# *Amministratori e componenti del Comitato controllo e rischi: Come valutare la governance in tema di rischi e controlli*

*Un contributo per l'effettiva implementazione delle disposizioni previste dal Codice di Autodisciplina, dicembre 2011, art. 7- Sistema di controllo interno e di gestione dei rischi*

*febbraio 2013*

## Executive Summary

Il Codice di Autodisciplina, emesso dal Comitato per la Corporate Governance nel dicembre 2011, ha chiarito in modo inequivocabile le responsabilità degli organi di governo che, nell'ambito della conduzione e della supervisione dell'attività di impresa, devono garantire una buona *governance* del sistema integrato di gestione dei rischi e dei relativi controlli interni.

Il documento *Amministratori e componenti del Comitato controllo e rischi:Come valutare la governance in tema di rischi e controlli* ha l'obiettivo di supportare in modo pratico il Consiglio di Amministrazione e, in particolare, i membri del Comitato controllo e rischi ma anche indirettamente il Collegio Sindacale nella trattazione di temi relativi a rischi e controlli. In proposito, i macro ambiti, che saranno analizzati nel seguito, oggetto di attenta valutazione da parte degli Amministratori e dei componenti del Comitato controllo e rischi, riguardano:

- l'adeguatezza del modello di riferimento adottato dagli organi di governo;
- una scala di maturità per la governance di rischi e controlli;
- il raggiungimento di una gestione equilibrata degli obiettivi di business e di governo;
- l'efficacia del risk management;
- l'efficacia e l'efficienza del sistema di controllo interno;
- l'adeguatezza della funzione di Internal Audit.

L'attività di studio e ricerca, finalizzata alla trattazione degli orientamenti qui presentati, ha considerato le *best practice* note in letteratura[1] anche a livello internazionale[2] e si caratterizza per i seguenti approcci distintivi:


- si riferisce alle componenti presentate nel modello internazionale *Enterprise Risk Management* (ERM), rappresentato graficamente di lato, ad oggi adottato in Italia solo parzialmente dalle società quotate; l'ERM fornisce agli organi di governo e di controllo, impegnati nella delicata e complessa attività di vigilanza sull'efficacia della *governance,* un quadro approfondito per la formulazione di opportune riflessioni relative alla misurazione e gestione dei rischi, al sistema dei controlli interni ed alla funzione di Internal Audit;
- facilita, mediante lo strumento di una 'scala di maturità' aziendale, di per sé coerente con il modello ERM, la disamina sistematica di alcuni ambiti di *governance* correlati a rischi e controlli; in questo modo, la scala di maturità consente al Comitato controllo e rischi ed al Consiglio di Amministrazione in generale, di valutare il posizionamento dell'impresa, di definire piani ed iniziative di sviluppo e di rafforzare la *governance* dei rischi e dei controlli in ottica di miglioramento continuo;
- formula orientamenti, mediante lo sviluppo di temi collegati a specifici quesiti sui quali il Comitato controllo e rischi dovrebbe interrogarsi, per valutare i sistemi di gestione dei rischi ed i controlli ad essi collegati e fornisce indicazioni su come superare tipiche problematiche che possono sorgere in ambito di rischi e controlli per raggiungere un effettivo sistema globale di *governance*;
- illustra la piena integrazione dei principi cardine del D.Lgs. 231/01 con il modello ERM al fine di rispondere contestualmente alle esigenze degli organi di governo, di controllo e di vigilanza delle

[1] Lo sviluppo del documento tiene conto di altre importanti pubblicazioni emesse da associazioni professionali, in particolare della 'Guida operativa breve per amministratori indipendenti e sindaci' di Assogestioni, novembre 2011

[2] Si fa riferimento in particolare alle linee guida emanate dalla *Federation of European Risk Management Associations* (FERMA), dalla *European Confederation of Directors Association* (ecoDa) di concerto con la *European Confederation of Institutes of Internal Auditing* (ECIIA) in merito all'art 41 dell'VIII direttiva comunitaria in materia di diritto societario, recepito in Italia con l'art. 19 del Decreto Legge 39/ 2010.

imprese che hanno adottato uno specifico modello di organizzazione e gestione volto alla prevenzione dell'ampio spettro dei c.d. reati 231.

Il documento nella sua articolazione svilupperà i temi introdotti dai seguenti interrogativi:

- In che modo gli obiettivi dell'organizzazione sono declinati a livello aziendale?
- Come procedere per una completa identificazione dei rischi ?
- Come avviene la valutazione dei rischi in termini di dimensionamento o rilevanza?
- Come viene definito il 'profilo di rischio'?
- Il processo di gestione del rischio è integrato nel sistema organizzativo aziendale?
- Su quali flussi informativi si basa l'attività del Comitato controlli e rischi al fine di monitorare l'evoluzione dei rischi?
- In che modo il top management dimostra una solida cultura di controllo?
- Il sistema delle deleghe, nei ruoli e nelle responsabilità, favorisce il sistema di controllo?
- L'insieme delle politiche/ procedure è adeguato al fine di supportare il sistema dei controlli ed il *risk management*?
- Le informazioni necessarie per le decisioni e le attività di controllo sono disponibili in modo tempestivo e affidabile?
- Le attività di controllo interno sono definite in modo coerente con gli obiettivi dell'organizzazione e con gli aspetti connessi alla gestione del rischio?
- In che modo sono monitorate le iniziative di miglioramento del management in risposta alle carenze del sistema di controllo interno conosciute?
- L'attività di Audit è svolta in modo corretto, completo ed efficiente?

Infine, in base alle tematiche trattate, gli argomenti da inserire nell'agenda del Comitato controllo e rischi, insieme agli elementi e le informazioni da valutare sono riassunti nella fase conclusiva del documento.

Con l'auspicio di fornire contributi concreti per l'effettiva implementazione delle disposizioni previste dal Codice di Autodisciplina e per migliorare l'efficacia della corporate governance in Italia, si augura buona lettura.

# Indice

## I - Introduzione

Il Codice di Autodisciplina, promosso da Abi, Ania, Assonime, Assogestioni, Borsa Italiana e Confindustria ed emesso nel dicembre 2011 dal Comitato per la Corporate Governance, ha chiarito in modo inequivocabile le responsabilità degli organi di governo che, nell'ambito della conduzione e della supervisione dell'attività di impresa, devono garantire una buona *governance* del sistema integrato di gestione dei rischi e dei relativi controlli interni.

