di cui all'articolo 17, comma 3, del Regolamento IVASS n. 38;
- regime semplificato: possibilità di non costituire il CCR e incaricare, ai sensi dell'articolo 17, comma 3, del Regolamento, almeno un membro dell'Organo amministrativo, adeguatamente competente in materia e privo di

[37] Decreto MEF 169/2020 «Regolamento in materia di requisiti e criteri di idoneità allo svolgimento dell'incarico degli esponenti aziendali delle banche, degli intermediari finanziari, dei confidi, degli istituti di moneta elettronica, degli istituti di pagamento e dei sistemi di garanzia dei depositanti».

[38] European Bank Authority (EBA) *Draft Guidelines on the management of ESG risks – Consultation Paper* del 18 gennaio 2024.

[39] EIOPA-BoS-14/253 IT.

deleghe, di monitorare l'adeguatezza e il corretto funzionamento del sistema di gestione dei rischi e di riferire all'Organo amministrativo le relative risultanze.

In ogni caso l'Ultima Società Controllante Italiana è tenuta alla costituzione dei comitati endo-consiliari (tra cui il Comitato Controllo Interno e Rischi) necessari per l'espletamento delle funzioni ad essa assegnate, anche in ragione della responsabilità ultima in materia di governance di gruppo in capo all'Organo amministrativo della stessa.

Le scelte effettuate dalle imprese assicurative devono essere motivate, formalizzate e comunicate ad IVASS e sono oggetto di confronto nell'ambito ordinaria attività di interlocuzione che viene svolta durante processo di controllo prudenziale.

3 Le funzioni del Comitato Controllo e Rischi

Le sezioni riportate nel seguito ripercorrono i seguenti principali argomenti, evidenziando anche le aree di necessario coordinamento e collegamento del CCR con gli altri comitati endoconsiliari (es. Comitato Nomine, Comitato Remunerazioni, Comitato Sostenibilità o altro):

a. **Il ruolo del CCR nell'ambito delle Linee di indirizzo SCIGR:** Il ruolo di supporto all'Organo di amministrazione nelle valutazioni e decisioni in merito al SCIGR.

b. **Il Modello di Risk Management:** Le attività di definizione del modello di Risk Management e del Risk Appetite Framework.

c. **Il supporto nel processo di pianificazione strategica:** Le attività di misurazione e valutazione dei rischi sottostanti la proposta di piano strategico, compresa la relativa politica di remunerazione.

d. **Il processo di gestione dei rischi:** Le attività di monitoraggio del profilo di rischio societario rispetto alla propensione al rischio definita.

e. **I rapporti con l'Internal Audit e le altre funzioni di controllo:** I rapporti con la funzione Internal Audit, in qualità di *assurance provider* indipendente, e con le altre funzioni di controllo di secondo livello (funzioni di Compliance, Risk Management, DPO, CIO, ecc.) nonché le modalità di coordinamento e i relativi flussi informativi tra le stesse e verso l'Organo di amministrazione.

f. **La valutazione di adeguatezza del SCIGR:** I vari aspetti, informazioni e attività che contribuiscono alla valutazione annuale complessiva del sistema.

g. **L'Informativa societaria:** Le attività di valutazione del processo di formazione dell'informativa societaria affinché sia funzionale a rappresentare correttamente il modello di business, le strategie, l'impatto delle sue attività e le performance conseguite.

Le diverse sezioni, oltre a riportare in **grassetto** una breve descrizione di quanto previsto dal Codice di Corporate Governance, evidenziano anche aspetti interpretativi forniti nella più diffusa leading practice internazionale o da normative di riferimento quali la CSRD[40].

Per ogni ambito trattato, sono altresì riportate, laddove esistenti, alcune tra le principali responsabilità aggiuntive previste dalla normativa di settore in capo al **CCR nelle aziende del settore finanziario**.

All'interno di ogni sezione sono approfonditi alcuni elementi al fine di chiarire alcuni aspetti chiave citati.

Si precisa che il presente documento non ha carattere di esaustività, dovendo lo stesso essere integrato o modificato sulla base delle eventuali ulteriori o diverse responsabilità che lo statuto o i regolamenti interni della società potrebbero aver attribuito al CCR. La declinazione dello strumento proposto dovrà essere valutata da ciascuna realtà aziendale e adattata alle caratteristiche dei modelli di business e delle dimensioni che la contraddistinguono. L'eterogeneità e la diversa complessità delle soluzioni impongono dunque di fare ricorso al principio di **proporzionalità** e a quello della **materialità.**

3.a) Il ruolo del CCR nell'ambito delle Linee di indirizzo SCIGR

Il CCR supporta l'Organo di amministrazione nei seguenti ambiti:

- **La definizione delle linee di indirizzo SCIGR e valutazione della sua adeguatezza ed efficacia.**
- **La nomina e revoca il responsabile della funzione di internal audit e approvazione del piano di audit,** assicurando altresì il rispetto delle "condizioni essenziali" di cui ai Global Internal Audit Standard[41] e favorendo le periodiche verifiche esterne di quality assurance sull'Internal Audit.
- **L'adozione di misure per garantire l'efficacia e l'imparzialità di giudizio delle altre funzioni di controllo.**
- **L'attribuzione, all'Organo di controllo o ad un organismo appositamente costituito, delle funzioni di vigilanza ex D.Lgs. 231/01, compresa una argomentazione delle scelte effettuate sulla composizione**

[40] A titolo esemplificativo e non esaustivo, il COSO "Internal Control", il COSO "Enterprise Risk Management", G20/OECD Principles of Corporate Governance, Codici di Corporate Governance Internazionali.
[41] Global Internal Audit Standards (2024).

dell'OdV.

- **La valutazione dei risultati esposti dalla società di revisione nella eventuale lettera di suggerimenti e nella relazione aggiuntiva** (cfr. par. 3.g: L'informativa societaria).
- **L'esame e contributo alla stesura della descrizione del SCIGR nella Relazione sul Governo Societario, che deve comprendere:**
  - **le modalità di coordinamento tra i soggetti coinvolti nel SCIGR;**
  - **l'indicazione dei modelli e le leading practice nazionali e internazionali di riferimento.**
- **Il coordinamento e sinergie con**
  - **l'Organo di controllo[42] (si veda par. "2.d Confronto tra CCR e Organo di controllo");**
  - **eventuale Comitato predisposto per "l'analisi dei temi rilevanti per la generazione di valore nel lungo termine";**
  - il Comitato Remunerazione per la verifica che il sistema di incentivi non stimoli un'eccessiva presa di rischio (fuori dal risk appetite).

Tali compiti sono ulteriormente declinati nei paragrafi che seguono.

PRINCIPALI DISPOSIZIONI PER IL SETTORE FINANZIARIO

- Supporta l'Organo di amministrazione nella definizione e approvazione degli indirizzi strategici e delle politiche di governo dei rischi, curandone l'adeguamento alla evoluzione dell'operatività aziendale e delle condizioni esterne. Nell'ambito di tali indirizzi approva le politiche di gruppo relative al sistema di controllo interno, al sistema di gestione dei rischi e alla revisione interna.
- Esprime valutazioni e pareri all'Organo di amministrazione sul rispetto dei principi cui devono essere uniformati il sistema dei controlli interni e l'organizzazione aziendale.
- Con particolare riguardo alla politica di revisione interna supporta l'Organo di amministrazione nell'assicurare che essa contenga la descrizione delle modalità con cui la funzione coordina le attività di revisione interna nel gruppo e garantisce l'osservanza dei requisiti di revisione interna a livello di gruppo.
- Porta all'attenzione dell'Organo di amministrazione gli eventuali punti di debolezza e le conseguenti azioni correttive da promuovere valutando a tal fine le proposte dell'organo con funzione di gestione.

3.b) Il Modello di Risk Management

Il CCR supporta l'Organo di amministrazione nella:

- **definizione della natura e del livello di rischio compatibile con gli obiettivi strategici;**
- **indicazione nella Relazione sul Governo Societario del modello SCIGR o framework utilizzato, in relazione a leading practice nazionali o internazionali;**
- **efficace progettazione e disegno del SCIGR in conformità con il modello indicato.**

A tal fine il CCR, nel coadiuvare l'Organo di amministrazione:

Risk Framework

- Promuove lo sviluppo di un **risk framework** adeguato al fine di supportare l'Organo di amministrazione nella definizione del profilo di rischio compatibile con la strategia e nella validazione almeno annuale dei rischi significativi in relazione all'approvazione del piano industriale. Nello spirito del Codice, l'analisi deve avere aspetti di trasversalità, sostenibilità e orizzonte temporale di lungo termine. La Società deve quindi predisporre un modello di gestione del rischio o risk framework per cogliere in modo adeguato i diversi aspetti di

[42] Il Codice promuove tale sinergia con il seguente indirizzo: "L'Organo di controllo e il Comitato Controllo e Rischi si scambiano tempestivamente le informazioni rilevanti per l'espletamento dei rispettivi compiti. Il presidente dell'Organo di controllo, o altro componente da lui designato, partecipano ai lavori del comitato controllo e rischi", sempre avendo ben presente che l'Organo di controllo è deputato a controllare anche l'attività del CCR, e non viceversa.

rischio, facendo riferimento alle leading practice nazionali o internazionali (cfr. par. 1.a) I Framework internazionali di riferimento). Tale framework dovrebbe essere applicato ex ante (in quanto le imprese dovrebbero promuovere la loro resilienza in caso di crisi) ed ex post (in quanto le imprese dovrebbero essere in grado di istituire processi di gestione delle crisi all'insorgenza di un evento negativo improvviso)[43]. Il risk framework deve inoltre tenere conto delle caratteristiche del settore e dell'azienda, considerare la prospettiva degli stakeholder più rilevanti, promuovere un approccio di portafoglio, individuando i rischi più significativi/prioritari in funzione del perseguimento di obiettivi strategici e del successo sostenibile. Può ad esempio basarsi su: aspetti ricompresi nell'Agenda dell'Organo di amministrazione e sui flussi informativi all'Organo di amministrazione; informazioni sui rischi operativi raccolte dai dirigenti responsabili delle funzioni aziendali coinvolte o dalle funzioni di controllo di secondo livello; operazioni societarie avvenute o in corso; eventi imprevisti; su analisi dell'Internal Audit**.** Il risk framework è sempre più frequentemente sviluppato e gestito anche nelle società non finanziarie da una funzione dedicata (definita "risk management" o "Enterprise Risk Management"). Nelle Società in cui è presente la funzione di risk management, il CCR incontra, di norma, trimestralmente tale funzione, discute l'analisi svolta, valuta l'adeguatezza del modello e la capacità di risposta ai rischi (si veda anche par. 4: L'agenda del CCR).

Soglie di rischio

- Può svolgere un'attività valutativa e propositiva necessaria affinché l'Organo di amministrazione, possa definire e approvare il Risk appetite e la soglia di tolleranza ("Risk tolerance") attraverso lo sviluppo di un *Risk Appetite Framework* (RAF) per la definizione da parte dell'Organo di amministrazione del livello di rischio massimo coerente con gli obiettivi strategici entro il quale il management deve operare, validando la scelta della metodologia per l'identificazione di *Key Performance Indicators* (KPI) e *Key Risk Indicators* (KRI). Il RAF è una metodologia di gestione del rischio particolarmente sviluppata nell'ambito del sistema finanziario nel quale è imposta dalla normativa di riferimento. Si sta gradualmente diffondendo anche nelle aziende non finanziarie e costituisce uno strumento estremamente utile per l'Organo di amministrazione per definire il profilo di rischio entro cui il management opera in autonomia. Il *risk appetite framework* è approvato dall'Organo di amministrazione, ed è il quadro di riferimento che definisce – in coerenza con il massimo rischio assumibile, il business model e il piano strategico – la propensione al rischio, le soglie di tolleranza, i limiti di rischio, le politiche di governo dei rischi, i processi di riferimento necessari per definirli e attuarli. Il *risk appetite* è declinato nei KPI/KRI riconducibili ai vari livelli dell'organizzazione e ai diversi stakeholder dell'azienda, e costituisce un riferimento nella selezione delle strategie, nelle decisioni di investimento e nelle operazioni di finanza straordinaria (acquisizioni, rifinanziamenti, ristrutturazioni finanziarie, …)[44].

