

## **L'Agenda del Comitato Controllo e Rischi**

*Un supporto pratico e concreto ai componenti del  
comitato controllo e rischi in particolare ed al consiglio di  
amministrazione in generale.*

*novembre 2016*

**Il presente documento è stato realizzato da Nedcommunity nell’ambito del  
“Reflection Group - La governance in materia di rischi e di controlli”.**

**Gruppo di lavoro:**

Carolyn Dittmeier (coordinatrice)  
Livia Aliberti Amidani  
Enrico Maria Bignami  
Graziella Capellini  
Rosalba Casiraghi  
Cesare Conti  
Elisabetta Magistretti  
Paola Schwizer

## L'Agenda del Comitato Controllo e Rischi

### Premessa

Una delle maggiori responsabilità di un Consiglio di Amministrazione è la gestione del rischio, che si traduce principalmente nel verificare che siano stati identificati e valutati i principali rischi dell'organizzazione e che siano stati adottati adeguati meccanismi di gestione e di mitigazione. In questo compito il Consiglio di Amministrazione può essere supportato dal Comitato Controllo e Rischi.

Il Comitato Controllo e Rischi è un organo consultivo che risponde all'esigenza di rafforzare la governance della società, garantire all'organo di governo un efficace esercizio dell'attività di supervisione sulla componente esecutiva e permettergli di addivenire in modo più informato e consapevole alle deliberazioni attinenti in generale al controllo interno e di gestione dei rischi, nonché a quelle relative all'approvazione delle relazioni finanziarie periodiche.

In considerazione dell'aumentata complessità e dell'ampiezza dei rischi che ormai ogni organizzazione deve affrontare, Nedcommunity intende fornire un supporto ai membri del Comitato Controllo e Rischi nella pianificazione delle attività necessarie ad ottemperare alle responsabilità poste in capo a tale organo.

A questo proposito si riporta di seguito una sintesi degli ambiti in cui assume rilievo il parere o il contributo del Comitato Controlli e Rischi e la relativa cadenza.

La tabella *L'Agenda del Comitato Controllo e Rischi* indica per ogni ambito trattato, le eventuali responsabilità aggiuntive previste dalla normativa di settore in capo al Comitato nelle aziende del settore finanziario.

Essa evidenzia altresì argomenti previsti in modo esplicito dal Codice di Autodisciplina e altri aspetti interpretativi forniti da Nedcommunity tramite la legenda seguente.

<b>Legenda:</b>	
Simbolo:	
➤	<b>Argomenti previsti in modo esplicito dal Codice di Autodisciplina</b>
❖	<b>Aspetti specifici evidenziati nel Paper Nedcommunity "Come valutare la governance in tema di rischi e controlli" (2-2013)</b>
<b>SCI GR Sistema di Controllo Interno e Gestione dei Rischi</b>	

Il presente documento riporta infine un utile confronto tra i compiti attribuiti al Comitato Controllo e Rischi e quelli attribuiti al Collegio Sindacale (appendice 1) e un estratto del Codice di Autodisciplina (appendice 2) anche per agevolare un maggiore coordinamento delle rispettive attività. Pur rilevando i due distinti ruoli di tali organi, 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 di Autodisciplina prevede la partecipazione necessaria del Presidente del Collegio Sindacale (o di altro sindaco all'uopo designato) e, con disposizione innovativa, la partecipazione (sebbene facoltativa) degli altri membri del Collegio Sindacale (art. 7.C.3). Un ottimale coordinamento tra questi due organi favorisce la corretta circolazione delle informazioni endo-consiliari e consente di migliorare l'efficienza del complessivo sistema dei controlli interni.

Infine si ritiene utile comunque menzionare il necessario coordinamento e collegamento del Comitato Controllo e Rischi con gli altri comitati endo-consiliari (es. comitato nomine o remunerazioni).

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 Comitato.

La declinazione dello strumento proposto dovrà essere valutata da ciascuna realtà aziendale per adattarlo 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.

