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

9 Maggio 2021

Il presente documento è stato realizzato da Nedcommunity
nell'ambito del "Reflection Group - La governance in materia di rischi e di controlli"[1].

[1] Si ringrazia il Gruppo di Lavoro: Graziella Capellini, Cesare Conti, Silvia Stefini per il contributo alla stesura del presente documento, e tutti i membri del Reflection Group (composto da: Carolyn Dittmeier - coordinatrice, Patrizia Giangualano - coordinatrice, Diana D'Alterio, Livia Aliberti Amidani, Giampiero Bambagioni, Enrico Maria Bignami, Graziella Capellini, Rosalba Casiraghi, Cesare Conti, Maria Luisa Di Battista, Giovanni Maria Garegnani, Gaudiana Giusti, Elisabetta Magistretti, Paola Schwizer, Leonardo Scimmi, Silvia Stefini) per le osservazioni e i suggerimenti.

Indice

Premessa: evoluzione del contesto di riferimento pag 1

1. Il ruolo del Comitato Controllo e Rischi nella governance della società pag 2
    a. Il Comitato Controllo e Rischi nei Modelli di Best Practice internazionali
    b. Composizione e funzionamento del CCR
    c. Composizione e funzionamento del CCR in ambito bancario

2. Le funzioni del Comitato Controllo e Rischi pag 7
    a. Aspetti di governance
    b. SCIGR: Risk framework
    c. SCIGR: Gestione dei rischi
    d. SCIGR: Internal auditing e altre funzioni di controllo
    e. Supporto alla pianificazione strategica
    f. Reporting finanziario e non finanziario

3. L'agenda del Comitato Controllo e Rischi pag 23

Appendice 1: Confronto tra Comitato Controllo e Rischi e Organo di Controllo pag 26

Appendice 2: Bibliografia e riferimenti sul tema pag 32

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 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 best practice internazionali (tra i principali, il framework del COSO[2], i principi internazionali stabiliti dal G20/OCSE[3], gli standard definiti dall'ISO[4] e dal Financial Stability Board[5]).

I seguenti tre principi chiave accomunano i riferimenti normativi e le best 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 non finanziari e una gestione dei rischi in ottica di sostenibilità 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 membri del Comitato Controllo e Rischi (di seguito "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 prima pubblicazione del 2016) tiene conto delle più recenti evoluzioni sia normative che di best 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), le indicazioni della Banca Centrale Europea e della European Banking Authority[6] mentre tra le best practice il COSO Framework che ha pubblicato nel 2017 l'aggiornamento *Enterprise Risk Management - Integrating with strategy and performance* e nel 2018 il paper *Applying enterprise risk management to Environmental, Social and Governance-related risks*.

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.

Il presente documento si articola in tre capitoli e in due Appendici. Il primo capitolo si sofferma sul ruolo del CCR nella governance aziendale. Il secondo riporta le principali funzioni del CCR sintetizzate in una tabella e poi commentate nelle relative note esplicative. Il terzo riporta una proposta di massima di agenda delle attività e la loro tempistica, che dovrà essere adattata ad ogni specifica realtà in considerazione della sua operatività, complessità e dimensione. Seguono due Appendici, che propongono, rispettivamente, un confronto tra i compiti del CCR e dell'Organo di Controllo, inteso anche a promuovere l'attivazione di potenziali sinergie, e una bibliografia con riferimenti per ulteriori approfondimenti.

---

[2] Committee of Sponsoring Organizations of the Treadway Commission (COSO) 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 prinicipi di Corporate Governance dell'OECD sono stati sottoscritti dal G20 nel 2015

[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 2020Gli "Orientamenti EBA" pubblicati dall'*European Banking Autority* (EBA) il 29 maggio 2020

1. Il ruolo del Comitato Controllo e Rischi nella governance della società

Il Codice di Corporate Governance delle Società Quotate alla Borsa Italiana[7] (gennaio 2020) – (di seguito il "Codice") – in linea con le best 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.

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 cerca di ridurre l'impatto sull'ambiente dovuto al cambiamento climatico. Questo concetto era già presente nel Codice di Autodisciplina del 2018, dove si parlava di "sostenibilità nel medio-lungo periodo dell'emittente", ma è ulteriormente sviluppato nel Codice del 2020 che richiama tutto l'Organo di Amministrazione e tutti i Comitati endoconsiliari a fare del successo sostenibile l'obiettivo che guida le scelte e i comportamenti. Si tratta quindi di un passaggio ulteriore rispetto al Codice di Autodisciplina del 2018, che incoraggiava le società appartenenti al FTSE MIB a costituire un Comitato dedicato alla sostenibilità[8]. Il nuovo 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*[9]*"*.

La nuova visione del Codice promuove un approccio più strategico al 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 (di seguito "SCIGR") è uno dei mezzi per perseguire l'obiettivo di gestione del rischio. In questa logica, il **"SCIGR" viene ridefinito "*insieme delle regole, procedure e strutture organizzative finalizzate a una effettiva e efficace identificazione, misurazione, e monitoraggio dei principali rischi, al fine di contribuire al successo sostenibile della società*"**. Il SCIGR coinvolge più entità e il management[10], ma l'Organo di Amministrazione ha la responsabilità ultima in quanto definisce le linee guida del sistema e ne valuta l'adeguatezza e l'efficacia complessiva, vigilando in particolare sul coordinamento tra i soggetti coinvolti e sull'efficacia dei flussi informativi, con lo specifico 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"[11].