Pertanto, il testo ha l'obiettivo di supportare in modo pratico il Consiglio di Amministrazione, in particolare il Comitato controllo e rischi, ed indirettamente il Collegio Sindacale nella trattazione di temi relativi a rischi e controlli, promuovendo analisi approfondite e discussioni proficue. A tal fine, nel prosieguo saranno presentati una serie di interrogativi ai quali seguiranno orientamenti e riflessioni volti a fornire agli organi di governo strumenti utili per la formulazione di valutazioni strategiche.

L'attività di studio e ricerca finalizzata alla trattazione dei temi qui presentati ha riguardato, tra l'altro, l'analisi di alcune *best practice* note in letteratura[3]; in particolare, nel contesto internazionale si fa riferimento alle recenti linee guida emanate dalla *Federation of European Risk Management Associations* (FERMA) e dalla *European Confederation of Directors Association (ecoDa)* di concerto con la *European Confederation of Institutes of Internal Auditing* (ECIIA)[4] in merito all'art 41 dell'VIII direttiva comunitaria[5] in materia di diritto societario, recepito in Italia con l'art. 19 del Decreto Legge 39/ 2010.

Inoltre, il documento, nella sua articolazione, fa riferimento alle componenti presentate nel modello internazionale *Enterprise Risk Management* (ERM), che in linea con quanto previsto dal Codice di Autodisciplina di Borsa Italiana, evidenzia l'importanza di un sistema integrato di gestione di rischi e controlli ai fini di una buona governance. Il modello ERM fornisce, infatti, agli organi di governo e di controllo, impegnati nella delicata e complessa attività di vigilanza sull'efficacia della *governance,* un quadro approfondito per la formulazione di opportune riflessioni strategiche sulla gestione dei rischi, sul sistema dei controlli interni e sulla funzione di Internal Audit.

Infine, si precisa che il saggio sebbene faccia formalmente riferimento al modello tradizionale delle società, illustra temi altresì applicabili alle organizzazioni che hanno scelto il modello dualistico.

## II - L'adozione di un modello di riferimento da parte degli organi di governo


Il Codice di Autodisciplina di Borsa Italiana, nel suo decalogo per le società emittenti, descrive il sistema dei controlli e di gestione dei rischi richiedendo che: 'Ogni emittente si doti di un sistema di controllo interno e di gestione dei rischi costituito dall'insieme delle regole, delle procedure e delle strutture organizzative volte a consentire l'identificazione, la misurazione, la gestione e il monitoraggio dei principali rischi. Tale sistema è integrato nei più generali assetti organizzativi e di governo societario adottati dall'emittente e tiene in adeguata considerazione i modelli di riferimento e le *best practices* esistenti in ambito nazionale e internazionale'[6].

In linea con tali prescrizioni, è utile far riferimento al modello E*nterprise Risk Management* (ERM) diffuso nel 2004 dal *Committee of Sponsoring*

[3] Lo sviluppo del documento tiene conto di altre importanti pubblicazioni emesse da associazioni professionali, in particolare della 'Guida operativa breve per amministratori indipendenti e sindaci' di Assogestioni.

[4] *Cfr*. *Making the most of the internal Audit Function: recommendations for Directors and Board Committees*, ECIIA and ecoDa, dicembre 2012; *Guidance on the 8th EU Company Law Directive* -article 41, ECIIA and FERMA, settembre 2010 e dicembre 2011.

[5] Direttiva 2006/43/CE.

[6] *Cfr*. Art.7 – Sistema di controllo interno e gestione dei rischi, Principi 7.P.1. del Codice di Autodisciplina.

*Organizations* (*CoSO*) e richiamato di recente anche dalla *task force* c.d. '*Reflection Group*' costituita della Commissione Europea[7]. Tale modello, sopra rappresentato, illustra appunto la correlazione, espressa in un rapporto matriciale e integrato, tra gli obiettivi generali perseguiti dall'azienda, le componenti del sistema di controllo e la struttura organizzativa societaria.

A tal proposito, giova ricordare che in precedenza (1992), il *Committee of Sponsoring Organizations of the Treadway Commission* aveva già emesso il '*CoSO Report'* (modello *CoSO*)[8] con le cinque componenti del sistema di controllo[9] che di fatto rappresenta il quadro di riferimento da cui è stato poi sviluppato l'ERM.

Si evidenzia, inoltre, che limitatamente alle finalità legate al *financial reporting* ed agli adempimenti del Dirigente Preposto alla redazione di documenti contabili societari, molte imprese italiane hanno adottato il modello CoSO[10]; infatti, da uno studio condotto sulle 40 società italiane quotate con maggior capitalizzazione di borsa[11], è emerso che oltre l'70% di tali società ha adottato un *framework* di gestione del rischio e di controllo interno funzionale focalizzato peraltro agli obiettivi di *reporting* finanziario.

Ora se da una parte il Modello *CoSO* costituisce un valido quadro di riferimento per gli adempimenti prescritti a carico del Dirigente Preposto, dall'altra invece non evidenzia un'ampia focalizzazione sulla gestione dei rischi e degli obiettivi strategico - operativi. In pratica, la struttura del Modello *CoSO* si presenta compatibile con il concetto di rischio puro[12] ma non tiene conto di rischi/ opportunità potenziali. In questo senso, le società che hanno scelto come quadro di riferimento interno il modello *CoSO*, anziché scegliere strategie di *risk management* di ampio respiro, si sono perlopiù orientate verso strategie di minimizzazione del rischio residuale[13].

Al riguardo, si precisa che il quadro di riferimento ERM rispetto al precedente modello *CoSO* presenta alcune importanti caratteristiche evolutive[14]:

- consente di governare anche gli obiettivi strategici oltre quelli operativi;
- esalta la definizione e la comunicazione degli obiettivi all'interno dell'organizzazione;
- sottolinea l'importanza dell'ambiente interno nel suo complesso e non solo limitatamente all'ambiente di controllo;
- considera anche i rischi/opportunità potenziali[15] articolando tutte le attività sottostanti alla gestione dei rischi.

Con riferimento a questo ultimo punto, si sottolinea che nel modello ERM l'estensione del concetto di rischio ad eventi dannosi anche solo latenti, implica l'adozione da parte dell'azienda di approcci di gestione del rischio

---

[7] *Cfr. Reflection Group on the future of EU Company Law, European Commission*, aprile 2011.