Tabella  
**L'Agenda del Comitato Controllo e Rischi**

Ambito	“Good o Best Practice”	Cadenza	Integrazioni per il Settore Finanziario (non esaustivo)
<b>Governance e Documenti Societari</b>	<ul style="list-style-type: none"> <li>➤ Rivisitazione del Modello di governance complessivo<sup>1</sup></li> <li>➤ Parere sulle Linee di indirizzo del sistema di controllo interno e di gestione dei rischi</li> <li>➤ Esame e contributo alla stesura della Relazione sul governo societario relativamente al sistema di controllo interno e di gestione dei rischi</li> <li>➤ Esame Relazione CSR (se non delegato ad altro comitato)</li> <li>➤ Approvazione Relazione CCR</li> </ul>	<p>Annuale</p>           <p>Semestrale</p>	
<b>Pianificazione Strategica</b>	<ul style="list-style-type: none"> <li>❖ Valutazione del processo di pianificazione strategica in ottica SCI GR<sup>2</sup></li> <li>❖ Proposta Piano Strategico oggetto di approvazione da parte del CdA, in ottica SCI GR</li> </ul>	<p>Annuale</p>	
<b>Sistema di controllo Interno e Gestione Rischi</b>	<ul style="list-style-type: none"> <li>➤ Parere sulla valutazione del sistema di controllo interno e di gestione dei rischi</li> <li>❖ Valutazione dell’ambiente interno<sup>3</sup>/assetto organizzativo<sup>4</sup> ai fini SCI GR</li> <li>❖ Sistemi di indirizzo, coordinamento e controllo del Gruppo</li> <li>❖ Analisi andamento sistema di controllo interno<sup>5</sup></li> <li>❖ Analisi periodica dell’evoluzione dei rischi significativi (Focus da definire in base al settore/risk model)<sup>6</sup></li> <li>❖ Valutazione Altre Politiche<sup>7</sup></li> </ul> <p><b>Funzione di Internal Audit</b></p> <ul style="list-style-type: none"> <li>➤ Parere su nomina e revoca del Responsabile</li> <li>➤ Approvazione del Piano annuale / pluriennale della funzione<sup>8</sup></li> <li>➤ Esame Relazione annuale</li> <li>➤ Remunerazione del responsabile</li> <li>➤ Monitoraggio e valutazione della funzione<sup>9</sup></li> </ul>	<p>Semestrale</p>  <p>Annuale</p>    <p>Periodico o ad evento</p>  <p>Annuale</p>  <p>Annuale o ad evento</p>  <p>Annuale o ad evento</p>	<ul style="list-style-type: none"> <li>● Esame Relazione su ICAAP (<i>Internal Control Adequacy Assessment Process</i>) e ILAAP (<i>Internal Liquidity Adequacy Assessment Process</i>)</li> <li>● Approvazione e Aggiornamento RAF (<i>risk appetite framework</i>)</li> <li>● Informativa risk adjusted capital/ solvency ratio</li> <li>● Risk Policy ai fini Capital ratio</li> <li>● Risk Reporting</li> <li>● 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</li> </ul>