Matrice di Valutazione Rischi

- Esamina le analisi effettuate in merito all'individuazione, valutazione e gestione dei rischi illustrati, in ottica integrata, all'interno della matrice dei rischi. La matrice dei rischi può essere costruita articolando in vario modo le varie tipologie di rischi e sulla base di diversi possibili criteri[45]. Con riguardo ai criteri utilizzati per costruire la matrice, le leading practice propongono solitamente una mappatura dei rischi che: a) consenta di distinguere i rischi anche in relazione alla loro attitudine a influire sul risk appetite e quindi sulla realizzabilità del business plan e degli obiettivi strategici; b) preveda una scala di priorità dei rischi costruita ad esempio sulla base del prodotto tra probabilità e impatto, dove l'impatto può essere di tipo economico-finanziario, reputazionale o operativo ed incidere o meno sulla sostenibilità dell'azienda; c) preveda la possibilità di intervenire sui rischi (attraverso la loro accettazione, riduzione, trasferimento, rimozione, …) e/o sulla attitudine del contesto aziendale a sopportarli (attraverso la dotazione di liquidità, interventi sul rapporto di indebitamento, la ristrutturazione degli attivi, ecc.); d) sia sistematicamente aggiornata per recepire l'impatto via via esercitato dai rischi emergenti e/o dalle decisioni aziendali non ricorrenti (acquisizioni, ristrutturazioni di attivi e passivi, nuovi investimenti rilevanti, ecc).

Mappatura Rischi

- Al fine di massimizzare l'efficienza del sistema di controllo interno e gestione dei rischi e ridurre le duplicazioni di attività o mitigare il rischio di omissioni, coerentemente con quanto indicato nel Codice di Corporate Governance[46], promuove il coordinamento e l'integrazione dei modelli di controllo con riferimento, da un lato, al disegno, supportando l'allineamento della mappatura dei rischi attraverso un quadro unificato, che collega rischi operativi, strategici, di compliance e ESG a una tassonomia di rischi condivisa, nonché

43 Secondo quanto indicato nei principi di Corporate Governance dell'OECD aggiornati, da ultimo, nel 2023.

44 Oltre alle leading practice, si rinvia al paper AIFIRM (2020) *Governance e strategia per gestione dei rischi nelle imprese non finanziarie*, da pagina 33 a pagina 40.

45 Per un esempio delle possibili tipologie di rischi si rinvia alla tassonomia riportata nel position paper AIFIRM (2020), *Governance e strategia per gestione dei rischi nelle imprese non finanziarie,* da pagina 52 in poi.

46 Codice Corporate Governance principio XX.

delle metodologie di identificazione, valutazione e trattamento dei rischi omogenee assicurando che tutti gli attori siano allineati; e dall'altro, con riferimento all'operatività, tramite il coordinamento delle attività di risk assessment e monitoraggio, favorendo l'integrazione dei processi di controllo a vari livelli aziendali ed evitando ridondanze o mitigando omissioni non giustificate. Questo approccio, grazie al dialogo e alla collaborazione fra le diverse funzioni coinvolte, garantisce che la gestione del rischio e dei controlli sia trasversale a tutta l'organizzazione, garantendo una vista unificata e coerente con riferimento alle varie aree di rischio.

Risk Framework integrato con ESG

- Può promuovere attività di integrazione tra ESG e ERM modificando l'approccio al risk management al fine di introdurre, nell'ambito del SCIGR, anche la valutazione dei fattori ESG e contribuire al successo sostenibile della Società. Dunque, non basta più considerare i fattori ESG come causa di possibili rischi reputazionali. Accanto agli strumenti di identificazione e misurazione del rischio si assiste all'adozione, sempre più diffusa, del processo di analisi di materialità e della mappatura dei rischi ESG e a una loro integrazione nelle politiche di gestione dei rischi. Il valore dell'impresa nel lungo termine sarà, in maniera crescente, direttamente correlato all'integrazione, nel piano industriale dell'impresa, dei fattori ESG. In generale, l'allineamento delle aziende all'obiettivo del successo sostenibile (di cui al primo principio del codice) e l'attenzione ai fattori ESG costituiscono importanti presupposti alla diffusione e alla implementazione di una cultura evoluta dell'ERM. Invertendo il ragionamento, si potrebbe anche dire che la presenza di un modello evoluto di ERM è la cartina di tornasole di una governance aziendale attenta al rispetto dei fattori ESG. Il Comitato promuove l'inclusione dei fattori ESG nella mappa dei rischi, attraverso la rivisitazione dei rischi del business in ottica ESG e l'identificazione di nuovi rischi emergenti[47]. Inoltre, anche le recenti evoluzioni normative in ambito di disclosure di sostenibilità quali la CSRD, prevedono, nell'ambito del processo di doppia rilevanza, attività che richiedono una revisione dei processi di risk management al fine di tener conto delle tematiche di sostenibilità. In particolare, la CSRD richiede l'individuazione e la disclosure di quei temi di sostenibilità che generano rischi od opportunità che incidono, o di cui si può ragionevolmente prevedere che incidano, sullo sviluppo dell'impresa, sulla sua situazione patrimoniale-finanziaria, sul risultato economico e sui flussi finanziari, sull'accesso ai finanziamenti o sul costo del capitale nel breve, medio o lungo periodo (financial materiality in ottica outside-in). Tale attività affianca l'impact materiality per la quale si individuano i temi di sostenibilità connessi ad impatti rilevanti dell'impresa, negativi o positivi, effettivi o potenziali, sulle persone o sull'ambiente nel breve, medio o lungo periodo (ottica inside-out). Diventa, pertanto, sempre più fondamentale integrare nei propri processi di risk management le questioni di sostenibilità, rivedendo processi, metodologie, metriche, tool e modalità di coordinamento con gli altri attori coinvolti.

Evoluzione dei Rischi

- Riserva particolare attenzione ai rischi trasversali - pro tempore - emergenti, quali attualmente il cyber risk[48], i rischi reputazionali, i rischi geopolitici e alla digital transformation inclusiva dell'eventuale utilizzo di artificial intelligence.
- Esamina le principali politiche aziendali da sottoporre all'approvazione dell'Organo di amministrazione.

47 Per la metodologia, si veda ad esempio il paper COSO (2018) "*Applying ERM to ESG-related risks*".

48 Il cyber risk, e più in generale il rischio informatico o rischio ICT, è solitamente generato da eventi non pianificati che esercitano un impatto negativo sulle risorse informatiche in termini di integrità, disponibilità, autenticità e riservatezza delle informazioni. Tale impatto può seriamente minare la continuità dei servizi o dei processi aziendali così come può portare alla violazione di norme/prassi in tema di sicurezza delle informazioni o, infine, può compromettere il posizionamento competitivo dell'azienda. I rischi connessi alla digital transformation sono in qualche modo legati ai rischi cyber e ICT. Essi derivano dalla evoluzione digitale del business e del contesto competitivo che l'azienda deve cercare di anticipare per garantire adeguati presidi. Il rischio reputazionale consiste nella possibilità che venga a deteriorarsi la percezione dell'immagine della società da parte dei vari stakeholders aziendali (clienti, fornitori, investitori, autorità di vigilanza, ecc.), sino a incidere sul posizionamento competitivo e sulla performance dell'azienda. Il rischio reputazionale può essere alimentato da eventi interni o esterni all'azienda (ad esempio originati sui social network) riconducibili ad altri rischi aziendali e, a sua volta, può generare un percorso vizioso che impatta in modo trasversale su tutti gli altri rischi aziendali, generando un effetto a catena. Per una visione d'insieme sul ruolo dell'Organo di amministrazione, si rinvia al paper EcoDa (2020*), Cyber Risk Oversight – Key principles and practical guidance for Corporate Boards in Europe*. Per approfondimenti sul contesto regolatorio, si rinvia alla Direttiva europea sulle misure per un livello comune elevato di cibersicurezza in tutta l'Unione (direttiva NIS2) del 2022, recepita in Italia con il D.Lgs. 138/2024, e al Regolamento Europeo del 2022 sul Digital Operational Resilience Act (DORA).

PRINCIPALI DISPOSIZIONI PER IL SETTORE FINANZIARIO

- Supporta l'Organo di amministrazione nella definizione del sistema degli obiettivi di rischio, definendo, sulla base delle valutazioni rilevanti, la propensione al rischio dell'impresa in coerenza con il fabbisogno di solvibilità globale della stessa, individuando le tipologie di rischio che ritiene di assumere e fissando in modo coerente i relativi limiti di tolleranza al rischio. Effettua le sue pre-valutazioni sulla base delle risultanze presentate dalla funzione di risk management in relazione alle analisi effettuate ricorrendo all'utilizzo di specifici stress test calibrati sul profilo di rischio della società o ad altre eventuali analisi quantitative. I rischi sono considerati negli orizzonti di breve, medio e lungo termine, e sono valutati potenziali eventi o future modifiche nelle condizioni economiche che possono avere un impatto sfavorevole sulla complessiva situazione finanziaria e sul patrimonio.
- Il Comitato pre-valuta in via continuativa le informazioni sui rischi (ivi inclusi quelli relativi ai fattori di sostenibilità), interni ed esterni, attuali e prospettici, a cui è esposta la società e che possono interessare tutti i processi operativi e le aree funzionali. Il Comitato supporta l'Organo di amministrazione nell'assicurare che la procedura di censimento dei rischi e i relativi risultati sono adeguatamente documentati. A tal fine, il Comitato si relaziona regolarmente con le funzioni fondamentali con cui sono istituiti regolari scambi informativi (es. analisi dei piani annuali, risultati delle attività di controllo, ecc.).
- Con riferimento al processo di valutazione interna del rischio e della solvibilità (i.e. ICAAP/ILAAP per il settore bancario o ORSA per il settore assicurativo), supporta l'Organo di amministrazione nel definire ed approvare le linee generali del processo, ne assicura la coerenza con il RAF e l'adeguamento tempestivo in relazione a modifiche significative delle linee strategiche, dell'assetto organizzativo, del contesto operativo di riferimento; promuove il pieno utilizzo delle risultanze di tale processo a fini strategici e nelle decisioni d'impresa.
- Il Comitato valuta le politiche di rischio prima dell'approvazione da parte dell'Organo amministrativo e monitora periodicamente la loro attuazione (mediante le informative delle funzioni fondamentali).

3.c) Il supporto nel processo di pianificazione strategica

L'Organo di amministrazione, con il supporto del CCR, definisce le linee di indirizzo[49] del sistema di controllo interno e di gestione dei rischi in coerenza con le strategie della società.

Il CCR ha il compito di valutare l'adeguatezza e l'efficacia del SCIGR in funzione della capacità di identificare i rischi del piano strategico ed incorporarli nella pianificazione. Questo ha una **duplice valenza**: il processo di elaborazione del piano strategico deve essere adeguato e il contenuto della strategia deve incorporare i rischi principali in ottica di successo sostenibile. A tal fine il CCR può:

- Promuovere la valutazione del processo di pianificazione strategica nella prospettiva del SCIGR prevedendo:
  - un'adeguata rilevazione e misurazione dei rischi aziendali nel periodo di pianificazione strategica (di mercato, regolatori, esogeni);
  - l'identificazione di misure per gestire i rischi.
- Formulare un parere sulla proposta del Piano Strategico oggetto di approvazione da parte dell'Organo di amministrazione, nella prospettiva del SCIGR ai fini del successo sostenibile, analizzando:
  - la coerenza tra obiettivi strategici, rischi aziendali e sostenibilità a lungo termine dell'azienda (inclusa la coerenza con i valori aziendali[50]);
  - l'identificazione di opportunità conseguenti a cambiamenti di scenario o rischi emergenti.