[8] Tradotto in italiano nel testo di PricewaterhouseCoopers, Il sistema di controllo interno: un modello integrato di riferimento per la gestione dei rischi aziendali, maggio 2008, Il Sole 24 ore.

[9] Secondo il Modello *CoSO* il sistema di controllo interno è costituito dal complesso integrato dei seguenti 5 elementi: ambiente di controllo, valutazione dei rischi, attività di controllo, informazione e comunicazione e monitoraggio.

[10] Ad esempio: Linee guida per la predisposizione di un regolamento per lo svolgimento delle attività del dirigente preposto alla redazione dei documenti contabili e societari, ANDAF(Associazione Nazionale Dirigenti Amministrativi e Finanziari), aprile 2008; Linee guida per lo svolgimento delle attività del dirigente preposto di Confindustria, dicembre 2007.

[11] L'esame è stato condotto analizzando le Relazioni sulla *corporate governance* e sugli assetti societari; in particolare, è stato considerato il *framework* di riferimento adottato per la verifica dell'adeguatezza e dell'effettiva applicazione dei controlli interni relativi all'informativa finanziaria per il bilancio 2011.

[12] Per rischio puro si intende la probabilità di subire perdite dovute al manifestarsi di eventi dannosi.

[13] Per rischio residuale s'intende il rischio connesso ad un evento dopo aver preso in considerazione i controlli implementati per ridurre l'effetto o la probabilità di accadimento dell'evento stesso; il rischio residuale non può mai essere eliminato del tutto.

[14] *Cfr.* Dittmeier Carolyn, Internal Auditing - Chiave per la Corporate Governance, EGEA, marzo 2011- Capitolo 5.

[15] Si precisa che per rischio potenziale si intende il rischio inerente ovvero l'attitudine di una classe di valori a presentare errori significativi indipendentemente dall'esistenza di procedure di controllo interno.

diversificati che non comportano solo la mera minimizzazione del rischio ma considerano anche le seguenti strategie: evitare, condividere, accettare il rischio[16].

Pertanto, l'adozione del modello ERM costituisce il punto di partenza per rispondere all'esigenza del Consiglio di Amministrazione di definire, previo parere del Comitato controllo e rischi, le linee di indirizzo nella gestione dei rischi e dei controlli interni coerenti con quanto prescritto dai criteri applicativi di cui all'Art. 7.C.1 del citato Codice di Autodisciplina.

Il quadro di riferimento delineato dall'ERM, in coerenza con i principi cardine del D.Lgs. 231/01 illustrati nell'immagine riportata di lato, risponde altresì pienamente alle esigenze delle imprese che adottano un adeguato modello di organizzazione e gestione al fine di prevenire responsabilità penali a carico delle società stesse derivanti da reati commessi nell'interesse o vantaggio degli enti (c.d. reati 231). Questo approccio, trattato approfonditamente nell'Appendice 2, sostiene l'esigenza di promuovere una maggiore efficienza del sistema dei controlli interni.


Inoltre, nel suo ruolo di vigilanza sul processo di *risk management* e di controllo interno, il Collegio Sindacale, in qualità di Comitato per il controllo interno e la revisione contabile, vigila sull'adozione da parte delle società di un adeguato modello di gestione del rischio e, in caso negativo, si accerta che il Consiglio di Amministrazione stia effettuando le opportune valutazioni.

In conclusione, la moderna concezione dei controlli non può prescindere dalla nozione di rischio; pertanto, il sistema di controllo interno e quello di gestione dei rischi devono essere considerati come un sistema unitario ed integrato le cui componenti sono tra loro coordinate in modo interdipendente ed il sistema, nel suo complesso, è inserito nell'assetto organizzativo della società a tutti i livelli.

## III – Una scala di maturità per la governance di rischi e controlli

Le scale di maturità della *governance* costituiscono per, il Comitato controllo e rischi ed il Consiglio di Amministrazione in generale, uno strumento di riferimento per la valutazione del livello di efficacia e del grado di ottimizzazione della *governance*, dei presidi di *risk management* e dei controlli aziendali[17]. Inoltre, tale approccio può supportare attività di *benchmarking* utili per delineare il livello minimo accettabile di *governance* che il Consiglio di Amministrazione intende ottenere.

La scala di maturità proposta, le cui componenti sono sostanzialmente riconducibili agli elementi dell'ERM precedentemente descritti, valuta i seguenti aspetti:

a. il sistema organizzativo delle competenze, delle deleghe, e dei comportamenti;
b. il livello di definizione degli obiettivi, dei piani strategici e del *risk management;*
c. la definizione dei processi e delle procedure operative ai vari livelli organizzativi;
d. i sistemi di comunicazione delle informazioni e le tecnologie di supporto;
e. i sistemi di misurazione e monitoraggio.

La scala di maturità, articolata in 5 livelli, descrive per ciascun ambito sopra riportato il grado di evoluzione e sviluppo della *governance* interna. In particolare, a livello 1, non esistono sistemi di

[16] Si ricorda che la strategia di 'evitare il rischio' implica la scelta di non effettuare alcune tipologie di attività, quella di 'condividere il rischio' consiste nel trasferirlo in parte a terzi attraverso assicurazioni, coperture, sistemi di outsourcing, ecc. mentre 'accettare il rischio' comporta il riconoscimento che i benefici di un certo progetto superano i costi di trasferimento o di mitigazione.
[17] *Cfr. Evaluating and Improving Organizational Governance, Bahrman Dean*, *IIA Research Foundation*, marzo 2011.

governo strutturati e le attività, dipendendo dalla volontà dei singoli individui, sono informali e poco sistematiche; a livello 3 le attività sono definite, consentono una chiara identificazione dei compiti e delle responsabilità ma la fase attuativa è ancora ad uno stadio iniziale; infine, il livello 5 rappresenta una fase ottimale per l'azienda che è consapevole del vantaggio competitivo raggiunto con l'adozione di un processo di *governance* integrato e sviluppato in tutti i suoi aspetti.

La disamina annuale, da parte del Consiglio di Amministrazione e del Comitato controllo e rischi, della scala di maturità e del relativo posizionamento dell'impresa, è un'ottima modalità sia per valutare l'effettivo risultato del processo di continuo miglioramento, che per definire piani ed iniziative di sviluppo e rafforzamento della *governance* di rischi e controlli.

A titolo esemplificativo, l'Appendice 1 illustra in modo diffuso le matrici per la valutazione del grado di maturità della governance aziendale.