## L'Agenda del Comitato Controllo e Rischi: Note Esplicative <sup>1)</sup>

- 1. La rivisitazione del modello di governance complessivo** da parte del CCR può riferirsi al Modello di riferimento (ERM, COSO, ecc.) adottato dalla Società; al Modello Organizzativo D.Lgs. 231/01; alle politiche di governance; di controllo e di risk management eventualmente adottate; all'ultima relazione approvata su governance/assetti proprietari; agli eventuali aggiornamenti sugli orientamenti in merito.
- 2. La valutazione del processo di pianificazione strategica in ottica SCI GR**, come elaborata nel Paper Nedcommunity n. 2/2013 prende in considerazione i seguenti elementi: tassonomia rischi; mappatura rischi; modalità quantitative/qualitative di misurazione dei rischi e metodi di correlazione; organigramma, ruoli, sistema delle deleghe; progetti formativi; modello adottato per l'esplicitazione degli obiettivi; informazioni fornite dall'amministratore incaricato di vigilare sul sistema di controllo e di gestione dei rischi, dall'internal audit e da altre funzioni interessate coinvolte nel processo; aspetti implementativi del Modello organizzativo 231; scala di maturità.
- 3. La valutazione dell'ambiente interno** è l'elemento fondamentale che rivela l'impostazione di un'organizzazione, poiché determina e permette di evidenziare il livello di sensibilità del Vertice e di tutto il personale alla necessità di controllo e la gestione consapevole dei rischi e il fatto che l'impresa sia condotta nel rispetto di corretti principi. Rappresenta uno degli otto componenti dell'Enterprise Risk Management, come definito dall'ente internazionale di riferimento COSO, e può riguardare 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 e modalità di raccolta delle segnalazioni; risultati dell'attività di internal audit in merito; informazioni fornite dall'amministratore incaricato del sistema di controllo e di gestione dei rischi, ed eventuali survey; scala di maturità. Comprende anche aspetti organizzativi ricompresi nel punto successivo.
- 4. 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 alle evoluzioni 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. Considera inoltre l'adeguatezza dei sistemi di comunicazione: i flussi informativi da e verso il CdA; informazioni fornite dall'amministratore incaricato di vigilare sul sistema di controllo e di gestione dei rischi; informazioni fornite dai responsabili delle funzioni di

---

<sup>1</sup> cfr. Paper Nedcommunity come valutare la governance in tema di rischi e controlli per informazioni integrative

<http://www.nedcommunity.com/Pages/pubblicazioni: come valutare la governance in tema di rischi e controlli - febbraio 2013>

risorse umane/ organizzazione e dal responsabile ICT; strutturazione e adeguatezza del *management reporting*/ reporting gestionale anche tra funzioni aziendali; informazioni fornite dai responsabili di controllo della seconda e terza linea; analisi scala di maturità.

5. **Analisi andamento sistema di controllo interno:** tale analisi può basarsi dall'adeguatezza dei flussi informativi al CdA; informative fornite dall'amministratore incaricato di vigilare sul sistema di controllo e di gestione dei rischi; focus sulle criticità emerse dalle verifiche di Internal Auditing e piani di rafforzamento; flussi informativi provenienti dalle funzioni di controllo di secondo livello; evoluzione delle politiche e linee guida di *governance*; evoluzione impianto procedurale; informazioni fornite dalla società di revisione; Informazioni fornite dal Collegio Sindacale.
6. **Analisi periodica dell'evoluzione dei rischi significativi:** può basarsi su aspetti ricompresi nell'Agenda del CdA e sui flussi informativi al CdA; 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 imprevisi; analisi dell'Internal Audit.

Si ricordano i seguenti argomenti caldi che dovranno essere trattati individualmente:

- Business Continuity
- Cyber Security
- Whistleblowing (anche in relazione del modello d.lgs 231/01)
- Tax Risk Management
- Transaction Risk (M&A)
- Politiche Assicurative

7. **Esempi di altri documenti e politiche oggetto di valutazione da parte del CCR:** codice etico; politiche sicurezza di lavoro, politiche di gruppo su specifici processi chiave all'azienda (es investimenti, procurement, outsourcing, gestione finanziaria, ecc).
8. Ai fini del **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; informative fornite dal Collegio Sindacale; la composizione dell'"universo di audit"; i criteri di risk assessment; i criteri di copertura audit di medio termine.
9. **Valutazione della funzione di Internal Audit:** gli aspetti oggetto di esame da parte del Comitato possono comprendere la Quality Assurance Review (QAR) interna o esterna 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); 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; 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 o eventuale altro comitato preposto alla governance, prende in considerazione tutti gli aspetti di merito in termini di requisiti professionali, remunerazione, motivazioni sottostanti la proposta, ecc.