[49] Nell'ambito delle linee di indirizzo del SCIGR definite dall'Organo di amministrazione sono introdotti di norma i principi generali (es. definizioni, articolazioni, obiettivi del SCIGR, etc.), i ruoli, responsabilità e modalità di coordinamento tra i soggetti coinvolti nel SCIGR (es. Organo di amministrazione, CCR, Collegio Sindacale, funzione Internal Audit, funzioni di controllo di II livello, etc.) e le modalità di attuazione del SCIGR ivi inclusa l'articolazione dei flussi informativi e di coordinamento tra i diversi attori coinvolti nel SCIGR.

[50] Peter Drucker, "Culture eats strategy for breakfast" e COSO ERM.

- Verificare l'integrazione tra pianificazione strategica, tematiche ESG e processo di ERM, inclusi:
  - impatto dei cambiamenti climatici e azioni da intraprendere;
  - evoluzione della governance aziendale per far fronte al cambiamento strategico.

Il processo

In particolare, per la valutazione del processo di pianificazione strategica nella prospettiva del SCIGR, il CCR valuta se il processo di pianificazione strategica, ivi incluso il relativo processo di definizione delle politiche di remunerazione, è adeguatamente supportato da un idoneo processo di analisi dei rischi[51], svolto in modo integrato considerando tra l'altro gli elementi di supporto: tassonomia dei rischi; mappatura dei rischi; modalità quantitative/qualitative di misurazione dei rischi e metodi di correlazione.

Incontri con il Risk Manager

Il CCR incontra le funzioni di risk management in preparazione dell'approvazione del piano strategico per discutere quali rischi siano presenti nel piano, come siano stati misurati e quali azioni siano previste. La maggiore difficoltà di previsione, l'allungamento dell'orizzonte temporale di riferimento e una più veloce propagazione dei rischi nel sistema hanno portato al crescente utilizzo e sviluppo di metodologie di analisi più sofisticate, quali *scenario planning*, *what if analysis, dynamic risk assessment*, scenari con metodo Montecarlo[52]. Infine, il CCR valuta i ruoli ed i sistemi di accountability o di deleghe al fine di determinare le modalità per assicurare la corretta esecuzione degli obiettivi strategici prefissati[53].

Le politiche aziendali

Anche nell'analisi delle politiche di remunerazione, il CCR verifica, in coordinamento con il Comitato Remunerazione, che all'interno delle stesse non siano stati definiti incentivi che pregiudichino il successo a lungo termine dell'azienda. In particolare, il CCR verifica che le politiche di remunerazione siano coerenti con i profili di rischio e con gli obiettivi strategici della società e non incentivino comportamenti che potrebbero esporre l'azienda a rischi operativi o reputazionali fuori dal risk appetite framework (RAF).

Un Piano integrato ESG

Inoltre, per la verifica della integrazione tra pianificazione strategica, tematiche ESG e processo di ERM con particolare riferimento all'impatto dei cambiamenti climatici, il CCR dovrà tenere in considerazione le diverse linee guida che sono state sviluppate su questo argomento, a partire dal World Economic Forum che ha sviluppato 8 principi[54]. Questo perché il cambiamento climatico è un fattore non solo di impatto ambientale ma detiene specifiche implicazioni finanziarie e può richiedere una modifica del posizionamento strategico anche a breve termine. Si ricorda inoltre, coerentemente con le *policy* definite a livello di Unione Europea con il *Green Deal* e il Next Generation EU, che le imprese e gli enti finanziari hanno un ruolo determinante da svolgere nella transizione verso un'economia a basse emissioni di carbonio e resiliente ai cambiamenti climatici. In quest'ottica, rischi e impatti di natura ambientale, sociale e finanziaria, connessi all'intera catena del valore, sono stati identificati anche negli "Orientamenti della Commissione europea sulla comunicazione di informazioni di sostenibilità: Integrazione concernente la comunicazione di informazioni relative al clima" (gli "Orientamenti")[55]. Anche lo European Confederation of Institute of Internal Auditors (ECIIA) ha pubblicato linee guida in tema di cambiamento climatico[56]. Infine, i nuovi European Sustainability Reporting Standard (ESRS) emanati ai fini della rendicontazione dell'informativa di sostenibilità ai sensi della CSRD, richiedono la rendicontazione da parte delle aziende del proprio piano di transizione per la mitigazione dei cambiamenti climatici. Informazioni utili relative alla valutazione dei rischi climatici e la costruzione del Transition Plan sono riportate nel working paper di Nedcommunity[57].

---

51 Come evidenziato nel paper Nedcommunity (2013), *Come valutare la governance in tema di rischi e controlli*.

52 Esempi di utilizzo di nuove tecniche sono descritti nel paper Nedcommunity (2020), *L'evoluzione della risk governance in chiave strategica* e nel paper AIFIRM (2020) *Governance e strategia per gestione dei rischi nelle imprese non finanziarie*, da pagina 49 a pagina 51.

53 Poiché il livello di integrazione del sistema di gestione dei rischi nel processo di pianificazione strategica dell'impresa è in continua evoluzione, il paper Nedcommunity (2013) "*Come valutare la governance in tema di rischi e controlli*" fornisce anche delle indicazioni per il Comitato su come valutare la scala di maturità dell'azienda del proprio sistema di risk management in ambito della definizione del piano strategico.

54 *WEF: How to Set Up Effective Climate Governance on Corporate Boards.* Si rimanda al sito di Chapter Zero – *the Nedcommunity climate change directors forum.*

55 Cfr.: «Orientamenti sulla comunicazione di informazioni di carattere non finanziario: Integrazione concernente la comunicazione di informazioni relative al clima» della Commissione europea (2019/C 209/01), pubblicati sulla GUCE il 20 giugno 2019 e gli Orientamenti, redatti a norma dell'articolo 2 della direttiva 2014/95/UE del Parlamento europeo e del Consiglio, costituiscono un documento integrativo degli orientamenti sulla comunicazione di informazioni di carattere non finanziario adottati dalla Commissione nel 2017 (C/2017/4234 final).

56 *Practical Guidance on climate change and environmental sustainability: How to tackle associated risks and harness opportunities? (ECIIA, 2020).*

57 Cfr. Working Paper (2024) "*Politiche di remunerazione ed engagement di executives e dipendenti a sostegno della transizione climatica*".

3.d) Il processo di gestione dei rischi

Il CCR:

- **supporta l'Organo di amministrazione nelle valutazioni relative alla gestione dei rischi derivanti da fatti pregiudizievoli[58];**
- **esprime pareri su specifici aspetti inerenti all'identificazione dei rischi;**
- **valuta l'effettiva implementazione del risk framework;**
- **valuta l'adeguatezza dell'assetto organizzativo, amministrativo e contabile della società e delle controllate aventi rilevanza strategica, con particolare riferimento al SCIGR e alle tre linee di controllo[59].**

L'analisi del modello di governance complessivo da parte del CCR si può basare sul modello delle leading practice di riferimento[60] adottato dalla Società; sul Modello Organizzativo D.Lgs. 231/01; sulle politiche di governance, di controllo e di risk management eventualmente adottate; sulle disposizioni organizzative inerenti le deleghe di potere e sui meccanismi di segregazione delle funzioni decisionali; sull'ultima relazione approvata sul governo societario e sugli assetti proprietari; sugli eventuali aggiornamenti sugli orientamenti in merito[61], sulle valutazioni dell'efficacia delle funzioni fondamentali di controllo (e/o fornitori di assurance).

Inoltre, il CCR svolge:

Rischi ben identificati

- La valutazione del periodico aggiornamento della matrice dei rischi, della loro evoluzione e dell'impatto sul business.
- La promozione di un periodico brainstorming sui rischi inusuali o sconosciuti o emergenti, inclusa la reportistica rispetto agli esiti di "war room exercise" da parte del Senior Management.

La mitigazione dei rischi (SCIGR)

- La valutazione dei piani di mitigazione per la gestione dei rischi e il controllo del livello di accettabilità dei rischi.

Risk tolerance

- La verifica che siano definiti i limiti di rischio accettabili e che questi limiti siano utilizzati nei processi aziendali rilevanti. Valutazione sull'utilizzo del Risk Appetite Framework e del Risk Appetite Statement.

Business Continuity

- Il monitoraggio dell'efficacia del piano di business continuity e di crisis management. La *Business Continuity* e il *Crisis Management* sono parti integranti del sistema di governo societario. La *Business Continuity* si basa innanzitutto sulla anticipazione e simulazione degli scenari avversi, grazie a strumenti chiave dell'organizzazione aziendale, come l'analisi d'impatto operativo (*Business Impact Analysis*), che garantisce sostenibilità e recupero di tutti i processi in caso di crisi. La preparazione alle emergenze parte da una solida cultura del rischio e dal pieno supporto di Comitato Controllo Rischi e *Top Management*, ma richiede anche piani di azione e comunicazione per ciascuna delle principali minacce, oltre a training specifici e simulazioni per i dipendenti delle aree a maggior rischio. Per la *Business Continuity* e il *Crisis Management*, il CCR supporta l'Organo di amministrazione nella validazione del framework di gestione delle crisi ed il piano di azione per i maggiori rischi individuati e assicura che questi elementi siano integrati nel più ampio sistema di controllo interno e gestione dei rischi. Il CCR è coinvolto nell'approvazione delle procedure per la gestione delle crisi e può ricoprire ruoli chiave nella Governance stessa della *Business Continuity* e del *Crisis Management* in caso di realizzazione di una crisi (ad es. la crisi recentemente determinata dal Covid-19), come ad esempio, l'attivazione di un flusso informativo nel continuo nei confronti del Comitato Controllo e Rischi su *Key Indicators*, oltre che sessioni dedicate su particolari argomenti. Inoltre, il Comitato Controllo e Rischi, in caso di crisi, dovrebbe verificare la presenza di un adeguato processo di gestione della comunicazione nei confronti di tutti gli *stakeholder*.

---

58 Ossia ogni atto posto in essere, da qualunque socio o persona autorizzata ad agire in nome e per conto della società, da cui derivano conseguenze dannose per la società.

59 The IIA's Three Lines Model.

60 COSO 2013, COSO 2017, FSB 2014, ISO31000 ecc.

61 Si veda per maggiore dettaglio il paper Nedcommunity (2013), Come valutare la governance in tema di rischi e controlli.

La cultura aziendale

- La valutazione della cultura aziendale in tema di *risk management* attraverso l'analisi dell'ambiente di controllo[62] e l'ambiente interno[63] in generale.

Il fattore umano

- La verifica della presenza delle competenze necessarie a progettare e implementare efficacemente il SCIGR.

Accountability

- L'analisi e valutazione delle principali politiche aziendali collegate con il SCIGR, anche in ottica di accountability, deleghe di poteri e segregazione dei ruoli. In particolare, la valutazione dell'assetto organizzativo a tutti i livelli e in coerenza con il modello delle tre linee, considera la tempestività di aggiornamento e la completezza della struttura organizzativa nonché la rispondenza di tale assetto alle esigenze di business e di governance in termini sia di professionalità che di capacità di raggiungere gli obiettivi strategici e operativi, tenendo conto dell'adeguatezza del sistema delle deleghe; considera a tale proposito la capacità del management di rispondere all'evoluzione del contesto (cd. *change management*) e di possedere le necessarie caratteristiche di leadership e di team skill per guidare in modo coeso il piano strategico. Include inoltre l'analisi della presenza di processi completi end-to-end, con chiara definizione di ruoli e responsabilità delle diverse funzioni coinvolte (*accountability*). La promozione della definizione e della diffusione di una cultura del rischio che sia coerente con l'obiettivo della creazione di valore sostenibile nel tempo e sia recepita negli schemi di remunerazione del management (coordinamento con Comitato Remunerazioni).