Un altro elemento di novità del Codice è l'attenzione verso il rigore metodologico dell'informativa non finanziaria e l'assegnazione al CCR della valutazione dell'idoneità di tale informativa (in aggiunta a quella finanziaria) e dell'esame del suo contenuto in relazione al "SCIGR"

---

[7] Comitato Corporate Governance (2020)

[8] Nel Codice di Autodisciplina 2018 si suggerisce: "Nelle società appartenenti all'indice FTSE-Mib, il consiglio di amministrazione valuta l'opportunità di costituire un apposito comitato dedicato alla supervisione delle questioni di sostenibilità connesse all'esercizio dell'attività dell'impresa e alle sue dinamiche di interazione con tutti gli stakeholder". Mentre nel Codice 2020, la Raccomandazione 1 a) fa riferimento a un eventuale Comitato che si dedica "all'analisi dei temi rilevanti per la generazione di valore nel lungo termine"

[9] Raccomandazione 1 c) del Codice

[10] La Raccomandazione 32 del Codice indica gli organi coinvolti nel controllo: l'Organo di Amministrazione, il CCR, l'organo di controllo, l'organismo di vigilanza, l'internal audit, le funzioni di controllo di secondo livello.

[11] Principio XX del Codice.

Questo aspetto amplia l'agenda del CCR e richiede attenzione alle modalità di attuazione del Decreto Legislativo 254/2016 sulla reportistica non finanziaria, in particolare in relazione al processo che porta alla formazione dei dati e alla rispondenza agli standard di rendicontazione non finanziaria internazionali, anche quando il presidio sulla struttura e sul contenuto di tale reportistica sia affidato ad un altro Comitato. Il Codice promuove quindi l'integrazione delle attività di controllo volte a verificare la correttezza del processo di formazione dell'informativa societaria.

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 finanziarie e non finanziarie periodiche.

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[12] 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 inerente 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.

1.a Il Comitato Controllo e Rischi nei Modelli di Best Practice internazionali

Il Codice del 2020 è allineato con l'evoluzione delle best practice internazionali che portano in evidenza l'importanza di un approccio integrato di analisi del rischio con la strategia e con i fattori non finanziari, tenendo conto di un ampio gruppo di *stakeholder*. In particolare, i modelli di best 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 best practice nazionale o internazionale usare, ma richiede di fare riferimento esplicito a quale scelta sia stata compiuta.

Il modello di best 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: quelle relative al controllo interno (*Internal Controls*, del 1992 aggiornato nel 2013) e quelle relative alla gestione del rischio (*Enterprise Risk Management*, del 2004 aggiornato nel 2017 con ulteriori approfondimenti su temi specifici emergenti attraverso i *thought papers*). I diversi framework del COSO possono essere integrati o applicati singolarmente. La Relazione sul Governo Societario deve indicare a quale specifico framework si faccia riferimento.

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: l'integrazione dell'ERM con il business model e la generazione di valore; l'importanza di catturare segnali di rischio in una fase preliminare e di avere meccanismi per prendere decisioni in situazioni di grande incertezza; 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

[12] 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 best practice vengono dai singoli componenti del Comitato per la Corporate Governance – Borsa Italiana S.p.A, ABI, ANIA, Assonime, Confindustria, Assogestioni.

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.*

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

TEMI PRINCIPALI APPROFONDITI DALLE "BEST PRACTICE" INTERNAZIONALI[13]

Le best 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 e di cultura aziendale.

Il Comitato deve avere la sensibilità di valutare e promuovere la cultura del rischio integrato nell'organizzazione (*enterprise risk management culture*), il coinvolgimento del CEO e del senior management (*tone from the top*), la chiarezza nella definizione delle responsabilità (*accountability*), la valorizzazione del capitale umano nei ruoli chiave di controllo e risk management (*attracts, develops, and retains capable individuals*), la coerenza tra i valori aziendali, la strategia e il sistema di controllo e gestione dei rischi (*demonstrates commitment to core values*).

Le best practice suggeriscono inoltre modalità per integrare risk management e discussioni di strategia e sostenibilità, oltre a fornire strumenti per l'Organo di Amministrazione (ad esempio: la *Heat map* o il *Risk Appetite Framework*, "RAF")

1.b Composizione e funzionamento 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"[14]

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 all'Appendice 1.

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

[13] Si veda la bibliografia essenziale nell'appendice 3. 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.
[14] Raccomandazione 35 del Codice

istruttoria da parte del Comitato su alcuni aspetti di controllo o gestione dei rischi.[15] È opportuno un intervento del CEO in CCR almeno una volta l'anno in occasione della valutazione da parte del CCR dell'adeguatezza del SCIGR, in virtù del ruolo del CEO definito dalla Raccomandazione 34 b del Codice[16]. 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 non finanziaria; 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**.

1.c Composizione e funzionamento del CCR in ambito bancario

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. Prerogative e funzioni del CCR relative al controllo dei rischi in ambito bancario 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). Si cita in particolare la Circolare Banca d'Italia 285 del 17 dicembre 2013 "Disposizioni di Vigilanza per le Banche".

DISPOSIZIONI SUL COMITATO CONTROLLO E RISCHI PER LE BANCHE[17]

1. 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;

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

I membri 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 comitato rischi 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 comitato 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.

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

[16] 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*"

[17] Circolare Banca d'Italia. 285 – Parte prima, Titolo IV, Capitolo 1, Sezione IV

Tra le recenti innovazioni normative e regolamentari di maggiore rilevanza per il sistema bancario che ricomprendono una specifica attenzione in tema di rischi, sostenibilità e fattori ESG, 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")[18] e la "Guida sui rischi climatici e ambientali" per le banche pubblicata dalla Banca Centrale Europea (BCE)[19], 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*».