**Appendici:**

Appendice 1: Confronto tra compiti del Comitato Controllo e Rischi e del Collegio sindacale

Appendice 2: I compiti del Comitato Controllo e Rischi - Estratto dal Codice di Autodisciplina delle società quotate italiane (luglio 2015)

1

## Appendice 1 Confronto tra compiti del Comitato Controllo e Rischi e del Collegio sindacale

### A. Ambito Sistema di Controllo e Gestione dei Rischi

Comitato Controllo Rischi (come dal Codice di Autodisciplina)	Collegio Sindacale
<p><b>Supportare le valutazioni e le decisioni del CdA relative al sistema di controllo interno e di gestione dei rischi (7.P.3)</b></p> <ul style="list-style-type: none"> <li>• Esprime pareri su specifici aspetti inerenti alla identificazione dei principali rischi aziendali (7.C.2.b)</li> <li>• Esprime parere sulle linee di indirizzo del sistema di controllo interno e di gestione dei rischi (7.C.1.a)</li> <li>• Esamina le relazioni periodiche, aventi per oggetto la valutazione del sistema di controllo interno e di gestione dei rischi, e quelle di particolare rilevanza predisposte dalla funzione Internal Audit (7.C.2.c)</li> <li>• Monitora l'autonomia, l'adeguatezza, l'efficacia e l'efficienza della funzione di Internal Audit (7.C.2.d)</li> <li>• Esprime parere sul piano di lavoro della funzione di Internal Audit (7.C.1.c)</li> <li>• Parere sulla nomina/remunerazione/risorse di Internal Audit</li> <li>• Esprime parere sui risultati esposti dal revisore legale nella eventuale lettera di suggerimenti e nella relazione sulle questioni fondamentali emerse in sede di revisione legale. (7.C.1.e)</li> <li>• Esprime parere sull'adeguatezza del sistema di controllo interno e di gestione dei rischi rispetto alle caratteristiche dell'impresa e al profilo di rischio assunto, nonché la sua efficacia (7.C.1.b)</li> <li>• Esprime parere sulla descrizione, nella relazione sul governo societario, delle principali caratteristiche del sistema di controllo interno e di gestione dei rischi, e valutazione sull'adeguatezza dello stesso (7.C.1.d)</li> </ul>	<ul style="list-style-type: none"> <li>• Vigila sull'efficacia dei sistemi di controllo interno e di gestione del rischio (TUF /D.Lgs 24/2/98 n.58, Art. 149,)</li> <li>• Vigila sull'efficacia dei sistemi di revisione interna (Dlgs27/1/10, Art 19);</li> <li>• Esprime parere al CdA sul Piano di Internal Audit (Cod. Autodisciplina 7.C.1)</li> <li>• Esprime parere in merito a supporto del Comitato Controllo Rischi e CdA (Cod. Autodisciplina 7.C.1)</li> <li>• Esprime le proprie considerazioni al CdA (Cod. Autodisciplina 7.C.1)</li> <li>• Vigila sull'adeguatezza del sistema di controllo interno (TUF /D.Lgs. 24/2/98 n.58, Art. 149)</li> </ul>

**Appendice 1, segue**  
**Confronto tra i compiti del Comitato Controllo e Rischi ed il Collegio sindacale**

**B. Ambito Reporting Finanziario**

<b>Comitato Controllo Rischi (come dal Codice di Autodisciplina)</b>	<b>Collegio Sindacale</b>
<p><b>Supportare le valutazioni e le decisioni del CdA relative all'approvazione delle relazioni finanziarie periodiche (7.P.3)</b></p> <ul style="list-style-type: none"> <li>Valuta il corretto utilizzo dei principi contabili e, nel caso di gruppi, la loro omogeneità ai fini del bilancio consolidato</li> </ul>	<ul style="list-style-type: none"> <li>Esprime Parere in merito a supporto del Comitato Controllo Rischi (cfr Cod. Autodisciplina)</li> <li>Vigila sull'adeguatezza dell'assetto organizzativo, amministrativo e contabile adottato dalla società sul suo concreto funzionamento (Art 2403 C.C.)</li> <li>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 )</li> <li>Vigila sul processo di informativa finanziaria; (D.Lgs del 27/1/10 n. 39 Art. 19 )</li> <li>Vigila sulla revisione legale dei conti annuali e dei conti consolidati (TUF /d.lg 24/2/98 n.58, Art. 149)</li> <li>Vigila sull'indipendenza del revisore legale o della società di revisione legale, in particolare per quanto concerne la prestazione di servizi non di revisione all'ente sottoposto alla revisione legale dei conti (D.Lgs del 27/1/10 n. 39 Art. 19 )</li> </ul>