## IV. - La comunicazione e l'equilibrata gestione degli obiettivi di business e di governo


Il complesso sistema organizzativo di persone e mezzi di cui l'impresa si compone è imperniato sulla definizione degli obiettivi formulati dagli organi di governo ed è rivolto al suo raggiungimento. A tal proposito, il Codice di Autodisciplina sottolinea l'importanza del contributo fornito da un efficace sistema di controllo interno e di gestione dei rischi nella conduzione dell'impresa in coerenza con gli obiettivi aziendali[18]. Tale principio riposa sul presupposto che considera il rischio come un deterrente per l'azienda nel raggiungimento degli obiettivi predefiniti ed il sistema di controllo come un strumento utile a mitigare il rischio ed assicurare il conseguimento di buoni risultati.

Pertanto, in considerazione della numerosità degli obiettivi strategici di business e di governance, ai fini di una gestione equilibrata, sarebbe opportuno che gli organi di governo riflettessero attentamente in merito alle modalità di comunicazione degli obiettivi stessi. Tuttavia, a livello internazionale, ed anche in Italia, si osserva quasi sempre la mancanza di una chiara esplicitazione degli obiettivi aziendali con conseguenti inefficienze nella gestione del rischio e nell'implementazione del sistema di controllo[19]. Pertanto, giova portare in evidenza alcuni orientamenti delineati per gli Amministratori in tema di effettiva formulazione e declinazione degli obiettivi aziendali.

Infine, si rimanda all'Appendice 1 dove, proprio con riferimento alla definizione degli obiettivi, la matrice della scala di maturità dell'azienda illustra le possibili classificazioni della governance aziendale.

### IV.1 In che modo gli obiettivi dell'organizzazione sono declinati nei diversi livelli aziendali?

Il Piano Strategico dell'impresa dovrebbe presentare in modo chiaro gli obiettivi strategici aziendali la cui diffusione all'interno dell'organizzazione rappresenta un momento essenziale per il corretto funzionamento del sistema di controllo; peraltro, la migliore esplicitazione degli obiettivi di *business*, di *governance* e di responsabilità sociale, è fondamentale al fine di declinare e comunicare correttamente gli stessi anche ai livelli operativi.

Tuttavia, quando si discute di obiettivi aziendali, l'aspetto che forse non è sufficientemente enfatizzato si riferisce al concetto di raggiungibilità degli obiettivi stessi. Tale elemento è invece estremamente

[18] *Cfr*. Art.7 – Sistema di controllo interno e gestione dei rischi, Principi 7.P.2. del Codice di Autodisciplina.
[19] *Managing Risk: a new framework*, R. Kaplan e M. Hannette, Harvard Business School, giugno 2012.

importante soprattutto se si considera l'esigenza di scomporre ciascun macro obiettivo ed assegnarlo in quota parte non solo ai livelli apicali ma anche a quelli intermedi ed operativi al fine di consentire ad ogni attore di concorrere alla realizzazione di un segmento, più o meno articolato, del Piano Aziendale.

La raggiungibilità degli obiettivi predefiniti rileva, inoltre, nei sistemi di *Management by Objectives* e può contribuire in modo significativo, con impatti positivi o negativi, alla definizione di logiche di *risk management* e di controllo; in questo senso, è importante che gli obiettivi non siano troppo sfidanti ed al tempo stesso siano perlopiù quantificabili in termini oggettivi.

In ragione di quanto detto, si sottolinea che, qualora il processo di definizione degli obiettivi aziendali non fosse adeguatamente implementato e comunicato, uno stesso obiettivo potrebbe essere interpretato in modo diverso. Ad esempio, se fosse dichiarato l'obiettivo di crescita della soddisfazione del cliente, questo singolo obiettivo per il reparto di produzione potrebbe essere interpretato e misurato con la riduzione dei tempi di consegna dei prodotti ai clienti, mentre per la funzione Amministrazione e Finanza potrebbe essere inteso come la riduzione dei reclami e dei resi. Questo semplice esempio evidenzia l'opportunità di accompagnare la comunicazione dei singoli obiettivi con una specifica analisi che misuri l'importanza dei diversi ruoli aziendali ed espliciti, in modo univoco per ogni funzione, i singoli obiettivi di dettaglio al fine di conseguire buoni risultati globali. A titolo esemplificativo, la tabella che segue presenta la declinazione di alcuni obiettivi strategici sui macroprocessi nei settori industriali e finanziari.

| OBIETTIVI IMPRESA | OBIETTIVI DEL PROCESSO PRODUZIONE | OBIETTIVI DEL PROCESSO SERVIZI FINANZIARI |
|---|---|---|
| **Obiettivi di *Business*:** | | |
| **1. Volume** | 1. Capacità di produzione | 1. Incremento delle transazioni |
| **2. Contenimento costi** | 2. Contenimento costi | 2. Contenimento costi |
| **3. Efficacia del processo** | 3. Qualità della produzione | 3. Servizio di assistenza |
| ***4. Customer satisfaction*** | *4. Time to market* | 4. Diminuire i reclami |
| **5. Profittabilità** | 5. - | 5. Profittabilità dei prodotti dei servizi finanziari |
| **6. Innovazione/tecnologica** | 6. Tecnologia dell'impianto di produzione | 6. Sistema informativo |
| **7. Quote di mercato** | 7. - | 7. Incremento della clientela |
| **8. Altro** | 8. - | 8. - |
| **Obiettivi di *Governance*:** | | |
| **1. Affidabilità informativa** | 1. Affidabilità dei report di monitoraggio | 1. Affidabilità del *reporting* finanziario e gestionale |
| **2. *Compliance* legale** | 2. *Compliance* agli standard di mercato | 2. *Compliance* alle regole del settore finanziario |
| **3. Sicurezza** | 3. Sicurezza nei luoghi di lavoro | 3. Sicurezza delle informazioni |
| **4. Responsabilità sociale** | 4. Riduzione dell'inquinamento | 4. - |
| **5. Altro** | | |

Per quanto detto, gli Amministratori, con il supporto del Comitato controllo e rischi, potrebbero valutare l'opportunità di:

- adottare, per le diverse categorie di obiettivi di *business*, di *governance* e di responsabilità sociale, un modello predefinito (*cfr*. nella tabella sopra riportata la colonna posta a sinistra) dal quale intraprendere la formulazione di piani e di procedure aziendali orientate all'esplicitazione di ciascun obiettivo;
- approvare il Piano Strategico assicurando che un adeguato livello di esplicitazione degli obiettivi sia basato su tale modello;
- verificare, tramite l'Amministratore incaricato di vigilare in particolar modo sul sistema di controllo e gestione dei rischi[20], se emergono conflitti significativi non risolti tra i vari obiettivi predefiniti;
- richiedere all'Amministratore incaricato di vigilare sul sistema di controllo e di gestione dei rischi di assicurare la continua verifica della funzionalità del sistema di incentivazione in relazione alle principali tematiche di rischio e controllo.