Si ricorda inoltre che nel decreto Ministero dell'Economia e delle Finanze n. 169, del 23 novembre 2020[20] 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).

[18] 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.

[19] 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.

[20] 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».

2. Le funzioni del Comitato Controllo e Rischi

Le attività del CCR sono di seguito schematizzate in una **TABELLA** che si propone di sintetizzare gli ambiti in cui assume rilievo il parere o il contributo del CCR. Si evidenziano in tale quadro anche le aree di necessario coordinamento e collegamento del CCR con gli altri comitati endoconsiliari (es. Comitato Nomine, Comitato Remunerazioni, Comitato Sostenibilità o altro).

La Tabella è articolata nelle seguenti sezioni:

a. **Aspetti di governance**
b. **SCIGR: Risk framework**
c. **SCIGR: Gestione dei rischi**
d. **SCIGR: Internal auditing e altre funzioni di controllo**
e. **Supporto alla pianificazione strategica**
f. **Reporting finanziario e non finanziario**

La Tabella evidenzia argomenti previsti in modo esplicito dal Codice di Corporate Governance e altri aspetti interpretativi forniti nella più diffusa best practice internazionale. La simbologia riportata nella seguente legenda aiuta a distinguere le parti desunte dal Codice da quelle tratte da una selezione di alcune best practice internazionali.

LEGENDA
➢ **Argomenti previsti in modo esplicito dal Codice di Corporate Governance** (e riferimenti alle principali norme del sistema legislativo italiano)
❖ **Alcuni ulteriori e rilevanti aspetti evidenziati da altre best practice internazionali** (si riportano a titolo di esempio soprattutto indicazioni del COSO 2017, non previste dal sistema legislativo italiano o dal Codice, che richiede solo di citare nella Relazione sul Governo Societario quali best practice vengono seguite)

La Tabella indica altresì, in una colonna separata per ogni ambito trattato, le principali responsabilità aggiuntive previste dalla normativa di settore in capo al **CCR nelle aziende del settore finanziario**.

All'interno della Tabella vi è un riferimento a **NOTE ESPLICATIVE,** che approfondiscono o chiariscono alcuni aspetti 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.**

a. Aspetti di governance	
Indicazioni tratte dal Codice di Corporate Governance e dalla best practice	**Disposizioni per il Settore Finanziario** (non esaustive)
➢ **Supporto all'Organo di Amministrazione nella:** • **definizione del sistema di governo societario (1, 2)** • **definizione delle linee di indirizzo SCIGR e valutazione della sua adeguatezza ed efficacia** • **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 best practice nazionali e internazionali di riferimento** • **attribuzione all'Organo di Controllo o ad un organismo appositamente costituito le funzioni di vigilanza ex d.lgs 231/01, compresa una argomentazione delle scelte eventualmente effettuate sulla composizione dell'OdV** ➢ **Predisposizione e presentazione all'Organo di Amministrazione, almeno in occasione delle relazioni finanziarie annuale e semestrale, di una relazione in cui il CCR riferisce dell'attività svolta nonché dell'adeguatezza (rispetto alle caratteristiche e al profilo di rischio dell'impresa) e dell'efficacia del SCIGR (2)** ➢ **Coordinamento e sinergie con** • **L'Organo di Controllo[21] (si veda Appendice 1)** • **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 comportamenti rischiosi	• Supporta l'Organo di Amministrazione nella definizione e approvazione degli indirizzi strategici e delle politiche di governo dei rischi. • 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; 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

[21] 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 Organo di controllo è deputato a controllare anche l'attività del CCR, e non viceversa.

b. SCIGR: Risk framework

Indicazioni tratte dal Codice di Corporate Governance e dalla best practice	Disposizioni per il Settore Finanziario (non esaustive)
➢ **Supporto all'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 best practice nazionali o internazionali** • **efficace progettazione e disegno del SCIGR in conformità con il modello indicato (3)** ❖ Esame sempre in ottica di sintesi della matrice dei rischi in ottica integrata (4): • utilizzando parametri di impatto e probabilità • includendo un'ottica di lungo periodo e eventuali impatti non economici • evidenziando gli aspetti ESG nei rischi esistenti o nuovi rischi dovuti a tematiche ESG (5) • riservando particolare attenzione ai rischi trasversali - pro tempore - emergenti, quali attualmente il cyber risk, i rischi reputazionali, i rischi geopolitici così come i rischi connessi al cambiamento climatico, alla pandemia e alla digital transformation (6); ❖ Eventuale sviluppo di un *Risk Appetite Framework* (7) per la definizione del rischio massimo approvato dall'Organo di Amministrazione 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) ❖ Esame del modello utilizzato per il sistema di controllo volto all'integrità dell'informativa finanziaria e non finanziaria – ad esempio il COSO Framework 2013 (8)	• Con riferimento alla solvibilità, supporta l'Organo di Amministrazione nella definizione del sistema degli obiettivi di rischio, definendo, sulla base delle valutazioni rilevanti, ivi inclusa la valutazione interna del rischio e della solvibilità, 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 • Con riferimento al processo ICAAP/ILAAP, 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 dell'ICAAP/ILAAP a fini strategici e nelle decisioni d'impresa; Esame delle principali politiche aziendali da sottoporre all'approvazione dell'Organo di Amministrazione • Attività valutativa e propositiva necessaria affinché l'Organo di Amministrazione, possa definire e approvare gli obiettivi di rischio ("*Risk appetite*") e la soglia di tolleranza ("*Risk tolerance*")