## Appendice 2

### I compiti del Comitato Controllo e Rischi

#### Estratto dal Codice di Autodisciplina delle società quotate italiane (luglio 2015)

##### 7.C.1. Il consiglio di amministrazione, previo parere del comitato controllo e rischi:

- a) definisce le **linee di indirizzo del sistema di controllo interno e di gestione dei rischi**, in modo che i principali rischi afferenti all'emittente e alle sue controllate risultino correttamente identificati, nonché adeguatamente misurati, gestiti e monitorati, determinando inoltre il grado di compatibilità di tali rischi con una gestione dell'impresa coerente con gli obiettivi strategici individuati;
- b) valuta, con cadenza almeno annuale, **l'adeguatezza del sistema di controllo interno e di gestione dei rischi** rispetto alle caratteristiche dell'impresa e al profilo di rischio assunto, nonché la sua efficacia;
- c) approva, con cadenza almeno annuale, il **piano di lavoro predisposto dal responsabile della funzione di Internal Audit**, sentiti il collegio sindacale e l'amministratore incaricato del sistema di controllo interno e di gestione dei rischi;
- d) **descrive, nella relazione sul governo societario, le principali caratteristiche del sistema** di controllo interno e di gestione dei rischi e le modalità di coordinamento tra i soggetti in esso coinvolti, esprimendo la propria **valutazione sull'adeguatezza dello stesso**;
- e) **valuta, sentito il collegio sindacale, i risultati esposti dal revisore legale** nella eventuale lettera di suggerimenti e nella relazione sulle questioni fondamentali emerse in sede di revisione legale.

Il consiglio di amministrazione, su proposta dell'amministratore incaricato del sistema di controllo interno e di gestione dei rischi e previo parere favorevole del comitato controllo e rischi, nonché sentito il collegio sindacale: - nomina e revoca il responsabile della funzione di **Internal Audit**; assicura che lo stesso sia dotato delle risorse adeguate all'espletamento delle proprie responsabilità; ne definisce la remunerazione coerentemente con le politiche aziendali.

##### 7.C.2 Il comitato controllo e rischi, nell'assistere il consiglio di amministrazione:

- a) valuta, unitamente al dirigente preposto alla redazione dei documenti contabili societari e sentiti il revisore legale e il collegio sindacale, **il corretto utilizzo dei principi contabili** e, nel caso di gruppi, la loro omogeneità ai fini della redazione del bilancio consolidato;
- b) esprime pareri su specifici aspetti inerenti alla **identificazione dei principali rischi** aziendali;
- c) **esamina le relazioni periodiche, aventi per oggetto la valutazione del sistema di controllo interno e di gestione dei rischi**, e quelle di particolare rilevanza predisposte dalla funzione *Internal Audit*;
- d) monitora l'autonomia, l'adeguatezza, l'efficacia e l'efficienza della **funzione di Internal Audit**;
- e) può chiedere alla funzione di *Internal Audit* lo svolgimento di verifiche su specifiche aree operative, dandone contestuale comunicazione al presidente del collegio sindacale;
- f) **riferisce al consiglio**, almeno semestralmente, in occasione dell'approvazione della relazione finanziaria annuale e semestrale, sull'attività svolta nonché sull'adeguatezza del sistema di controllo interno e di gestione dei rischi;
- g) supporta, con un'adeguata attività istruttoria, le valutazioni e le decisioni del consiglio di amministrazione relative alla gestione di rischi derivanti da fatti pregiudizievoli di cui il consiglio di amministrazione sia venuto a conoscenza.

**7.C.3.** Ai lavori del comitato controllo e rischi partecipa il presidente del collegio sindacale o altro sindaco da lui designato; possono comunque partecipare anche gli altri sindaci.