La mitigazione dei rischi (SCIGR)

- L'approfondimento sui sistemi di controllo a fronte dei rischi valutati significativi. Il CCR potrà richiedere approfondimenti specifici sui processi aziendali di controllo interno per alcune tematiche significative che emergono nel corso dell'analisi dei rischi, della pianificazione strategica, dell'analisi dei risultati di internal audit, ecc. A titolo esemplificativo: IT – sicurezza informatica, Ambiti del Supply Chain (Procurement ...), Operazioni M&A, Salute e Sicurezza sul lavoro e rischi ambientali (Environment Health and Safety - EHS), Tax

---

62 L'ambiente di controllo rappresenta uno dei componenti del COSO Internal Control - Integrated Framework ed è definito come l'insieme di norme, valori, processi e strutture alla base del Sistema di controllo interno e di gestione dei rischi delle organizzazioni. L'Organo di amministrazione e il *management* stabiliscono la struttura del SCIGR, inclusi gli standard di comportamento attesi, attraverso le direttive emanate, le azioni e i comportamenti agiti. Il ruolo del *management* della Società, a tutti i livelli, rinforza e sottolinea l'importanza degli standard di comportamento desiderati. L'ambiente di controllo rappresenta le fondamenta dell'intero SCIGR e pertanto esercita la sua influenza sulle altre componenti del COSO nonché su tutta la struttura organizzativa societaria. In particolare, l'ambiente di controllo richiede che siano individuati i seguenti aspetti:

- i principi di integrità ed etici cui l'organizzazione deve adeguarsi;
- gli elementi che consentono all'Organo di amministrazione di svolgere azioni di indirizzo per il *management* e di svolgere i propri compiti di supervisione;
- la definizione della struttura organizzativa e l'assegnazione di ruoli e responsabilità;
- il processo per attrarre, sviluppare e trattenere il personale;
- la metodologia per la misurazione delle *performance* e la definizione di incentivi e premi.

L'ambiente di controllo è influenzato da una varietà di fattori endogeni ed esogeni quali la storia della Società, i valori, i mercati di riferimento, lo scenario competitivo e la normativa di settore. Inoltre, influenza le attività di valutazione dei rischi ai fini del raggiungimento degli obiettivi aziendali, le Attività di Controllo, l'uso delle informazioni e dei sistemi di comunicazione nonché le Attività di Monitoraggio. In base all'impostazione *principles based* del COSO 2013, tesa a favorire e facilitare la valutazione del SCIGR, l'ambiente di controllo è composto da 5 principi, il cui disegno e la cui operatività sono il presupposto per la valutazione dell'adeguatezza dell'intera componente. Molto utile in tal senso la monografia Assirevi "COSO Framework: guida alla lettura".

63 **L'ambiente interno** era uno degli 8 componenti del COSO Framework ERM 2004. Esso rivela l'impostazione di un'organizzazione, poiché evidenzia il livello di sensibilità del Vertice e di tutto il personale rispetto al tema del SCIGR. Con la pubblicazione del COSO Framework ERM (2017), framework complementare e non fungibile rispetto al COSO – Integrated Control Framework del 2013, **l'ambiente interno** si integra nella "Risk governance & culture", cioè come l'impresa nel suo complesso affronta il rischio e la cultura del rischio, che riguarda gli atteggiamenti e i valori di chi opera nell'azienda. L'ambiente interno di un'organizzazione è definito come l'insieme degli elementi interni che possono influenzare anch'essi il conseguimento degli obiettivi aziendali e determina i modi in cui il rischio è considerato e affrontato dalle persone che operano in azienda, come pure la filosofia della gestione del rischio, i livelli di accettabilità del rischio, l'integrità e i valori etici e l'ambiente di lavoro in generale. Gli stakeholder interni sono soggetti che lavorano per l'organizzazione e possono influire direttamente sulle decisioni aziendali (gli amministratori, il management, etc.). Come per l'ambiente esterno, anche i fattori che compongono l'ambiente interno possono essere suddivisi in diverse categorie, quali ad esempio: capitale, risorse umane, processi e tecnologia. Possono includere tra l'altro i seguenti aspetti: sistemi di incentivazione; sistema disciplinare; sistemi di aggiornamento organizzativo (compreso succession planning, ciò di concerto con il Comitato Nomine); iniziative formative; sistemi aziendali di comunicazione, codici etici e deontologici; eventuali survey. Considera inoltre l'efficacia dei flussi di comunicazione quali informazioni fornite dai responsabili delle funzioni di risorse umane e dal responsabile ICT; la strutturazione e adeguatezza del reporting gestionale anche tra funzioni aziendali; le informazioni fornite dai responsabili di controllo della seconda e terza linea; l'analisi della scala di maturità.

compliance/governance e Gestione finanziaria. Inoltre, a fronte delle recenti normative[64] in tema di intelligenza artificiale (AI), il CCR può richiedere approfondimenti in merito alla gestione dei relativi rischi e alle modalità intraprese dalle organizzazioni per garantire un corretto utilizzo dell'AI. In particolare, con l'evoluzione della tecnologia legata all'AI, diventa necessario identificare e analizzare i rischi correlati al suo utilizzo e mantenere in continuo aggiornamento le relative politiche e le procedure, ivi incluse quelle relative all'AI Governance.

Tali approfondimenti dovrebbero permettere il Comitato a comprendere le modalità di governance, comprese eventuali progettualità di miglioramento in corso, di un determinato processo aziendale, tramite specifiche presentazione da parte del management.

PRINCIPALI DISPOSIZIONI PER IL SETTORE FINANZIARIO

- Supporta l'OFSS (Organo con Funzione di Supervisione Strategica) nella verifica della corretta attuazione delle strategie, delle politiche di governo dei rischi e del RAF. In particolare, con riferimento al RAF, svolge l'attività valutativa e propositiva necessaria affinché l'organo con funzione di supervisione strategica possa definire e approvare gli obiettivi di rischio ("Risk appetite") e la soglia di tolleranza ("Risk tolerance"). Inoltre, accerta che gli incentivi sottesi al sistema di remunerazione e incentivazione siano coerenti con il RAF.
- Supporta l'Organo di amministrazione nell'assicurare che la società sia dotata di un sistema di registrazione e di reportistica dei dati che ne consenta la tracciabilità al fine di poter disporre di informazioni complete ed aggiornate sugli elementi che possono incidere sul profilo di rischio della società e sulla sua situazione di solvibilità.
- Supporta l'Organo di amministrazione nell'assicurare che i sistemi informatici siano appropriati rispetto alla natura, portata e complessità dell'attività della società, nonché dei conseguenti rischi e possano fornire informazioni, sia all'interno che all'esterno, rispondenti ai principi di buona governance.
- Supporta l'Organo di amministrazione nell'assicurare che siano adottate procedure per garantire la continuità dei processi aziendali, attraverso sistemi di disaster recovery e piani di business continuity con le opportune misure organizzative, tecniche e di comunicazione.

3.e) I Rapporti con l'Internal Audit e le altre funzioni di controllo

Il CCR supporta l'Organo di amministrazione:

- **nella nomina e revoca del responsabile della funzione di internal auditing, definendo la sua remunerazione, assicurando l'adeguatezza di risorse** (umane, finanziarie, tecnologiche) anche ai fini di assicurare il rispetto degli Standard professionali di riferimento, globalmente riconosciuti ed espressamente richiamati sia nel Codice di Corporate Governance sia nella Regolamentazione del settore finanziario[65];
- **nell'approvazione del piano di lavoro di internal auditing sentito l'Organo di controllo e il CEO;**
- **nella valutazione della opportunità di adottare misure per garantire efficacia e imparzialità di giudizio delle funzioni aziendali coinvolte nei controlli diverse dall'internal auditing (esempio: risk management, presidio del rischio legale e di non conformità), articolate in relazione a dimensione, settore, complessità e profilo di rischio dell'impresa;**
- **nella nomina dell'organismo di vigilanza ai sensi del D.Lgs. 231/2001[66] nonché nel garantire adeguati flussi informativi da e verso tale organismo, anche avuto riguardo alla necessità delle imprese di assicurare il coordinamento, anche informativo, fra organi e funzioni di controllo;**
- **nella richiesta all'internal audit di svolgere verifiche su specifiche aree operative/ strategiche;**

64 Regolamento europeo n.1689 del 13 giugno 2024 "*Artificial Intelligence Act*".
65 Rif. Circolare 285 Banca d'Italia e Regolamento 38 IVASS.
66 Utili in tal senso anche i seguenti documenti: La gestione dei flussi informativi tra Collegio Sindacale e Organismo di Vigilanza ex D.Lgs. 231/01 (https://www.aodv231.it/documenti-di-approfondimento/la-gestione-dei-flussi-informativi-tra-collegio-sindacale-e-organismo-di-vigilanza/) e Regolamento dell'Organismo di Vigilanza (https://www.aodv231.it/documenti-di-approfondimento/regolamento-dellorganismo-di-vigilanza/).

- **nel monitoraggio di autonomia, adeguatezza, efficacia ed efficienza della funzione di internal audit,** anche i) promuovendo verifiche esterne di quality assurance ai sensi degli Standard professionali globalmente riconosciuti; ii) assicurando opportuni flussi informativi verso l'internal audit; iii) assicurando la partecipazione dell'internal audit, quale standing *invitee*, almeno al Comitato Controllo e Rischi stesso e ai Comitati di Sostenibilità, prevedendo periodicamente anche sessioni private senza la presenza del Management;
- **nell'analisi delle relazioni periodiche e quelle di particolare rilevanza predisposte dalla funzione di internal auditing.**

Inoltre, nell'espletamento dei propri compiti, il CCR può svolgere:

- l'analisi delle relazioni periodiche predisposte dall'Organismo di Vigilanza, che svolge vigilanza sistemica[67], per informativa all'Organo di amministrazione;
- l'analisi delle relazioni periodiche predisposte dalle altre funzioni di controllo di secondo livello (CIO, Conformità, Risk Manager, ecc.);
- la verifica della separazione e della indipendenza tra i controlli di secondo livello (risk management, compliance, ecc.) e terzo livello (internal audit e vigilanza sistemica dell'Organismo di Vigilanza), nonché del perimetro delle funzioni di secondo livello e dell'efficace ed efficiente sistema di flussi informativi tra le funzioni di controllo, in linea con il modello delle tre linee[68];
- l'analisi di ulteriori documenti e politiche significative al fine del controllo interno incluse quelle sul coordinamento fra le diverse funzioni di controllo e/o cosiddetti "fornitori di assurance".

Il Piano Audit

Il CCR può quindi prendere in esame: la pianificazione annuale e pluriennale dell'internal audit[69] (obiettivi della funzione, piano delle risorse, piano di internal audit) e il suo monitoraggio anche al fine di poter apportare delle modifiche in funzione dell'evoluzione dei rischi (dynamic audit plan); il piano di vigilanza ai sensi del D.Lgs. 231/01; l'informativa fornita dall'Organo di controllo; la composizione dell'"universo di audit"; i criteri di risk assessment indipendenti dell'internal audit; laddove pertinente, i criteri di copertura dell'audit di medio termine. Secondo la leading practice espressa dall'Institute of Internal Auditors (di seguito "IIA"), ci si aspetta che il piano sia risk-based, dinamico e aggiornato tempestivamente in risposta a eventuali cambiamenti intervenuti in azienda[70]. Nell'effettuare le proprie valutazioni il CCR opera in sinergia con l'Organo di controllo e con il CEO, in quanto l'Organo di controllo e il CEO devono essere sentiti dall'Organo di amministrazione per l'approvazione del Piano.

Gli esiti di Audit

L'analisi delle relazioni periodiche della funzione Internal Audit include anche il monitoraggio delle attività di follow up dei piani di rimedio e di situazioni di criticità non ancora risolte[71]. Tali analisi contribuiscono in modo significativo anche alla valutazione del SCIGR.

Per quanto riguarda il monitoraggio del governo della funzione**,** i nuovi standard professionali, i Global Internal Audit Standards, intendono guidare la professione di Internal Auditing a livello mondiale e rappresentano la base per valutare e migliorare la qualità dell'operato della funzione Internal Audit. Il cuore degli Standard è costituito da 15 principi guida. Ogni principio è supportato da Standard che contengono requisiti, indicazioni per l'implementazione ed esempi di conformità. L'insieme di questi elementi aiuta gli Internal Auditor a rispettare i propri principi e a realizzare il Purpose dell'Internal Auditing.