c. Gestione dei rischi

Indicazioni tratte dal Codice di Corporate Governance e dalla best practice	Disposizioni per il Settore Finanziario (non esaustive)
➢ **Supporto all'Organo di Amministrazione nelle valutazioni relative alla gestione dei rischi derivanti da fatti pregiudizievoli** ➢ **Espressione di pareri su specifici aspetti inerenti all'identificazione dei rischi** ➢ **Valutazione dell'effettiva implementazione del risk framework** ➢ **Valutazione dell'adeguatezza dell'assetto organizzativo, amministrativo e contabile della società e delle controllate aventi rilevanza strategica, con particolare riferimento al SCIGR (1,2)** ❖ Valutazione del periodico aggiornamento della matrice dei rischi, della loro evoluzione e dell'impatto sul business ❖ Valutazione dei piani di mitigazione per la gestione dei rischi e il controllo del livello di accettabilità dei rischi ❖ Promozione di un periodico brainstorming sui rischi inusuali o sconosciuti o emergenti. ❖ Verifica che siano definiti i limiti di rischio accettabili e che questi limiti siano utilizzati nei processi aziendali rilevanti. Valutazione sull'utilizzo del RAF e del RAS (7) ❖ Monitoraggio dell'efficacia del piano di business continuity e di crisis management (9) ❖ Valutazione della cultura aziendale in tema di *risk management* attraverso l'analisi dell'ambiente di controllo e l'ambiente interno in generale (10) ❖ Verifica della presenza delle competenze necessarie a progettare e implementare efficacemente il SCIGR; ❖ Analisi e valutazione delle principali politiche aziendali collegate con il SCIGR, anche in ottica di accountability, deleghe di poteri e segregazione dei ruoli (11) ❖ 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) ❖ Approfondimento sui sistemi di controllo a fronte dei rischi valutati significativi (12). Si veda la sezione successiva	• Supporto all'OFSS (Organo con Funzione di Supervisione Strategica) nella verifica della corretta attuazione delle strategie, delle politiche di governo dei rischi e del RAF • Esame informativa periodica sui rischi dell'attività bancaria e sui loro impatti sui coefficienti patrimoniali e di liquidità (risk adjusted capital/solvency ratio) • Esame Resoconto ICAAP *(Internal Control Adequacy Assessment Process)* e ILAAP *(Internal Liquidity Adequacy Assessment Process)*

d. SCIGR: Internal auditing e altre funzioni di controllo

Indicazioni tratte dal Codice di Corporate Governance e dalla best practice	Disposizioni per il Settore Finanziario (non esaustive)
➢ **Supporto all'Organo di Amministrazione:** • **nomina e revoca del responsabile della funzione di internal auditing, definendo la sua remunerazione, assicurando l'adeguatezza di risorse** • **approvazione del piano di lavoro di internal auditing (13) sentito l'organo di controllo e il CEO** • **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** • **costituzione organismo di vigilanza ai sensi del D.Lgs. 231/2001**	• Individuazione e proposta 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 • Esame del piano di attività e delle relazioni periodiche delle funzioni di controllo, oltre a quelle di particolare rilevanza, indirizzate all'Organo di Amministrazione • Valutazioni e 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;
➢ **Richiesta all'internal audit di svolgere verifiche su specifiche aree operative**	• Valutazioni e pareri in merito alla politica aziendale di esternalizzazione di funzioni aziendali di controllo;
➢ **Monitoraggio di autonomia, adeguatezza, efficacia ed efficienza della funzione di internal audit (14)**	• Supporto all'Organo di Amministrazione in merito alla predisposizione del documento di coordinamento delle funzioni e organi di controllo
➢ **Analisi delle relazioni periodiche e quelle di particolare rilevanza predisposte dalla funzione di internal auditing (14)**	
❖ Analisi delle relazioni periodiche predisposte dalle altre funzioni di controllo di secondo livello (Dirigente Preposto, Ufficio Legale, Conformità, Risk Manager, ecc.) e dall'Organismo di Vigilanza	
❖ Verifica della separazione e della indipendenza tra i controlli di secondo livello (risk management, compliance, ecc) e terzo livello (internal audit); Valutazione perimetro delle funzioni di secondo livello; Valutazione dell'efficace ed efficiente sistema di flussi informativi nelle tre Linee di Difesa	
❖ 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" (15)	

e. Supporto alla pianificazione strategica

Indicazioni tratte dal Codice di Corporate Governance e dalla best practice	Disposizioni per il Settore Finanziario (non esaustive)
➢ **L'organo di amministrazione, con il supporto del CCR, definisce le linee di indirizzo 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 ❖ Valutazione del processo di pianificazione strategica nella prospettiva del SCIGR (16): - Adeguata rilevazione e misurazione dei rischi aziendali nel periodo di pianificazione strategica (di mercato, regolatori, esogeni) - Identificazione di misure per gestire i rischi ❖ Formulazione di 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 (16) - Coerenza tra obiettivi strategici, rischi aziendali e sostenibilità a lungo termine dell'azienda - Identificazione di opportunità conseguenti a cambiamenti di scenario o rischi emergenti ❖ Verifica della integrazione tra pianificazione strategica, tematiche ESG e processo di ERM, inclusi: - Impatto dei cambiamenti climatici e azioni da intraprendere (17) - Evoluzione della governance aziendale per far fronte al cambiamento strategico (16)	• Supporta l'Organo di Amministrazione nella definizione e approvazione degli indirizzi strategici