## V. - L'efficacia del Risk Management

Il Codice di Autodisciplina prevede che il Consiglio di Amministrazione, con l'ausilio del Comitato controllo e rischi, valuti appunto l'adeguatezza del sistema di controllo interno e di gestione dei rischi considerando le caratteristiche dell'impresa ed il profilo di rischio assunto[21].

A tal proposito, considerando che i termini rischio e gestione del rischio coprono indistintamente tutti gli aspetti connessi al *business* e si riferiscono sia alle opportunità che alle minacce, i temi trattati nel prosieguo rappresentano un valido orientamento, ispirato alla matrice a tre dimensioni del modello internazionale ERM, e potranno essere considerati unitamente al posizionamento dell'azienda sulla 'scala di maturità' (*cfr*. Appendice 1) e all'adozione di modalità di *risk management* più o meno complesse all'interno dell'organizzazione.

In questo senso, il Consiglio di Amministrazione ed il Comitato controllo e rischi dovrebbero intraprendere un percorso progressivo verso il raggiungimento di una adeguata strutturazione metodologica e di sistema; inoltre, il Collegio Sindacale, in qualità di Comitato per il controllo interno e la revisione contabile, potrà a sua volta ragionare sugli indirizzi suggeriti da questo testo qualora, nell'ambito della sua attività di vigilanza, osservi che il Consiglio di Amministrazione effettui analisi incomplete o non del tutto corrette in merito a tali temi strategici.


### V.1 Come procedere per una completa identificazione dei rischi ?

Il citato Codice di Autodisciplina prevede che l'Amministratore incaricato di vigilare sul sistema di controllo e di gestione dei rischi curi la mappatura dei principali rischi aziendali[22] e la sottoponga periodicamente alla valutazione del Consiglio di Amministrazione[23].

In questo senso, il Consiglio di Amministrazione deve verificare che l'azienda

[20] *Cfr*. Art.7 – Sistema di controllo interno e gestione dei rischi, Principi 7.P.3 punto *(i)* del Codice di Autodisciplina dove si precisa che il 'Consiglio di Amministrazione individua al suo interno: uno o più amministratori incaricati dell'istituzione e del mantenimento di un efficace sistema di controllo e di gestione dei rischi'.
[21] *Cfr*. Art.7 – Sistema di controllo interno e gestione dei rischi, Criteri applicativi 7.C.1 punto *(b)* del Codice di Autodisciplina.
[22] Con riferimento al processo di identificazione del rischio si rimanda, peraltro, a titolo esemplificativo alla 'Guida operativa breve per amministratori indipendenti e sindaci' di Assogestioni, novembre 2011.
[23] *Cfr*. Art.7 – Sistema di controllo interno e gestione dei rischi, Criteri applicativi 7.C.4 punto *(a)* del Codice di Autodisciplina.

abbia effettuato un adeguato censimento dei molteplici rischi connessi con l'attività svolta dall'impresa per poi garantire che gli stessi siano parte integrante di un processo strutturato di gestione del rischio.

A tal fine, ancora una volta, si sottolinea che il Modello ERM rispetto al precedente Modello *CoSO* presenta un'ampia focalizzazione sul rischio che consente alle relative attività di identificazione e rilevazione di evolvere da una concezione limitata ai soli rischi puri verso una visione più completa che consideri anche i rischi /opportunità potenziali significativamente condizionati dalle scelte strategiche.

In questo senso, il Consiglio di Amministrazione ed il Comitato controllo e rischi dovrebbero prendere visione della tassonomia dei rischi adottata dall'azienda e delle relative fonti per valutare se tale classificazione è coerente con le esigenze di *Risk Management* dell'organizzazione. In particolare, il Comitato controllo e rischi dovrebbe verificare che la classificazione adottata:

- garantisca un livello di dettaglio utile per il management stesso nel processo di valutazione costante dei rischi e dei controlli, tenendo conto della contrapposizione dei ruoli interfunzionali (*cfr*. par. V.4)
- supporti adeguatamente i sistemi di gestione del rischio promuovendo analisi relative alla quantificazione degli impatti ed alla stima delle probabilità utili per il tessuto organizzativo aziendale;

Talvolta, nello sviluppo di una strategia basata sull'identificazione dei rischi, le maggiori difficoltà risiedono nella riluttanza a pensare l'impensabile il che significa prendere in considerazione anche i rischi potenziali; infatti, in molti casi si è restii a considerare l'eventualità di una forte volatilità di mercati, la possibilità di frodi o di attacchi, l'avverarsi di catastrofi naturali o di atti di terrorismo. In questo contesto, il Consiglio di Amministrazione ed il Comitato controllo e rischi possono accrescere il livello di consapevolezza del rischio prevedendo con cadenza almeno annuale dibattiti sulle strategie e sui rischi, durante i quali presentare osservazioni concrete e realistiche e formulare domande sfidanti focalizzate sugli interessi degli azionisti e degli *stakeholder*.

## V.2 Come avviene la valutazione dei rischi in termini di dimensionamento o rilevanza?


Misurare e valutare i rischi che l'organizzazione deve affrontare richiede una adeguata metodologia[24] che consideri il rischio non solo in termini di misura della probabilità e dell'impatto, ma anche in relazione all'intensità della sua correlazione con uno o più obiettivi strategici. A tal motivo, occorre assicurare che i responsabili di tale processo strategico posseggano specifiche competenze ed utilizzino pratiche e procedure operative coerenti con la dimensione, la natura e la complessità aziendale.

In base all'esperienza acquisita dall'azienda, la valutazione del rischio[25] può essere fortemente quantitativa o qualitativa e, in ogni caso, richiede opportune considerazioni in merito a tutte le risorse aziendali correlate al rischio siano esse economiche, finanziarie, fisiche, intellettuali e tecnologiche, così come presuppone l'esame degli andamenti storici delle perdite operative.