---

67 "L'organismo di vigilanza: struttura, funzione e responsabilità" di Rocco Blaiotta in Rivista Sistema Penale; Articolo "Una sentenza modello della Cassazione pone fine all'estenuante vicenda "Impregilo"" di Carlo Piergallini su Rivista Sistema Penale; "Il caso Impregilo: luci e ombra sulla questione Giustizia" – caso Assonime 4/2022.

68 The IIA's Three Lines Model.

69 Rif Global Internal Audit Standards (2024).

70 Si rinvia al Global Internal Audit Standards dell'IIA 2024 "Standard 9.4 Piano di Audit".

71 Rif Global Internal Audit Standards (2024).

In tale contesto, secondo quanto riportato dai Global Internal Audit Standards, vi sono svariati aspetti che possono essere presi in esame da parte del CCR al fine di supportare l'Organo di amministrazione nell'espletamento dei propri compiti[72].

Le funzioni di controllo di secondo livello

Nell'ambito del modello delle tre linee di controllo, il CCR si avvale dell'operato di funzioni di controllo che operano nell'ambito del secondo livello. In particolare, assumono un ruolo sempre più cruciale, nell'ambito del SCIGR le funzioni di risk management e compliance affiancate, in base alla complessità e alla rilevanza del profilo di rischio, da funzioni specialistiche dedicate a rischi specifici quali, ad esempio, i rischi in materia di salute e sicurezza, Privacy, antiriciclaggio, antitrust, anticorruzione, cybersecurity, ecc. Tali funzioni di secondo livello si caratterizzano per autonomia e indipendenza, ricevendo il mandato organizzativo direttamente dall'Organo di amministrazione o dall'organo delegato. Inoltre, in taluni casi, riportano funzionalmente all'Organo di amministrazione, per il tramite del Comitato Controllo e Rischi. Con riferimento agli obiettivi e alle attività operative, svolgono, ex ante, attività di risk assessment finalizzate all'identificazione e alla valutazione dei rischi ed, ex post, attività di monitoraggio, al fine di verificarne l'andamento nonchè la robustezza dei controlli interni implementati per la loro mitigazione. I modelli operativi si ispirano ai medesimi framework di controllo (es. COSO framework) e agiscono in modo in integrato con la funzione Internal Audit.

Il CCR dovrebbe esaminare tutti gli aspetti sostanziali dei processi di risk e compliance management presenti in azienda. Tale esame dovrà comprendere la valutazione del perimetro di attività e le modalità di pianificazione delle stesse, nonché esaminare i risultati delle attività di assessment e monitoraggio.

In tale contesto, il CCR può valutare, a titolo esemplificativo, ulteriori **documenti e politiche** quali il codice etico; la procedura per la gestione delle segnalazioni interne (*whistleblowing*), le politiche sicurezza sul lavoro, le politiche di gruppo su specifici processi chiave all'azienda (es investimenti, procurement, outsourcing, gestione finanziaria, ecc.), le politiche di remunerazione con riferimento agli aspetti legati al SCIGR.

[72] In particolare, tali aspetti posso comprendere:
- il mandato della funzione di Audit;
- l'Internal Audit Charter che include il purpose, l'impegno ad aderire ai Global Internal Audit Standards e il mandato della funzione e la posizione organizzativa e reporting;
- le modalità di supporto da parte dell'Organo di amministrazione, in termini ad esempio all'accesso ai dati, alle comunicazioni regolari e dirette, all'analisi di eventuali restrizioni, e del Top Management, ad esempio in termini di collaborazione nell'ambito degli interventi di audit;
- l'indipendenza organizzativa tenendo conto della linea di reporting gerarchico e funzionale e le qualifiche dell'internal audit valutate anche in termini di anzianità nella posizione, le risorse, le competenze, i titoli professionali e le certificazioni degli Auditor. Il CCR fornisce parere sulla nomina o revoca del responsabile della funzione, svolta in sinergia con il Comitato Nomine e/o Remunerazione o eventuale altro comitato preposto alla governance, che prende in considerazione tutti gli aspetti di merito in termini di requisiti professionali, remunerazione, motivazioni sottostanti la proposta. Questa attività nella prassi è spesso svolta in sinergia anche con l'Organo di controllo;
- le risorse sufficienti per soddisfare il Mandato di Internal Audit e realizzare il piano (dinamico) risk based di Internal Audit;
- il monitoraggio del programma sistematico di miglioramento (QAIP – Quality Assurance Improvement Program) comprensivo sia dei Quality Assessment interni sia di quelli esterni come richiesti dagli standard professionali (la valutazione esterna è richiesta almeno ogni cinque anni e fornisce, tra l'altro, un parere sul livello di conformità della funzione al framework di standard professionali internazionali IIA);
- il grado di copertura dell'attività svolta dalla funzione di Audit rispetto all'"universo" di audit; l'approccio metodologico adottato per le valutazioni di audit.

Nell'ambito del proprio posizionamento, la funzione Internal Audit, in alcuni contesti, riporta funzionalmente al CCR. In altri, laddove il riporto non è non formalizzato esplicitamente, dispone ad ogni modo di un accesso costante al CCR tramite un'interlocuzione continua con il Comitato al fine di rendicontare i risultati delle attività svolte in qualsiasi momento in base alle necessità. Tale interlocuzione si coniuga inoltre con la possibilità del CCR di richiedere, in qualsiasi momento, all'Internal Audit di svolgere opportune verifiche su specifiche aree operative e/o strategiche.
Il Comitato dovrebbe svolgere almeno una volta all'anno incontri privati (cioè, senza il CEO o il management) con il responsabile dell'Internal Audit, al fine di controllare l'assenza di circostanze che potrebbero inficiare l'indipendenza della funzione o l'efficacia dello svolgimento del ruolo.

PRINCIPALI DISPOSIZIONI PER IL SETTORE FINANZIARIO

- Individua e propone la nomina/revoca del responsabile della funzione di Internal Audit e delle altre funzioni di controllo (Risk Management, Compliance, AML, ecc.) con il supporto del comitato nomine (ove presente).
- Supporta l'Organo di amministrazione nella complessiva supervisione dell'assetto organizzativo (ivi incluse le attività esternalizzate) in termini di completezza, funzionalità ed efficacia.
- Esamina preventivamente il piano di attività e le relazioni periodiche delle funzioni di controllo, oltre a quelle di particolare rilevanza, indirizzate all'Organo di amministrazione.
- Esprime valutazioni e formula pareri all'Organo di amministrazione sui requisiti che devono essere rispettati dalle funzioni di controllo; portare all'attenzione dell'organo gli eventuali punti di debolezza e le conseguenti azioni correttive da promuovere, valutando le proposte dell'organo con funzione di gestione.
- Contribuisce, per mezzo di valutazioni e pareri, alla definizione della politica aziendale di esternalizzazione di funzioni aziendali di controllo.
- Supporta l'Organo di amministrazione in merito alla predisposizione del documento di coordinamento delle funzioni e organi di controllo e verifica che le funzioni aziendali di controllo si conformino correttamente alle indicazioni e alle linee dell'organo ivi definite.
- Anche attraverso i flussi istituiti con le funzioni di controllo, supporta l'Organo di amministrazione nell'assicurare che siano adottati e formalizzati adeguati processi decisionali, che sia attuata una appropriata separazione di funzioni e che i compiti e le responsabilità siano adeguatamente assegnati, ripartiti e coordinati in linea con le politiche dell'impresa e riflessi nella descrizione degli incarichi e delle responsabilità. Tutti gli incarichi rilevanti devono essere assegnati, deve essere istituito un adeguato sistema di deleghe e devono essere evitate sovrapposizioni non necessarie, promuovendo un'efficace cooperazione tra tutti i membri del personale.
- Collabora con gli altri organi e funzioni cui è attribuita una funzione di controllo (es. internal audit, risk management, compliance, antiriciclaggio, rischi ICT, sicurezza, ecc.) assicurando un'adeguata collaborazione, anche informativa, per l'assolvimento dei compiti ad esso assegnati. I collegamenti tra gli stessi sono stabiliti dall'Organo di amministrazione.

3.f) La valutazione di adeguatezza del SCIGR

Il CCR, nel coadiuvare l'Organo di amministrazione:

- **riferisce all'Organo di amministrazione, almeno in occasione dell'approvazione della relazione finanziaria annuale e semestrale, sull'attività svolta e sull'adeguatezza del sistema di controllo interno e di gestione dei rischi.**

La valutazione periodica del SCIGR a supporto dell'Organo di amministrazione è la sintesi degli esiti dell'attività svolta dal CCR in merito al SCIGR elencate nei paragrafi precedenti. In tale valutazione il CCR tiene conto delle linee di indirizzo del sistema di controllo interno e gestione dei rischi approvate dall'Organo di amministrazione.

La valutazione può anche riguardare le informazioni fornite dall'amministratore delegato[73] e dal dirigente preposto alla redazione dei documenti contabili e societari, l'efficacia e l'effettiva indipendenza della funzione di Internal Auditing nonché le criticità emerse dalle attività di Internal Auditing e relativi piani di rafforzamento del management; i flussi informativi provenienti dalle funzioni di controllo di secondo livello o altre funzioni aziendali coinvolte nei controlli; le informazioni fornite dalla società di revisione nella relazione aggiuntiva (eventuali carenze significative del SCIGR) trasmesso all'Organo di amministrazione tramite l'Organo di controllo, l'evoluzione delle politiche e delle linee guida di *governance;* l'evoluzione dell'impianto procedurale; le informazioni fornite dalla società di revisione o dall'Organo di controllo.

[73] Nell'ambito del suo ruolo in relazione al SCIGR definito dalla Raccomandazione 34 b del Codice.

La valutazione dovrà inoltre comprendere gli esiti dell'analisi dell'ambiente di controllo e dell'ambiente interno (cfr. sezione 3.d) la gestione del rischio). Il parere può essere espresso in base alle politiche adottate sia in forma di *positive assurance* (cioè l'esplicita conferma che il SCIGR risulti essere adeguato) o di *negative assurance* (cioè la conferma che il SCIGR risulti essere adeguato perché non c'è evidenza del contrario, in altre parole affermare che non ci sono evidenze tali da indicare che il SCIGR non sia adeguato)[74].

DISPOSIZIONI PER IL SETTORE FINANZIARIO [non esaustive]

- Identifica tutti i flussi informativi che a esso devono essere indirizzati in materia di rischi (oggetto, formato, frequenza ecc.) e deve poter accedere alle informazioni aziendali rilevanti.
- Riceve la valutazione di adeguatezza del sistema di controllo interno.

3.g) L'informativa societaria

Il CCR svolge le seguenti attività di:

- **supporto all'Organo di amministrazione nell'esame della relazione finanziaria e di rendicontazione di sostenibilità (Legge 262/2005 e D.Lgs. 125/2024);**
- **valutazione dell'idoneità dell'informazione periodica, finanziaria e di sostenibilità, a rappresentare il modello di business, le strategie e le performance;**
- **analisi del contenuto dell'informazione periodica a carattere non finanziario rilevante ai fini del SCIGR;**
- **supporto all'Organo di amministrazione nella valutazione dei risultati esposti dalla società di revisione nella eventuale lettera di suggerimenti e nella relazione aggiuntiva;**
- **valutazione (sentiti il dirigente preposto, la società di revisione e l'Organo di controllo) sul corretto utilizzo dei princìpi contabili** e degli standard di rendicontazione di sostenibilità (standard ESRS ai sensi della CSRD);
- analisi del processo e dell'esito dell'impairment test;
- analisi delle modalità di rilevazione, gestione, monitoraggio, rappresentazione in bilancio e comunicazione dei rischi finanziari, rischio di credito e rischio di liquidità, nonché delle modalità, conformemente agli obblighi previsti dal 2° comma dell'art. 2086 del c.c., introdotto dal D.Lgs. 14 del 12 gennaio 2019 denominato "Codice della crisi d'impresa e dell'insolvenza", con cui l'impresa ha attivato un processo di monitoraggio per la preventiva individuazione degli eventuali squilibri di carattere economico – finanziari;
- analisi dell'adeguatezza della comunicazione relativa all'impatto dei rischi principali sulla performance attraverso l'informativa finanziaria e di sostenibilità;
- analisi delle relazioni periodiche che il dirigente preposto alla redazione dei documenti contabili societari e, laddove differente, il dirigente preposto alla rendicontazione di sostenibilità, predispongono con riferimento ai sistemi di controllo sull'informativa finanziaria e di sostenibilità.