f. Reporting finanziario e non finanziario

Indicazioni tratte dal Codice di Corporate Governance e dalla best practice	Disposizioni per il Settore Finanziario (non esaustive)
➢ **Supporto all'Organo di Amministrazione nell'esame della relazione finanziaria e non finanziaria (riferimento Legge 262/2005 e D.Lgs 254/2016)** ➢ **Valutazione dell'idoneità dell'informazione periodica, finanziaria e non finanziaria, a rappresentare il modello di business, le strategie e le performance (18)** ➢ **Analisi del contenuto dell'informazione periodica a carattere non finanziario rilevante ai fini del SCIGR (18)** ➢ **Supporto all'Organo di Amministrazione nella valutazione dei risultati esposti dal revisore nella eventuale lettera di suggerimenti e nella relazione aggiuntiva** ➢ **Valutazione (sentiti il dirigente preposto, il revisore e l'organo di controllo) sul corretto utilizzo dei princìpi contabili** ❖ 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 ❖ Analisi dell'adeguatezza della comunicazione relativa all'impatto dei rischi principali sulla performance attraverso l'informativa finanziaria e non finanziaria	• Valutazione del 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. • Supporto 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

NOTE ESPLICATIVE

1. L'analisi del modello di governance complessivo da parte del CCR si può basare sul modello delle best practice di riferimento (COSO 2013, COSO 2017, FSB 2014, ISO31000 ecc.) 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. Si veda per maggiore dettaglio il paper Nedcommunity (2013), *Come valutare la governance in tema di rischi e controlli*.

2. **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 nelle sezioni 2,3,4 della Tabella. 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 (nell'ambito del suo ruolo in relazione al SCIGR definito dalla Raccomandazione 34 b del Codice) 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 dal revisore legale 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. La valutazione dovrà inoltre comprendere gli esiti dell'analisi dell'ambiente di controllo e dell'ambiente interno trattato nel successivo punto 10. Il parere può essere espresso in base alle politiche adottate sia in forma di *positive assurance* (cioè l'esplicita conferma che il SCIGR è adeguato) o di *negative assurance* (cioè la conferma che il SCIGR è 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). 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.*

3. Definizione del profilo di rischio e disegno del risk framework. Il Codice richiede all'Organo di Amministrazione di definire il profilo di rischio compatibile con la strategia e validare i rischi significativi almeno annualmente 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 rischio, facendo riferimento alle best practice nazionali o internazionali. Il CCR supporta l'Organo di Amministrazione nel promuovere lo sviluppo di un risk framework adeguato. Il risk framework deve 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 "ERM"). Quando tale funzione è presente, il CCR incontra trimestralmente tale funzione, discute l'analisi svolta, valuta l'adeguatezza del modello e la capacità di risposta ai rischi (si veda anche la sezione 3 della Tabella).

4. La 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. 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. Con riguardo ai criteri utilizzati per costruire la matrice, le best 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 frequenza 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) .

5. Integrazione tra ESG e ERM. L'integrazione tra ESG e ERM si attua modificando l'approccio al risk management al fine di introdurre anche la valutazione dei fattori ESG. 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 (per la metodologia, si veda ad esempio il paper COSO (2018) "*Applying ERM to ESG-related risks*".

6. Alcuni rischi emergenti: cyber risk, digital transformation e rischi reputazionali. 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*.

7. Il Risk Appetite Framework (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 importante per l'Organo di Amministrazione per definire il profilo di rischio entro cui il management opera in autonomia. Il *risk appetite è* approvato dall'Organo di Amministrazione, declinato nei KPI/KRI riconducibili ai vari livelli dell'organizzazione e ai diversi stakeholder dell'azienda, costituisce un riferimento nella selezione delle strategie, nelle decisioni di investimento e nelle operazioni di finanza straordinaria (acquisizioni, rifinanziamenti, ristrutturazioni finanziarie, …). Oltre alle best practice, si rinvia al paper AIFIRM (2020) *Governance e strategia per gestione dei rischi nelle imprese non finanziarie*, da pagina 33 a pagina 40.

8. Il modello di best practice per il Controllo Interno più diffuso è il COSO Framework (2013) *Internal Controls* – Integrated Framework, emesso dal Committee of Sponsoring Organizations of the Treadway Commission negli Stati Uniti nel 1992 e aggiornato nel 2013. Il COSO Framework (2013) ha costituito, in tutti questi anni, il modello di riferimento più importante sia per le autorità di vigilanza (standard setter) sia per le imprese. Tra i vari ambiti di applicazione del COSO Framework, senza dubbio quello relativo al sistema di controllo interno sull'informativa finanziaria è uno tra i più noti e diffusi a livello internazionale. Più recentemente, l'affermazione delle tematiche di sostenibilità nell'ambito della corporate governance e l'obbligo per alcuni enti di interesse pubblico (che rientrano nei limiti definiti dalla legge) di dare disclosure sull'informativa non finanziaria (cfr. Direttiva 2014/95/UE attuata in Italia con il D.Lgs. 254/16) 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). Al fine di assicurare, anche in questo ambito, l'affidabilità delle informazioni non finanziarie 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. D'altra parte 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. Il COSO Framework (2013) coglie e tratta tutti gli elementi che caratterizzano l'attuale scenario di rischio. L'approccio olistico e integrato di tutte le componenti del Sistema di Controllo Interno, ancorché riorganizzato per principi e punti di attenzione (principles based approach), presenta un certo livello di complessità, in fase di applicazione, derivante soprattutto dalla scalabilità delle soluzioni proposte al contesto e alle dimensioni dell'impresa. 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; attendibilità delle informazioni (interne ed esterne, finanziarie e non finanziarie); 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.