In tema di misura, rileva altresì la natura degli elementi di valutazione del rischio; a riguardo si osserva che i fattori di valutazione del rischio ed i relativi sistemi, a garanzia di una misura oggettiva, dovrebbero essere nativamente quantitativi e solo in presenza di un rapporto costi - benefici sbilanciato in termini di onerosità, possono prevedere misurazioni di tipo qualitativo. Inoltre, i sistemi di valutazione dovrebbero tener conto anche di eventi rari ed incerti, non misurabili e non limitarsi a considerare soltanto le serie storiche relative ad eventi imprevedibili ma misurabili.

[24] Con specifico riferimento al settore bancario alla misurazione dei rischi contribuisce anche la determinazione del patrimonio vigilanza e quindi la metodologia è sviluppata sulla base di quanto disposto dal Comitato di Basilea.

[25] Con riferimento al processo di valutazione del rischio si rimanda, peraltro, alla sezione B della 'Guida operativa breve per amministratori indipendenti e sindaci' di Assogestioni, novembre 2011.

Infine, nell'ambito del complesso processo di valutazione dei rischi non si può prescindere dal considerare l'interdipendenza sistemica esistente tra i vari eventi rischiosi secondo la quale, come illustrato nell'immagine riportata di lato, ogni impatto può diventare a sua volta una causa e generare a cascata il c.d. effetto domino.


In definitiva, il Comitato controllo e rischi, al fine valutare in modo appropriato il posizionamento dell'azienda sulla scala di maturità, dovrebbe acquisire dall'Amministratore incaricato di vigilare sul sistema di controllo e di gestione dei rischi, informazioni circostanziate in merito a:

- la completezza della mappatura dei rischi di riferimento;
- le modalità qualitative e/o quantitative di misurazione dei rischi stessi;
- la conoscenza del grado di interdipendenza sistemica tra rischi differenti.

## V.3 Come viene definito il 'profilo di rischio'?

Il Codice di Autodisciplina, nell'ambito delle sue prescrizioni, suggerisce al Consiglio di Amministrazione di valutare l'adeguatezza del sistema di gestione dei rischi unitamente al 'profilo di rischio assunto'[26]dall'azienda; ora la definizione di profilo di rischio[27] lascia sul terreno molti dubbi interpretativi che esamineremo nel prosieguo della trattazione.

Considerando quanto sopra esposto nell'ambito dell'identificazione dei rischi pertinenti all'attività d'impresa, il profilo di rischio e la sua misurazione si completano con la definizione di propensione e di tolleranza.

La nozione di propensione al rischio è parte integrante del termine anglosassone '*risk appetite*' e fa riferimento, in particolare, all'insieme dei rischi assunti, che l'organizzazione è disposta a sopportare in via residuale per il raggiungimento degli obiettivi di crescita del valore aziendale, dopo aver disposto adeguati presidi di prevenzione e controllo a fronte dei singoli rischi; pertanto, la propensione al rischio è strettamente connessa con le priorità stabilite dagli obiettivi strategici.

Il concetto di tolleranza (*risk tolerance*) invece riguarda perlopiù gli orientamenti seguiti dall'azienda nella valutazione dei rischi indipendentemente dal sistema di controllo interno, pertanto si può dire che rappresenta la capacità dell'azienda di sopportare il rischio in funzione di specifici risultati economici/finanziari.

Il Consiglio di Amministrazione nell'ambito dell'approvazione del piano strategico evidenzia gli obiettivi dell'azienda ponendoli in correlazione con la propensione al rischio dichiarata. A titolo esemplificativo, tale approccio è rappresentato nella tabella che segue.

[26] *Cfr*. Art.7 – Sistema di controllo interno e gestione dei rischi, Criteri applicativi 7.C.1 punto *(b)* del Codice di Autodisciplina.
[27] In generale, per profilo di rischio si intende l'attitudine più o meno pronunciata dell'azienda ad assumere rischi legati all'attività di impresa e non solo.

| Obiettivi | Rischi | Propensione al Rischio |
|---|---|---|
| Incremento della quota di mercato | Concorrenza | Politica aggressiva in termini di *pricing*, campagne commerciali ecc. senza raggiungere livelli di *dumping*. |
| Stabilità portafoglio clientela | Clienti | Politica di *retaining* di media rischiosità in termini di riduzione dei ricavi volta a bilanciare la qualità del prodotto rispetto ai costi di post vendita e di produzione. |
| *Compliance* normativa | Leggi e regolamentazione | Massimo rispetto degli *standard* al fine di minimizzare il rischio di sanzioni e attenta valutazione degli impatti reputazionali. |
| Ricerca e Sviluppo | Evoluzione tecnologia | Approccio mediamente rischioso in termini di riduzione dei costi di investimento, in coerenza con un posizionamento non *leader* nel settore tecnologico. |
| Copertura da rischi finanziari | Processi finanziari | Approccio prudente con eliminazione dei rischi speculativi. |

Inoltre, la propensione al rischio è strettamente legata ai valori diffusi all'interno dell'organizzazione ed alle aspettative degli azionisti e/o degli *stakeholder*. A tal proposito, è importante che il Consiglio di Amministrazione e il management sviluppino in merito alla propensione e alla tolleranza al rischio una visione comune al fine di bilanciare opportunamente le due esigenze di protezione e creazione di valore.

In generale, si osserva che i settori industriali che richiedono investimenti senza alcuna garanzia di ritorno sono costituiti da imprese ad alto rischio e le organizzazioni con un'alta propensione al rischio perseguono investimenti che possono rivelarsi molto profittevoli ma che in caso di fallimento non consentono neanche di recuperare i costi già sostenuti. Viceversa le organizzazioni con bassa propensione per il rischio si propongono di preservare il valore del capitale e perseguono una crescita più graduale.

La capacità di assumere rischi è legata anche alla situazione finanziaria dell'organizzazione e all'entità degli investimenti in iniziative analoghe; ad esempio, una società fortemente indebitata con un limitato capitale di esercizio, perseguendo una strategia di crescita veloce, potrebbe superare facilmente il livello di tolleranza del rischio. In tali circostanze, è opportuno per il Consiglio di Amministrazione, almeno nel breve periodo, riconsiderare la direzione strategica della società moderando l'esposizione al rischio in relazione alla situazione contingente. Invece, una società che finanzia la sua crescita con la liquidità generata dalla gestione della sua attività operativa, può avere una maggiore capacità di assumersi i rischi della sua crescita strategica.