L'analisi dell'informazione periodica di sostenibilità è materia relativamente recente ed in fase di forte evoluzione[75]. Data la rilevanza crescente di tale informativa per il mercato e la valutazione dell'impresa, i regolatori e gli organi di autodisciplina stanno ponendo particolare attenzione agli aspetti di formazione e controllo degli indicatori non finanziari. Il decreto legislativo 6 settembre 2024, n. 125 di recepimento della CSRD esplicita le responsabilità degli attori coinvolti nell'ambito dell'informativa di sostenibilità, tra cui l'Organo di controllo, la società di revisione e il dirigente responsabile dell'attestazione ai sensi dell'art.154-bis del D.Lgs. n.58 24 febbraio 1998. Il Codice di Corporate Governance (2020) ha esplicitato le responsabilità "minime" del CCR sull'informativa di sostenibilità assimilabile a quelle sull'informativa finanziaria, volte a esaminare il contenuto in funzione del SCIGR e a valutare l'idoneità a rappresentare il modello di business.

[74] Maggiori indicazioni nel paper Nedcommunity (2013), *Come valutare la governance in tema di rischi e controlli* e nel paper AIIA (2021), *L'Overall Opinion come strumento di comunicazione strategica per le organizzazioni*.

[75] Come sintetizzato nel paper Nedcommunity- KPMG (2020), *Informativa extra finanziaria: da compliance a governance strategica dei rischi e delle opportunità*.

- Per quanto riguarda il SCIGR, il CCR valuta la presenza di sistemi e procedure per la costruzione delle metriche (includendo l'identificazione delle funzioni responsabili di ciascun indicatore e l'esistenza di un meccanismo per il controllo) e l'adeguatezza rispetto agli standard di riferimento indicati nell'informativa di sostenibilità[76]. Nello svolgere questi compiti, il CCR incontra la società di revisione e sente l'Organo di controllo nonché l'eventuale società di revisione per l'attestazione del bilancio di sostenibilità, qualora diversa dalla società di revisione incaricata per l'informativa finanziaria.
- Per quanto riguarda l'idoneità a rappresentare il modello di business, il CCR valuta la coerenza con il piano strategico, l'analisi della rilevanza e l'impatto delle componenti di sostenibilità sulle analisi di rischio verticali specifiche e/o di entreprise risk management dell'azienda. A tale scopo si coordina con il Comitato eventualmente predisposto nell'ambito dell'Organo di amministrazione con i compiti definiti nella Raccomandazione 1 a) ("*l'analisi dei temi rilevanti per la generazione di valore nel lungo termine*") (es. Comitato Sostenibilità).

CSRD

La CSRD inoltre introduce la necessità per le aziende a cui si applica la normativa, di rendicontare le caratteristiche dei propri sistemi di controllo e gestione del rischio in relazione alla rendicontazione di sostenibilità e al processo decisionale[77]. Viene pertanto introdotta la necessità di instaurare, in linea con i sistemi di controllo interno sull'informativa finanziaria, dei sistemi di controllo legati all'informativa di sostenibilità (SCIS).

In tale ambito, gli ESRS prevedono che le Società debbano divulgare le caratteristiche principali dei propri sistemi interni di controllo e gestione del rischio di rendicontazione di sostenibilità fornendo le seguenti informazioni ambito, caratteristiche principali e componenti:

- approccio di valutazione dei rischi;
- principali rischi identificati, strategie di mitigazione e relativi controlli;
- descrizione dell'integrazione dei risultati del risk assessment e dei controlli interni nei propri processi;
- descrizione della comunicazione periodica dei risultati agli organi di amministrazione, gestione e controllo.

Il CCR supporta l'Organo di amministrazione anche nell'esame del modello utilizzato per il sistema di controllo volto a garantire l'integrità dell'informativa finanziaria e di sostenibilità. Il modello di riferimento maggiore ai fini del financial reporting è il COSO Framework (2013) *Internal Controls* – Integrated Framework, emesso dal Committee of Sponsoring Organizations of the Treadway Commission negli Stati Uniti meglio descritto nel paragrafo 1.

Più recentemente, l'affermazione delle tematiche di sostenibilità nell'ambito della corporate governance e l'obbligo per alcune società (che rientrano nei limiti definiti dalla legge) di dare disclosure sull'informativa di sostenibilità (cfr. CSRD) ha introdotto, per tali imprese, un nuovo ambito di rendicontazione delle proprie performance di sostenibilità (ambiente, comunità di riferimento, personale, rispetto dei diritti umani, lotta alla corruzione attiva e passiva).

Il modello COSO per il reporting ESG

Al fine di assicurare, anche in questo ambito, l'affidabilità delle informazioni di sostenibilità diffuse al pubblico, le imprese dovrebbero predisporre e implementare un adeguato Sistema di Controllo Interno. Assumere come modello di riferimento il COSO Framework, consente, tra le altre cose, di valorizzare quanto già esistente a presidio dei rischi sull'informativa finanziaria. In particolare, il COSO Framework è stato concepito, sin dalla sua prima edizione del 1992, come un modello integrato ovvero idoneo a stabilire un Sistema di Controllo Interno a presidio di tutti i rischi aziendali. A tale proposito, come anticipato, il 30 marzo 2023, il COSO ha emanato la guida integrativa intitolata "*Achieving Effective Internal Control of Sustainability Reporting (ICSR)*" che rappresenta ad oggi un autorevole riferimento per la definizione di un efficace sistema di controllo sull'informativa di sostenibilità (SCIS) e che evidenzia, tra l'altro, la necessità di fare sinergie con sistemi di controllo già esistenti. La linea guida del COSO, richiama integralmente quanto già definito nell'ambito del COSO Framework, e pone l'attenzione sui seguenti principali aspetti:

---

76 Particolarmente utile la lettura del documento del **WEF** (2020), *Toward Common Metrics and Consistent Reporting of Sustainable Value Creation*, che fa riferimento ai principali standards di rendicontazione (Global Reporting Initiative, Sustainability Accounting Standards Board, Task Force on Climate-related Financial Disclosures).

77 Articolo 29 ter "Principi di rendicontazione di sostenibilità" che *[…] I principi di rendicontazione di sostenibilità specificano, tenendo conto dell'oggetto di un determinato principio di rendicontazione di sostenibilità:*
[…] c) le informazioni che le imprese sono tenute a comunicare riguardo ai seguenti fattori di governance:
[…] ii) le caratteristiche principali dei sistemi interni di controllo e gestione del rischio dell'impresa, in relazione alla rendicontazione di sostenibilità e al processo decisionale".

- Governance: i ruoli e responsabilità rispecchiano il “Three Lines Model” e includono l’Organo di amministrazione, i Comitati, le Funzioni di business e di supporto, gli assurance provider e l’Internal Audit.
- Customization and Adaptation: Nel SCIS sono presenti e funzionanti i 17 principi disciplinati dal COSO Internal Control e il livello di raggiungimento di tali principi tiene conto delle caratteristiche di ciascuna organizzazione, del livello di maturità e del settore di appartenenza.
- Top down & Risk Based approach: Il SCIS copre un subset di datapoint tra quelli previsti dalla normativa e applicabili alla Società, selezionati tra quelli più rilevanti per la crescita sostenibile dell’azienda e per la creazione di valore.
- Integration & Leverage: il SCIS rappresenta una nuova applicazione dei principi di controllo che si sono consolidati negli anni nell’ambito del reporting finanziario. Una parte di informativa di sostenibilità richiede l’istituzione di nuovi processi e controlli. Tuttavia, alcuni controlli che già esistono nell’ambito del reporting finanziario o in altre aree di reporting aziendale possono essere adattati per essere applicati al reporting di sostenibilità.

PRINCIPALI DISPOSIZIONI PER IL SETTORE FINANZIARIO

- Valuta il corretto utilizzo dei principi contabili per la redazione dei bilanci d’esercizio e consolidato, coordinandosi con il dirigente preposto alla redazione dei documenti contabili e con l’Organo di controllo.
- Supporta l’Organo di amministrazione:
  - nella definizione delle politiche e dei processi di valutazione delle attività aziendali, inclusa la verifica che il prezzo e le condizioni delle operazioni con la clientela siano coerenti con il modello di business e le strategie in materia di rischi;
  - nella pre-istruttoria della Dichiarazione sulla Sostenibilità in vista dell’approvazione da parte da perte dell’Organo di amministrazione nell’ambito della Relazione sulla Gestione, assicurando che la redazione avvenga in osservanza delle norme di riferimento e rifletta l’andamento dell’impresa alla luce dei fattori di sostenibilità;
  - nell’esame dell’andamento dei rischi in materia di sostenibilità nell’ambito della rendicontazione periodica trasmessa dalle funzioni aziendali di controllo e nell’adozione delle misure di presidio;
  - nell’assicurare l’integrazione nelle attività di controllo svolte sulla Dichiarazione sulla Sostenibilità e l’attuazione di azioni di rimedio ove necessario.

4 L'agenda del CCR

Le funzioni del CCR, come definite nel capitolo precedente, possono essere più o meno ampie a seconda della realtà specifica e dovranno essere quindi adattate. Fattori molto rilevanti sono il settore di appartenenza, la dimensione, la complessità e numerosità delle diverse aree di business, le geografie di riferimento e il grado di esposizione alla volatilità di fattori esterni. La maturità dell'organizzazione e il modello di governance complessiva, incluso il ruolo di altri Comitati endoconsiliari, sono inoltre essenziali per definire e articolare nel regolamento le specifiche attività e le modalità di funzionamento.

L'efficacia del CCR dipende proprio dalla sua capacità di adattamento alla realtà specifica e di ascolto e dialogo con le strutture interne e con gli altri organi coinvolti nel SCIGR. Di particolare rilevanza è la relazione costruttiva e sinergica che si crea con gli scambi con l'Organo di controllo. Rimandiamo al par. "2.d Confronto tra CCR e Organo di controllo" per un'analisi dei rispettivi ruoli al fine di facilitare la consapevolezza dei ruoli reciproci.

Di seguito riportiamo in modo semplificato l'indicazione di un'agenda di massima delle attività del CCR con le relative frequenze (annuale, semestrale, trimestrale), che potrebbe supportare l'efficace allineamento alle indicazioni del Codice di Corporate Governance e alle leading practice di riferimento, ricordando di tener conto della regolamentazione specifica per il settore finanziario. Tale proposta, come già accennato, deve essere adattata alla specifica realtà aziendale e beneficerebbe della specificazione i) degli invitati permanenti al CCR (standing invitees) e degli invitati "on an ad-hoc basis" (ad hoc invitees); ii) di eventuali sessioni periodiche in modalità privata con l'internal audit, con il risk management e, all'occorrenza, con altre funzioni di controllo.

Trimestralmente

Il processo di gestione dei rischi

- Incontri periodici con Responsabile risk management – monitoraggio dei rischi; esame dell'avanzamento delle attività rispetto al piano.

I rapporti con l'Internal Audit e le altre funzioni/organi di controllo

- Incontri periodici con Responsabile Internal audit; esame risultati di audit del trimestre, anche rispetto al piano, e analisi di follow-up; esame effettivo rispetto dei piani di rimedio da parte del management.
- Incontri periodici con Internal Audit e Organismo di Vigilanza, esame dei risultati delle rispettive attività di audit di terzo livello e della vigilanza sistemica di terzo livello.
- Incontri con la funzione Compliance, se presente; esame dell'avanzamento delle attività rispetto al piano.