9. Il 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 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 Comitato 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 Comitato 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 Mangement* 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 Rischi su *Key Indicators*, oltre che sessioni dedicate su particolari argomenti. Inoltre il Comitato Rischi, in caso di crisi, dovrebbe verificare la presenza di un adeguato processo di gestione della comunicazione nei confronti di tutti gli *stakeholder*

10. La valutazione dell'ambiente di controllo e dell'ambiente interno. L'ambiente di controllo rappresenta uno dei componenti del COSO Framework (2013) *Internal Controls – 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 (SCIGR) delle organizzazioni. Il Consiglio 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 al Consiglio 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 (trattato anche nel successivo punto 11);
- 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 e 20 punti di attenzione, il cui disegno e la cui operatività sono il presupposto per la valutazione dell'adeguatezza dell'intera componente.

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 l'aggiornamento del framework attraverso la pubblicazione del COSO Framework ERM (2017) **l'ambiente interno** evolve 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. Comprende anche aspetti organizzativi che sono brevemente ricompresi nel punto successivo

11. La valutazione dell'assetto organizzativo 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*).

12. Approfondimenti sui sistemi di controllo a fronte dei rischi valutati significativi

Il Comitato 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 compliance/governance
- Gestione finanziaria

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.

13. Parere sul Piano della Funzione di Internal Audit: il CCR può prendere in esame: la proposta di piano annuale e pluriennale di Internal Audit; il piano di verifiche rilevanti 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; i criteri di copertura audit di medio termine. Secondo la best practice espressa dall'Institute of Internal Auditors (di seguito "IIA"), ci si aspetta che il piano sia *risk-based* (Si rinvia alla practical guidance dell'IIA 2020, *Developing a Risk-based Internal Audit Plan)* 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.

14. Valutazione della funzione di Internal Audit e delle sue relazioni periodiche: L'analisi delle relazioni periodiche include anche il monitoraggio delle attività di follow up dei piani di rimedio e di situazioni di criticità non ancora risolte. Per quanto riguarda il monitoraggio della funzione**,** gli aspetti oggetto di esame da parte del Comitato possono comprendere: la Quality Assurance Review (QAR) esterna e Quality Assurance Improvement Program (QAIP) interna richiesta dagli standard professionali (la valutazione esterna è richiesta ogni cinque anni e fornisce, tra l'altro, un parere sul livello di

conformità della funzione al framework di standard professionali internazionali IIA[22]); il mandato della funzione di Audit; la linea di reporting gerarchico e funzionale e l'indipendenza in generale, valutata anche in termini di anzianità nella posizione; le risorse, le competenze, i titoli professionali e le certificazioni degli Auditor; il dimensionamento delle risorse; la effettiva messa a disposizione del budget; 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; il 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. Il Comitato dovrebbe svolgere 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.

15. Altri documenti e politiche oggetto di valutazione da parte del CCR: Si citano ad esempio: 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.). Il CCR può esaminare tutti gli aspetti sostanziali del sistema GRC "Governance – Risk Management – Compliance" presenti in azienda.

16. La valutazione del processo di pianificazione strategica nella prospettiva del SCIGR: come elaborata nel paper Nedcommunity (2013), *Come valutare la governance in tema di rischi e controlli*, il Comitato valuta se il processo di pianificazione strategica è adeguatamente supportato da un idoneo processo di analisi dei rischi, 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.
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. 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.
Infine il Comitato 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. 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 già citato (2013) fornisce anche delle indicazioni per il Comitato su come valutare la scala di maturità dell'azienda del proprio sistema di

[22] International Professional Practice Framework (IPPF) dell'Institute of Internal Auditors inclusivo degli standard professionali riconosciuti

risk management in ambito della definizione del piano strategico.

17. Verifica della integrazione tra pianificazione strategica, tematiche ESG e processo di ERM con particolare riferimento all'impatto dei cambiamenti climatici. Il cambiamento climatico è un fattore non solo di impatto ambientale ma con specifiche implicazioni finanziarie e può richiedere una modifica del posizionamento strategico anche a breve termine. Il Comitato 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 (si rimanda al sito di Chapter Zero – *the Nedcommunity climate change directors forum*). 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 carattere non finanziario: Integrazione concernente la comunicazione di informazioni relative al clima"[23] (gli "Orientamenti")[24]. Anche lo European Confederation of Institute of Internal Auditors (ECIIA) ha pubblicato line guida in tema di cambiamento climatico: *Practical Guidance on climate change and environmental sustainability: How to tackle associated risks and harness opportunities? (ECIIA, 2020).*

18. L'analisi dell'informazione periodica a carattere non finanziario. L'informativa non finanziaria è materia relativamente recente ed in fase di forte evoluzione, come sintetizzato nel paper Nedcommunity- KPMG (2020), *Informativa extra finanziaria: da compliance a governance strategica dei rischi e delle opportunità*. 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. Consob nel regolamento n. 20267/2018 ha elencato le responsabilità della società di revisione e dell'organo di controllo. Il Codice di Corporate Governance (2020) ha esplicitato le responsabilità "minime" del CCR sull'informativa non finanziaria 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.