Infine, si rileva che recentemente ed in particolar modo nei processi di pianificazione strategica, per determinare l'esposizione al rischio, si tiene conto in modo esplicito della relativa propensione e della capacità dell'impresa di utilizzare tecniche come l'analisi di sensitività.

## V.4 Il processo di gestione del rischio è integrato nel sistema organizzativo aziendale?


L'Amministratore incaricato di vigilare sul sistema di controllo e di gestione dei rischi ne cura la progettazione e la realizzazione in termini di adeguatezza ed efficacia[28]; in questo senso, tenendo conto delle linee di indirizzo elaborate dal Consiglio di Amministrazione:

- favorisce lo sviluppo di un sistema organizzativo teso ad una gestione integrata dei rischi a tutti i livelli mediante un'adeguata supervisione sul processo di pianificazione strategica;
- assicura che la pianificazione strategica tenga nella giusta considerazione l'attività di identificazione e misurazione dei rischi interni ed esterni e presenti sia gli scenari favorevoli sia quelli meno vantaggiosi.

In tale ambito, le valutazioni relative al rischio sono espresse in termini di potenziali minacce, di punti di forza e di debolezza del sistema ma anche in termini di eventuali opportunità che, se connesse con obiettivi strategici, possono concretamente influenzare la propensione al rischio (*risk appetite*) della organizzazione stessa.

L'integrazione tra le attività connesse con la gestione del rischio - incluse le previsioni e le assunzioni formulate dal management - e quelle legate allo sviluppo ed all'attuazione del piano strategico trova un importante momento di sintesi nei documenti di pianificazione e budget.

Al fine di assicurare un corretto coordinamento del processo di gestione del rischio, le aziende operanti soprattutto nel settore finanziario prevedono l'istituzione di un *Risk Officer*[29] che sostiene il coordinamento tra i processi di *risk management* e quelli di pianificazione. In altri assetti organizzativi, invece, all'interno della funzione di pianificazione strategica, è previsto l'inserimento di un *Risk Manager*. In ogni caso, ciascuna unità di business ha un chiaro ruolo nella gestione del rischio, pertanto, le funzioni appena nominate non possono eliminare la responsabilità dei manager e dei relativi collaboratori che presidiano i vari processi aziendali.

Per quanto detto, i Responsabili delle divisioni di business, considerando anche i propri obiettivi di performance, forniscono un importante contributo alle attività di pianificazione strategica ed operativa nell'individuazione dei rischi - opportunità connessi al business aziendale, nella definizione del livello di risorse necessarie per la gestione dei rischi stessi e nella formulazione di opportuni indicatori sia nella fase di pianificazione che in quella strategica - operativa.


A tal riguardo, come si è accennato in precedenza, è importante evidenziare la distinzione tra il soggetto che subisce il rischio (*risk subject*), il soggetto che ne è responsabile (*risk owner*), e colui che detiene le leve di governo (*control owner*). Nell'immagine, riportata di lato a titolo di esempio, è facile comprendere i differenti ruoli ricoperti dalle tre figure: il direttore acquisti ha il compito di selezionare i fornitori che garantiscano un adeguato livello di qualità, il direttore di produzione subisce l'eventuale scarsa qualità delle materie prime ed il direttore commerciale è responsabile del rischio della perdita della clientela in caso di insufficiente qualità del prodotto. Ora il coordinamento tra queste tre figure in tema di rischio può essere assicurato all'interno dell'azienda proprio da una funzione preposta per il *Risk Management,* che dispone delle specifiche competenze.

---

[28] *Cfr*. Art.7 – Sistema di controllo interno e gestione dei rischi, Criteri applicativi 7.C.4 punto *(b)* del Codice di Autodisciplina.

[29] Il *Risk Officer* è responsabile della gestione efficiente ed efficace dei rischi significativi e della valutazione delle opportunità connesse e definisce le modalità di censimento e misurazione dei rischi.

Inoltre, con riguardo al collegamento tra la titolarità del rischio ed il sistema delle deleghe, nelle organizzazioni mature rileva la definizione di *process owner* intesa come soggetto/ funzione a cui è chiaramente attribuita una delega di responsabilità su specifiche aree di rischio.

In merito ai processi di governo del rischio si sottolinea altresì che l'Amministratore incaricato di vigilare sul sistema di controllo e di gestione dei rischi dovrebbe garantire una buona integrazione tra la funzione di *risk management* e quella di pianificazione e *budgeting* ed, in particolare, assicurarsi che le risorse aziendali siano allocate in modo equilibrato e coerente con l'identificazione dei rischi e la loro prioritizzazione. Inoltre, la funzione di Risorse Umane e Organizzazione, il Dirigente Preposto e la funzione di Pianificazione svolgono un ruolo strategico di supporto finalizzato ad un corretto bilanciamento delle diverse esigenze, mentre la funzione Internal Audit assiste l'intero processo con la finalità di identificare eventuali disallineamenti funzionali e facilitarne il corretto indirizzo.

In definitiva, nell'ottica di vigilare in materia di rischi e controlli, il Consiglio di Amministrazione al fine di garantire che il processo di gestione del rischio sia ben integrato con il sistema organizzativo, potrà tenere nella giusta evidenza i seguenti aspetti:

- l'analisi dei rischi esposta nel piano strategico d'impresa;
- l'utilizzo di indicatori di rischio nell'ambito del processo pianificazione e *budgeting* e dell'attività operativa;
- la presenza di un *Risk Manager* che svolga all'interno dell'organizzazione funzioni di coordinamento e disponga di un il quadro completo dei rischi maggiormente significativi;
- la definizione di *Process Owner* e lo sviluppo di un sistema delle deleghe basato anche sulla titolarità ed il dimensionamento del rischio;
- il modello organizzativo redatto ai sensi del D.Lgs. 231/01 con riferimento ai protocolli – procedure aziendali che seppure non specificatamente dedicati alla gestione dei rischi 231, siano integrati nel compendio delle procedure generali dell'azienda.