Semestralmente

Il ruolo del CCR nell'ambito delle linee di indirizzo del SCIGR

- Approvazione della Relazione sulle attività del CCR nel semestre.

I rapporti con l'Internal Audit e le altre funzioni/organi di controllo

- Esame relazioni sull'attività semestrale (Internal Audit, Organismo di Vigilanza, Risk Manager, Responsabile Compliance, altri responsabili di funzioni di controllo di secondo livello) e incontri con i relativi responsabili.
- Approfondimenti e aggiornamenti con altre funzioni quando rilevante (Legale – contenziosi, IT – sicurezza informatica, intelligenza artificiale, data protection officer, segnalazioni (*whistleblowing*), Salute e Sicurezza sul lavoro, Ambiente (HSE), Procedure fiscali, Tax compliance, M&A, Procurement, Assicurazioni, laddove rilevante responsabile antiriciclaggio).

L'informativa societaria

- Esame Relazione finanziaria semestrale supportato da opportuni incontri con:
  - Dirigente Preposto: Impairment test, adeguatezza del Sistema di Controllo dell'Informativa Societaria (SCIS), rispetto procedure amministrative e contabili.
  - Responsabile finanziario: Rischi finanziari, rischio di credito, rischio di liquidità.
  - Società di revisione, in sinergia con l'Organo di controllo.

Annualmente

Il ruolo del CCR nell'ambito delle linee di indirizzo del SCIGR

- Parere su Linee guida del SCIGR.
- Valutazione assetto organizzativo, anche con riferimento al Modello delle Tre Linee e all'efficacia delle funzioni di controllo e/o cosiddetti "fornitori di assurance"[78].
- Valutazione dell'efficacia e adeguatezza del SCIGR.
- Esame Relazione sul Governo Societario e Relazione sulla Gestione: sezioni relative al SCIGR.

Il modello di risk management

- Monitoraggio sull'aggiornamento del modello, sulla tassonomia dei rischi, sulla mappa dei rischi.
- Definizione soglie di tolleranza per il Risk appetite Framework.

Il supporto nel processo di pianificazione strategica

- Scenari di piano strategico, integrato con gli obiettivi di sostenibilità, e analisi dei rischi di piano.

Il processo di gestione dei rischi

- Valutazione dell'effettiva implementazione del risk framework.
- Incontri con il management di una selezione di *business unit* rilevanti per l'attuazione delle strategie d'impresa.
- Politica di remunerazione: sezioni relative al SCIGR e monitoraggio che il sistema di remunerazione non incentivi l'eccessiva presa di rischio, fuori da risk appetite.

I rapporti con l'Internal Audit e le altre funzioni/organi di controllo

- Esame Relazioni annuali e incontri con Internal Audit, le funzioni di controllo di secondo livello, l'Organo di controllo, l'Organismo di Vigilanza.
- Incontro con l'Amministratore incaricato al sistema di controllo interno e gestione dei rischi.
- Esame del Piano strategico di audit[79].
- Esame del Piano di Internal Audit e relativo budget proposto per l'approvazione da parte dell'Organo di amministrazione (oltre ad eventuali ulteriori piani annuali delle altre funzioni di controllo ove presenti).
- Valutazione adeguatezza organizzativa dell'Internal Audit anche mediante analisi delle relazioni periodiche di Quality Assurance (quelle interne, almeno annualmente, quelle esterne, almeno ogni cinque anni)[80].
- Valutazione del Responsabile Internal Audit e livello/sistema remunerativo, avuto riguardo al suo posizionamento quale "n-1" posto il riporto all'Organo di amministrazione, all'autorevolezza e al fine di favorire virtuose rotazioni da e/o verso altre funzioni di business.

La valutazione di adeguatezza del SCIGR

- Valutazione dell'efficacia e adeguatezza del SCIGR.

L'informativa societaria

- Esame Relazione Finanziaria annuale. Incontri con:
  - Dirigente Preposto per la redazione dei documenti contabili e societari: Impairment test, adeguatezza del Sistema di Controllo dell'Informativa Societaria rispetto procedure amministrative e contabili.
  - Direttore Finanza: Rischi finanziari, rischio di credito, rischio di liquidità.
  - Società di revisione (in sinergia con l'Organo di controllo): aspetti materiali, metodologia di impairment e altre valutazioni contabili che richiedono valutazioni soggettive, piano e stato di avanzamento della

78 Rif Global Internal Audit Standards (2024), THE IIA'S THREE LINES MODEL.
79 Rif Global Internal Audit Standards (2024).
80 Rif Global Internal Audit Standards (2024).

revisione.

- Esame reportistica di sostenibilità ex CSRD. Incontri con:
  - Eventuale Comitato endoconsiliare preposto all'analisi della generazione di valore a lungo termine: coerenza con matrice di materialità e con modello di business.
  - Dirigente responsabile rendicontazione di sostenibilità (qualora diverso dalla figura del Dirigente Preposto): adeguatezza procedure di rilevazione e controllo metriche, rispetto degli standard ESRS a fini CSRD nonché eventuale adesione a standard di rendicontazione internazionali.
  - Società di revisione: processi e standard di rendicontazione.

APPENDICE 1 – Confronto dei compiti del CCR e dell'Organo di controllo in base alla normativa di riferimento

Il CCR …		L'Organo di controllo …
Il Comitato supporta l'Organo di amministrazione (Cfr. Codice - Raccomandazione 33) nella: • definizione delle linee di indirizzo del sistema di controllo interno e di gestione dei rischi; • descrizione, nella relazione sul governo societario, delle principali caratteristiche del sistema di controllo interno e di gestione dei rischi e delle modalità di coordinamento tra i soggetti in esso coinvolti, indicando i modelli e le *best practice* nazionali e internazionali di riferimento, esprimendo la propria valutazione complessiva sull'adeguatezza del sistema stesso e dando conto delle scelte effettuate in merito alla composizione dell'organismo di vigilanza). Il Comitato, nel coadiuvare l'Organo di amministrazione riferisce, almeno in occasione dell'approvazione della relazione finanziaria annuale e semestrale, sull'attività svolta e sull'adeguatezza del sistema di controllo interno e di gestione dei rischi.	**Linee di indirizzo e valutazione del SCIGR**	L'Organo di controllo: • vigila sull'adeguatezza della struttura organizzativa della società per gli aspetti di competenza, del sistema di controllo interno e del sistema amministrativo-contabile nonché sull'affidabilità di quest'ultimo nel rappresentare correttamente i fatti di gestione (TUF /D.Lgs 24/2/98 n.58, Art. 149, -1.c)); • vigila sull'adeguatezza della struttura organizzativa della società per gli aspetti di competenza e del sistema di controllo interno (TUF /D.Lgs 24/2/98 n.58, Art. 149 – 1.c)) ; • vigila 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 (TUF /D.Lgs 24/2/98 n.58, Art. 149 – 1.c-bis)).
Il Comitato, nel coadiuvare l'Organo di amministrazione, esprime pareri su specifici aspetti inerenti alla identificazione dei principali rischi aziendali e supporta le valutazioni e le decisioni dell'organo di amministrazione relative alla gestione di rischi derivanti da fatti pregiudizievoli di cui quest'ultimo sia venuto a conoscenza.	**Gestione del rischio**	L'Organo di controllo controlla l'efficacia dei sistemi di controllo interno della qualità e di gestione del rischio dell'impresa e, se applicabile, della revisione interna, per quanto attiene all'informativa finanziaria e, ove presente, alla rendicontazione individuale o consolidata di sostenibilità, senza violarne l'indipendenza (D.L. 39/2010 art. 19, c))
Il Comitato supporta l'Organo di amministrazione (Cfr. Codice - Raccomandazione 33) nella: • nomina e revoca del responsabile della funzione di internal audit, definendone la remunerazione coerentemente con le politiche aziendali, assicurandosi che lo stesso sia dotato di risorse adeguate all'espletamento dei propri compiti; I rapporti con l'IA; • approvazione, con cadenza almeno annuale, del piano di lavoro predisposto dal responsabile della funzione di internal audit, sentito l'organo di controllo e il chief executive officer. Il Comitato, nel coadiuvare l'Organo di amministrazione • esamina le relazioni periodiche 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 affidare alla funzione di internal audit lo svolgimento di verifiche su specifiche aree operative, dandone contestuale comunicazione al presidente dell'organo di controllo.	**Rapporti con l'Internal Audit**	L'Organo di controllo: • vigila sull'efficacia dei sistemi di revisione interna (D.L. 39/2010 art. 19, c); • viene sentito dall'Organo di amministrazione in merito alla nomina e alla revoca dei responsabili delle funzioni aziendali di controllo (Circolare 285 per le banche - Titolo IV, Cap. 3) • viene sentito dall'Organo di amministrazione ai fini della nomina e della revoca del titolare della funzione di revisione interna (IVASS regolamento 38, art. 37); • esprime un parere sul piano di lavoro del responsabile della funzione di internal audit (Codice di Corporate Governance Racc. 33 - c); • coloro che sono preposti al controllo interno riferiscono anche all'organo di controllo di propria iniziativa o su richiesta anche di uno solo dei suoi componenti (TUF /d.lg 24/2/98 n.58, Art. 150 c.4); • controlla l'efficacia dei sistemi di controllo interno della qualità e di gestione del rischio dell'impresa e, se applicabile, della revisione interna, per quanto attiene all'informativa finanziaria e, ove presente, alla rendicontazione individuale o consolidata di sostenibilità, senza violarne l'indipendenza (D.L. 39/2010 art. 19, c)).