- Per quanto riguarda il SCIGR, il Comitato 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

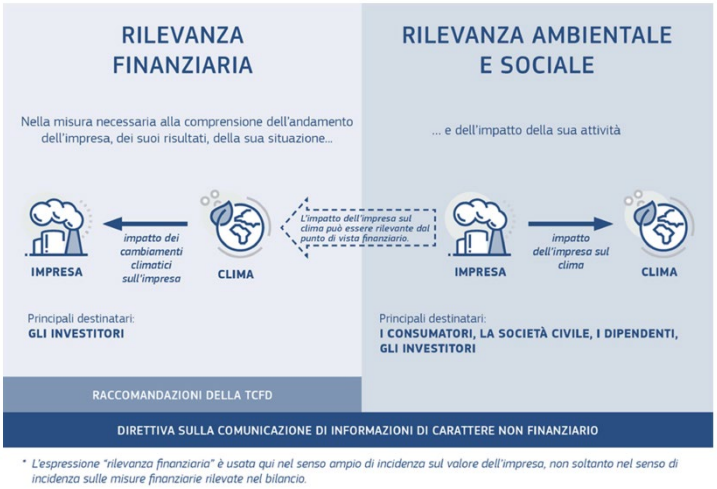
[23] Cfr.: «Orientamenti sulla comunicazione di informazioni di carattere non finanziario: Integrazione concernente la comunicazione di informazioni relative al clima» della Commissione europea (2019/C 209/01), pubblicati sulla GUCE il 20 giugno2019.

[24] 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).

controllo) e l'adeguatezza rispetto agli standard di riferimento indicati nell'informativa non finanziaria[25]. Nello svolgere questi compiti, il CCR incontra la società di revisione e sente l'organo di controllo.

- Per quanto riguarda l'idoneità a rappresentare il modello di business, il CCR valuta la coerenza con il piano strategico, l'analisi della materialità e l'impatto delle componenti non finanziarie sulle analisi 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"*)

Si ricorda inoltre di tenere in considerazione i summenzionati "Orientamenti della Commissione europea sulla comunicazione di informazioni di carattere non finanziario: Integrazione concernente la comunicazione di informazioni relative al clima" che offre una visione d'insieme.



Fonte: Orientamenti della Commissione europea sulla comunicazione di informazioni di carattere non finanziario

[25] 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). Tale disclosure mira a porsi quale parte integrante della relazione
https://www.weforum.org/whitepapers/toward-common-metrics-and-consistent-reporting-of-sustainable-value-creation
Rilevante anche lo sforzo di sviluppare standards europei di cui si occupa **EFRAG** (European Financial Reporting Advisory Group), sintetizzati nel *Progress report of the project task force on preparatory work for the elaboration of possible EU non-financial reporting standards* (novembre 2020)
https://www.efrag.org/News/Project-449/Progress-report-published-for-project-on-preparatory-work-for-the-elab

3. 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 all’Appendice 1 per un’analisi dei rispettivi ruoli al fine di facilitare la consapevolezza dei ruoli reciproci.

Di seguito riportiamo in modo semplificato un’indicazione di un’agenda di massima delle attività del CCR con le relative frequenze (annuale, semestrale, trimestrale), in linea con le indicazioni del Codice di Corporate Governance e le best practice di riferimento. Tale proposta, come già accennato, può essere adattata alla specifica realtà aziendale.

Annualmente

a) Aspetti di governance

- Parere su Linee guida del SCIGR
- Valutazione assetto organizzativo
- Valutazione dell'efficacia e adeguatezza del SCIGR
- Esame Relazione sul Governo Societario e Relazione sulla Gestione: sezioni relative allo SCIGR

b) SCIGR: Risk Framework

- Monitoraggio sull'aggiornamento del modello, sulla tassonomia dei rischi, sulla mappa dei rischi

c) SCIGR: Gestione dei rischi

- Valutazione dell'effettiva implementazione del risk framework
- Incontri con il management di una selezione di *business unit*

d) SCIGR: Internal Auditing e altre funzioni 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
- Approvazione Piano di Internal Audit e relativo budget
- Valutazione del Responsabile Internal Audit e livello/sistema remunerativo
- Valutazione adeguatezza organizzativa Internal Audit

e) Supporto alla pianificazione strategica

- Scenari di piano strategico e analisi dei rischi di piano

f) Reporting Finanziario e Non Finanziario

- 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 (SCIS), 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 revisione
- Esame reportistica non finanziaria ex D.Lgs 254/2016. 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 non finanziaria: adeguatezza procedure di rilevazione e controllo metriche, adesione a standard di rendicontazione internazionali
  - Società di revisione: processi e standard di rendicontazione

Semestralmente
a) Aspetti di governance • Approvazione della Relazione sulle attività del CCR nel semestre **d) SCIGR: Internal Auditing e altre funzioni 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 • Aggiornamenti con altre funzioni quando rilevante (Legale – contenziosi; IT – sicurezza informatica, segnalazioni (*whistleblowing*), Salute e Sicurezza sul lavoro, Ambiente (EHS), Procedure fiscali, Tax compliance, M&A, Procurement, Assicurazioni) **f) Reporting Finanziario e Non finanziario** • 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 - Direttore Finanza: Rischi finanziari, rischio di credito, rischio di liquidità - Società di revisione, in sinergia con l'organo di controllo
Trimestralmente
c) SCIGR: Gestione dei rischi • Incontri periodici con Responsabile risk management – monitoraggio dei rischi **d) SCIGR: Internal Auditing e altre funzioni di controllo** • Incontri periodici con Responsabile Internal audit; esame risultati di audit del trimestre e analisi follow-up

APPENDICE1

Confronto tra compiti del Comitato Controllo e Rischi e dell'Organo di Controllo

La presente appendice riporta un **confronto tra i compiti attribuiti al CCR e quelli attribuiti all'Organo di Controllo,** anche per agevolare un maggiore coordinamento delle rispettive attività. Pur rilevando i due distinti ruoli di tali soggetti (in quanto il Comitato 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 membro all'uopo designato) e, con disposizione innovativa, la partecipazione (sebbene facoltativa) degli altri membri dell'Organo di Controllo[26]. 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. Questo coordinamento è reso ancora più esplicito per gli istituti bancari.

Nelle pagine successive sono dettagliate le sinergie tra CCR e Organo di Controllo, facendo anche riferimento alla normativa specifica. In sintesi:

- L'Organo di Controllo effettua un controllo di maggiore dettaglio in relazione ai processi relativi alla reportistica e al lavoro dell'audit esterno (società di revisione)
- Il CCR prende atto dei pareri e delle osservazioni dell'Organo di Controllo
- L'Organo di Controllo effettua un monitoraggio del funzionamento del CCR

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 efficientizzare il flusso informativo e il coordinamento[27].

DISPOSIZIONI PER LE BANCHE[28]

Il comitato e l'organo con funzione di controllo scambiano tutte le informazioni di reciproco interesse e, ove opportuno, si coordinano per lo svolgimento dei rispettivi compiti. Almeno un componente dell'organo con funzione di controllo partecipa ai lavori del comitato.

Per una comprensione più completa delle attività dell'Organo di Controllo (in aggiunta a quanto riportato di seguito 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.

[26] La raccomandazione 37 del Codice 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"

[27] 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 membri del CCR e dell'Organo di Controllo.

[28] Banca d'Italia, cir. 285 – Parte prima, Titolo IV, Capitolo 1, Sezione IV – COMITATO RISCHI

Comitato Controllo Rischi (come dal Codice di Corporate Governance)[29]	Organo di Controllo[30]
Il Comitato supporta l'Organo di Amministrazione (Cfr. raccomandazione 33) nella:	
a) definizione delle linee di indirizzo del sistema di controllo interno e di gestione dei rischi;	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))

[29] 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)**.

[30] 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.

Comitato Controllo Rischi (come dal Codice di Corporate Governance)[29]	Organo di Controllo[30]
b) 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;	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)
c) 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*;	Esprime un parere sul piano di lavoro del responsabile della funzione di internal audit (Codice di Corporate Governance Racc. 33 - c)
d) 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	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 dell'ente sottoposto a revisione, senza violarne l'indipendenza (D.L. 39/2010 art. 19, a));
e) 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;	*A*i fini dello svolgimento dell'attività di vigilanza, l'organo di controllo 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. L'organo di controllo 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)
f) 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;	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))
g) 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	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))

Comitato Controllo Rischi (come dal Codice di Corporate Governance)[29]	Organo di Controllo[30]
valutazione complessiva sull'adeguatezza del sistema stesso e dando conto delle scelte effettuate in merito alla composizione dell'organismo di vigilanza di cui alla precedente lettera e).	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:	
a) 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	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, 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));
b) 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);	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.lg 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 trasmette a

Comitato Controllo Rischi (come dal Codice di Corporate Governance)[29]	Organo di Controllo[30]
	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 presenta le raccomandazioni o le proposte volte a garantirne l'integrità (D.L. 39/2010 art. 19, b));
c) esamina il contenuto dell'informazione periodica a carattere non finanziario rilevante ai fini del sistema di controllo interno e di gestione dei rischi;	L'organo di controllo, 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. 254/2016[31], art. 3 c.7). 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. 254/2016, art. 3 c.8).
d) 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;	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 l'informativa finanziaria dell'ente sottoposto a revisione, senza violarne l'indipendenza (D.L. 39/2010 art. 19, a));
e) esamina le relazioni periodiche e quelle di particolare rilevanza predisposte dalla funzione di *internal audit*;	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).
f) monitora l'autonomia, l'adeguatezza, l'efficacia e l'efficienza della funzione di internal audit;	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 l'informativa finanziaria dell'ente sottoposto a revisione, senza violarne l'indipendenza (D.L. 39/2010 art. 19, a));
g) può affidare alla funzione di internal audit lo svolgimento di verifiche su specifiche aree operative,	

[31] DECRETO LEGISLATIVO 30 dicembre 2016, n. 254: Attuazione della direttiva 2014/95/UE del Parlamento europeo e del Consiglio del 22 ottobre 2014, recante modifica alla direttiva 2013/34/UE per quanto riguarda la comunicazione di informazioni di carattere non finanziario e di informazioni sulla diversità da parte di talune imprese e di taluni gruppi di grandi dimensioni.

Comitato Controllo Rischi (come dal Codice di Corporate Governance)[29]	Organo di Controllo[30]
dandone contestuale comunicazione al presidente dell'organo di controllo;	
h) 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.	

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

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/

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

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/

Best practice internazionali

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

G20/OECD Principles of Corporate Governance

OECD (2015), *G20/OECD Principles of Corporate Governance*, OECD Publishing, Paris, https://doi.org/10.1787/9789264236882-en
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) and its subsidiary **ECIIA**

https://na.theiia.org/Pages/IIAHome.aspx
International Professional Practices Framework (IPPF)
2020 - *Developing a Risk-based Internal Audit Plan*
2020 - *The IIA's three lines model – an update of the three lines of defense*

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

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/