Il Comitato supporta l'Organo di amministrazione (Cfr. Codice - Raccomandazione 33) nella: • valutazione circa l'opportunità di adottare misure per garantire l'efficacia e l'imparzialità di giudizio delle altre funzioni aziendali coinvolte nei controlli (quali le funzioni di risk management e di presidio del rischio legale e di non conformità), articolate in relazione a dimensione, settore, complessità e profilo di rischio dell'impresa • attribuzione all'organo di controllo o a un organismo appositamente costituito le funzioni di vigilanza ex art. 6, comma 1, lett. b) del Decreto Legislativo n. 231/2001.	**Rapporti con funzioni di controllo**	L'Organo di controllo: • controlla l'efficacia dei sistemi di controllo interno della qualità e di gestione del rischio dell'impresa e, se applicabile, della revisione interna, per quanto attiene all'informativa finanziaria e, ove presente, alla rendicontazione individuale o consolidata di sostenibilità, senza violarne l'indipendenza (D.L. 39/2010 art. 19, c)); • ai fini dello svolgimento dell'attività di vigilanza, acquisisce informazioni dall'organismo di vigilanza in merito al compito ad esso assegnato dalla legge di vigilare sul funzionamento e l'osservanza del modello ex D.lgs. n. 231/2001 e sul suo aggiornamento; • verifica che il modello preveda termini e modalità dello scambio informativo dell'Organismo di Vigilanza a favore dell'organo amministrativo e dello stesso organo di controllo. (Norme di comportamento per l'organo di controllo di società quotate).
Il Comitato supporta l'Organo di amministrazione (Cfr. raccomandazione 33) nella valutazione, sentito l'organo di controllo, dei risultati esposti dal revisore legale nella eventuale lettera di suggerimenti e nella relazione aggiuntiva indirizzata all'organo di controllo. Il Comitato, nel coadiuvare l'Organo di amministrazione • valuta, sentiti il dirigente preposto alla redazione dei documenti contabili societari, il revisore legale e l'organo di controllo, il corretto utilizzo dei princìpi contabili e, nel caso di gruppi, la loro omogeneità ai fini della redazione del bilancio consolidato; • valuta l'idoneità dell'informazione periodica, finanziaria e non finanziaria, a rappresentare correttamente il modello di business, le strategie della società, l'impatto della sua attività e le performance conseguite, coordinandosi con l'eventuale comitato previsto dalla raccomandazione 1, lett. a); • esamina il contenuto dell'informazione periodica a carattere non finanziario rilevante ai fini del sistema di controllo interno e di gestione dei rischi.	**Informativa societaria**	L'Organo di controllo: • esprime un parere sui risultati esposti dal revisore legale nella eventuale lettera di suggerimenti e nella relazione aggiuntiva (Codice di Corporate Governance Racc. 33 - f)); • vigila sull'adeguatezza dell'assetto organizzativo, amministrativo e contabile adottato dalla società sul suo concreto funzionamento (Art 2403 C.C.) • vigila sull'adeguatezza del sistema amministrativo - contabile nonché sull'affidabilità dello stesso nel rappresentare correttamente i fatti di gestione; (TUF /D.Lgs 24/2/98 n.58, Art. 149 -1.c)) • esprime il parere obbligatorio sulla nomina del dirigente preposto alla redazione dei documenti contabili societari (TUF /d.lg 24/2/98 n.58, Art. 154-bis) • monitora la revisione legale del bilancio d'esercizio e del bilancio consolidato e, ove presente, l'attività di attestazione della conformità della rendicontazione individuale o consolidata di sostenibilità, anche tenendo conto di eventuali risultati e conclusioni dei controlli di qualità svolti dalla Consob a norma dell'articolo 26, par. 6, del Regolamento europeo (Reg. UE n. 537/2014), ove disponibili (D.L. 39/2010 art. 19, d)); • fornisce una proposta motivata all'assemblea, in merito al conferimento e alla revoca dell'incarico di revisione legale e alla determinazione del corrispettivo (D.L. 39/2010 art. 13); • l'Organo di controllo e la società di revisione legale si scambiano tempestivamente i dati e le informazioni rilevanti per l'espletamento dei rispettivi compiti (TUF /d.lgs. 24/2/98 n.58, Art. 150 - c.3); • informa l'Organo di amministrazione dell'ente sottoposto a revisione dell'esito della revisione legale e, ove applicabile, dell'esito dell'attività di attestazione della rendicontazione di sostenibilità, e trasmette a tale organo la relazione aggiuntiva di cui all'articolo 11 del Regolamento europeo (Reg. UE n. 537/2014), corredata da eventuali osservazioni (D.L. 39/2010 art. 19, a)); • monitora il processo di informativa finanziaria e, ove applicabile, della rendicontazione individuale o consolidata di sostenibilità, compresi l'utilizzo del formato elettronico, e le procedure attuate dall'impresa ai fini del rispetto degli standard di rendicontazione di sostenibilità, nonché presenta le raccomandazioni o le proposte volte a garantirne l'integrità (D.L. 39/2010 art. 19, b)); • nell'ambito dello svolgimento delle funzioni ad esso attribuite dall'ordinamento, vigila sull'osservanza delle disposizioni in materia di informativa non finanziaria e ne riferisce nella relazione annuale all'assemblea (D.L. 125/2024 , art. 10 c.1); • fornisce parere circa la possibilità di omettere, in casi eccezionali, le informazioni concernenti sviluppi imminenti ed operazioni in corso di negoziazione, qualora la loro divulgazione possa compromettere gravemente la posizione commerciale dell'impresa (D.L. 125/2024 , art. 3 c.5, art.4 c.5).

Per una comprensione più completa delle attività dell'Organo di controllo (in aggiunta a quanto riportato in precedenza che si limita all'analisi sul coordinamento con il CCR) si suggerisce di fare riferimento, oltre alla normativa al riguardo e alle disposizioni Consob, alle linee guida pubblicate dal Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili citati in bibliografia.

APPENDICE 2 - Bibliografia e riferimenti sul tema

Riferimenti nazionali

Comitato Corporate Governance (2020), Codice di Corporate Governance, relative Q&A, relazione e lettera annuale

https://www.borsaitaliana.it/comitato-corporate-governance/homepage/homepage.htm

Siti web dei promotori del Codice di Corporate Governance

ABI: www.abi.it

ANIA: www.ania.it

Assogestioni: www.assogestioni.it

Assonime: www.assonime.it

Borsa Italiana S.p.A.: www.borsaitaliana.it

Confindustria: www.confindustria.it

Consob https://www.consob.it/web/area-pubblica/governo-societario

Banca d'Italia …

IVASS …

CNDCEC - Consiglio Nazionale dei Dottori Commercialisti ed Esperti Contabili

https://commercialisti.it/norme-di-comportamento-del-collegio-sindacale-verbali-e-procedure

AIIA - Associazione Italiana Internal Auditors - https://www.aiiaweb.it/knowledge-center

2021 - *L'Overall Opinion come strumento di comunicazione strategica per le organizzazioni.*

2021 - *La Governance aziendale alla prova dell'emergenza*

2020 - *Agile Reporting*

2020 - *L'Evoluzione della Funzione IA: da assurance ispettiva a assurance positiva*

AODV 231 - Associazione dei Componenti degli Organismi di Vigilanza AODV 231 – vari position papers https://www.aodv231.it/

ASSONIME

2022 - *Il caso Impregilo: luci e ombra sulla questione Giustizia* - caso Assonime 4/2022

Alcuni studi di sintesi ed esempi

AIFIRM (2020), **Governance e strategia per la gestione dei rischi nelle imprese non finanziarie,** Associazione Italiana Financial Industry Risk Managers, position paper 24

https://www.aifirm.it/wp-content/uploads/2020/11/2020-Position-Paper-24-Governance-e-RM-imprese-corporate.pdf

Nedcommunity - position papers **Reflection Group "La governance in tema di rischi e controlli"**

https://www.nedcommunity.com/pubblicazioni/pubblicazioni-sulla-corporate-governance-rg/

Nedcommunity (2020), Evoluzione della risk governance in chiave strategica

Nedcommunity-KPMG (2020), Informativa extra finanziaria: da compliance a governance strategica

Nedcommunity-PWC (2017), La riforma della revisione

Nedcommunity (2015), Risk governance e obiettivi strategici d'impresa

Nedcommunity (2013), Come valutare la governance in tema di rischi e controlli

Nedcommunity (2023), LUISS School of Law con Nedcommunity, La Governance delle società: i comitati endoconsiliari tra informazione e responsabilità

Nedcommunity (2024), WP Politiche di remunerazione ed engagement di executives e dipendenti a sostegno della transizione climatica

EcoDa (2020), *Cyber-risk oversight*

https://ecoda.org/wp-content/uploads/2019/08/2020-ecoDa-ISA-AIG-Handbook-on-Cybersecurity-summary-v3-2.pdf

Chapter Zero – The Nedcommunity Climate Change Directors' Forum

https://www.nedcommunity.com/chapter-zero-modelli-sostenibili-governo-societario/

Banca Centrale Europea (2020), *Guida sui rischi climatici e ambientali. Aspettative di vigilanza in materia di gestione dei rischi e informativa*

Banca d'Italia (2022), *Aspettative di vigilanza sui rischi climatici e ambientali*

Banca d'Italia (2022), *Orientamenti della Banca d'Italia sulla composizione e sul funzionamento dei consigli di amministrazione delle LSI*

European Bank Authority (2024), *Draft Guidelines on the management of ESG risks – Consultation Paper*

European Bank Authority (2021), *Final Report on Guidelines on internal governance under Directive 2013/36/EU*

WEF (2019), *How to Set Up Effective Climate Governance on Corporate Boards*

WEF (2020), *Toward Common Metrics and Consistent Reporting of Sustainable Value Creation*

Rivista Sistema Penale, R. Blaiotta (2021), *L'organismo di vigilanza: struttura, funzione e responsabilità*

Rivista Sistema Penale, C. Piergallini (2022), *Una sentenza modello della Cassazione pone fine all'estenuante vicenda "Impregilo"*

Gazzetta ufficiale dell'Unione europea (2019), *Orientamenti sulla comunicazione di informazioni di carattere non finanziario: Integrazione concernente la comunicazione di informazioni relative al clima*

Leading practice internazionali

UK Corporate Governance Code

UK Corporate Governance Code (frc.org.uk)

Corporate Governance Code Guidance (frc.org.uk)

COSO (2004, 2013, 2017, Thoughts papers) https://www.coso.org/Pages/default.aspx

Frameworks

1992 - updated in 2013 - Internal Controls - Integrated Framework

2004 - Enterprise Risk Management - Integrated Framework

2017 - Enterprise Risk Management - Integrating with Strategy and Performance

Thoughts papers (selezione)

2018 - Applying enterprise risk management to Environmental, Social and Governance-related risks

2019 - Managing cyber risk in a digital age

2020 - Risk appetite critical to success - using risk appetite to thrive in a changing world

2020 - Compliance risk management: applying the COSO ERM framework

2023 - Achieving Effective Internal Control of Sustainability Reporting (ICSR)

G20/OECD Principles of Corporate Governance

OECD (2023), *G20/OECD Principles of Corporate Governance*, OECD Publishing, Paris,

G20/OECD Principles of Corporate Governance 2023 | OECD

OECD (2014), Risk Management and Corporate Governance, Corporate Governance, OECD Publishing. http://dx.doi.org/10.1787/9789264208636-en

IIA (Institute of Internal Auditors – and member of COSO)

https://na.theiia.org/Pages/IIAHome.aspx

2020 - Developing a Risk-based Internal Audit Plan

2020 - The IIA's three lines model - an update of the three lines of defense

2024 - Global Internal Audit Standards

Complete Global Internal Audit Standards (theiia.org)

ECIIA - European Confederation of Institutes of Internal Auditing) - https://www.eciia.eu/

2020 - Practical Guidance on climate change and environmental sustainability How to tackle associated risks and harness opportunities? 2020

2020 - Practical Guidance on Cybersecurity and Data Security

2024 - Risk in Focus 2025: Hot topics for internal auditors

2024 - DORA 2024 – Internal Audit's Role and Strategies Ahead of Compliance Deadline

2024 - New Guide on ESG governance: six ways for boards to lead the sustainability transition

ISO (2018), ISO 31000: Risk Management - Guidelines https://www.iso.org/standard/65694.html

FSB (2014), Guidance on Supervisory Interaction with Financial Institutions on Risk Culture: A Framework for Assessing Risk Culture https://www.fsb.org/2014/04/140407/

*Il presente documento, comprensivo di testi, dati, analisi, grafici e qualsiasi altro contenuto in esso incluso, è di proprietà congiunta di **Nedcommunity** - associazione italiana di amministratori non esecutivi e indipendenti e della società **KPMG Advisory S.p.A.** (di seguito, congiuntamente, i "Titolari").*

Tutti i diritti relativi al presente lavoro sono riservati ai Titolari. È consentita la citazione di parti del documento a fini scientifici, accademici o informativi, purché ne venga chiaramente indicata la fonte con i seguenti riferimenti:

- ***Titolo del paper:*** *Il Comitato Controllo e Rischi: ruolo, funzioni e agenda per un'efficace governance*
- ***Autori:*** Il *Reflection Group (Graziella Capellini, Rosalba Casiraghi, Diana D'Alterio, Carolyn Dittmeier - coordinatrice, Patrizia Giangualano - coordinatrice, Leonardo Scimmi) e i membri del team KPMG Advisory S.p.A. (Jennifer Altmeyer Cucolo, Aldo Cinquegrana, Antonio Mansi, Alessandra Rizzo, Nicolò Zanghi)*
- ***Nome dei Titolari*** *(Nedcommunity - associazione italiana di amministratori non esecutivi e indipendenti - e KPMG Advisory S.p.A.)*
- ***Anno di pubblicazione:*** *2025*

Qualsiasi utilizzo diverso dalla mera citazione, inclusa ma non limitata la riproduzione integrale, modifica, distribuzione, pubblicazione, commercializzazione o altro sfruttamento del presente documento o di sue parti, è espressamente vietato senza il previo consenso scritto congiunto dei legali rappresentanti di Nedcommunity e KPMG Advisory S.p.A.

I Titolari si riservano ogni diritto non espressamente concesso dal presente disclaimer.

© 2025 KPMG Advisory S.p.A. è una società per azioni di diritto italiano e fa parte del network KPMG di entità indipendenti affiliate a KPMG International Limited, società di diritto inglese. Tutti i diritti riservati.