Giova rilevare, inoltre, che il Consiglio di Amministrazione esercitando un ruolo attivo nel rafforzamento del processo di gestione dei rischi, oltre a garantirne la relativa integrazione nel tessuto organizzativo dell'azienda, promuove in modo proattivo uno stile manageriale improntato a comportamenti etici, consapevoli e responsabili. In questo senso, il Consiglio di Amministrazione e/o il Comitato controllo e rischi verificano le iniziative volte a promuovere la cultura del *risk management* e l'Amministratore deputato alla vigilanza sul sistema di controllo e di gestione dei rischi, monitora e relaziona in merito ad eventuali specifiche iniziative rivolte a:

- la comunicazione di principi e valori in tema di rischio estesa ad ambiti più ampi rispetto a quelli disciplinati dal D.Lgs. 231/01;
- la promozione di progetti finalizzati alla formazione ed all'addestramento;
- l'avvio di processi di autodiagnosi guidati dalla funzione di Internal Audit oppure da altra funzione preposta al monitoraggio dei rischi.

In merito alla diffusione dei principi in tema di rischio, il processo di comunicazione dovrebbe essere volto a trasmettere tra i dipendenti le informazioni relative a politiche e linee guida sulla gestione dei rischi stessi ed a rafforzare l'approccio che considera il rischio d'impresa parte integrante delle operazioni giornaliere e non un fattore da considerare separatamente. In questo senso, è di fondamentale importanza che il Consiglio d'Amministrazione, la dirigenza e gli stessi dipendenti dell'azienda, abbiano maturato una interpretazione univoca e condivisa di ciò che il termine rischio significa, anche in termini di responsabilità individuali.

Per quanto attiene alla formazione, si sottolinea l'importanza di programmi finalizzati ad accrescere a livello aziendale la conoscenza e la consapevolezza dei rischi; infine, con riguardo ai processi di autodiagnosi, il *self*

*assessment* che svolge il Consiglio di Amministrazione con cadenza annuale[30] deve tenere nella opportuna considerazione gli eventuali processi di auto valutazione aziendale. Infatti, la consapevolezza e la cultura del rischio nelle unità operative e nelle funzioni aziendali può essere regolarmente monitorata utilizzando varie tecniche: analisi svolte dall'Internal Audit, incontri di autovalutazione (*control self assessment*) e/o invio di questionari ai dipendenti.


## V.5 Su quali flussi informativi si basa l'attività del Comitato controllo e rischi al fine di monitorare l'evoluzione dei rischi?

In linea generale, i temi relativi alle analisi ed alle rendicontazioni in materia di rischi emergenti sono trattati nelle riunioni del Consiglio di Amministrazione unitamente agli aspetti connessi alle strategie aziendali.

Il Comitato controllo e rischi deve monitorare i punti da trattare all'ordine del giorno nelle riunioni del Consiglio di Amministrazione, avendo cura di osservare che gli stessi, anche con il supporto di eventuali Comitati, riguardino:

- eventi o evoluzioni di scenario con impatto sul piano strategico, sui principali rischi aziendali e sull'effettiva validità delle ipotesi sottostanti;
- rischi operativi specifici, con il supporto dei dirigenti responsabili di alcune funzioni aziendali o di controlli di secondo livello;
- eventuali emergenze prevedibili quali: la perdita improvvisa di un membro dell'Alta Direzione, il ritiro dal mercato di un prodotto, il guasto di un importante impianto produttivo, un disastro naturale o un atto di terrorismo;
- operazioni societarie quali fusioni, acquisizioni, disinvestimenti o introduzione di nuovi prodotti e cambiamenti importanti nei processi;
- eventi significativi emersi nel corso di interventi di Internal Audit o problematiche evidenziate dalla società di revisione.

L'Alta Direzione, dal canto suo, fornisce informazioni tempestive al Comitato controllo e rischi e al Consiglio di Amministrazione in generale in merito a:

- qualsiasi evento che abbia significative implicazioni finanziarie o possa danneggiare la reputazione dell'organizzazione, causando, ad esempio, gravi lesioni o incidenti mortali;
- sospetti di gravi violazioni del codice di condotta.

Il Comitato controllo e rischi deve garantire che il Consiglio di Amministrazione e i suoi Comitati abbiano redatto adeguate politiche e procedure in materia di *governance* e che le stesse analizzino anche il tema del rischio e le sue evoluzioni. Peraltro, qualora il Consiglio di Amministrazione decida di delegare specifiche responsabilità relative ai rischi ad alcuni Comitati, essi sono tenuti a condividere le loro attività con il Consiglio stesso oppure con il Comitato controllo e rischi che a sua volta relaziona al Consiglio almeno una volta l'anno in sede di riunione plenaria.

Il Consiglio di Amministrazione al fine di stabilire, le priorità nei flussi informativi e determinare l'ambito, la profondità e la tempistica del suo coinvolgimento nel processo di gestione del rischio, prende in considerazione:

- la natura e lo stato dell'organizzazione, la tipologia del business, il posizionamento dell'impresa sulla c.d. scala di maturità dell'implementazione dei processi di *risk management*;

[30] *Cfr*. Art.1 – Ruolo del Consiglio di Amministrazione, Criteri applicativi 1.C.1 punto *(g)* del Codice di Autodisciplina.

- il livello di esperienza dell'Amministratore incaricato di vigilare sul sistema di controllo e di gestione dei rischi e dell'Amministratore Delegato;
- il grado e la velocità di cambiamento del settore industriale e di altri rilevanti fattori esterni;
- la misura con cui l'organizzazione richiede revisioni della propria strategia per cogliere opportunità emergenti e/o rispondere a possibili rischi;
- l'efficacia delle strutture e dei processi che il Consiglio di Amministrazione ha già stabilito.

## VI. - L'efficacia e l'efficienza del sistema di controllo interno

Il modello delle 'Tre Linee di Difesa' recepito sostanzialmente anche dal Codice di Autodisciplina[31], seppure sia un valido riferimento, adottato anche a livello internazionale[32], si presta talvolta ad interpretazioni poco precise in merito al sistema di controllo che è descritto come un insieme di attori e non come un sistema integrato di mezzi. Tale sistema, infatti, costituito da risorse, tecnologie, strumenti e competenze, rappresenta la rete dei presidi volti ad assicurare, per ciascun processo, il raggiungimento degli obiettivi di controllo in risposta alle politiche di *risk management*.

In considerazione di tali aspetti, è opportuno che gli Amministratori acquisiscano informazioni di dettaglio in merito:

- al funzionamento dell'assetto organizzativo in termini di adeguata responsabilizzazione di ogni livello di *process ownership* previsto nel sistema delle deleghe;
- all'impianto di politiche e procedure ed al relativo funzionamento;
- ai risultati di audit in termini di difettosità e raccomandazioni relative al sistema di controllo.

Ciascuno di questi temi sarà approfondito nel prosieguo mediante la formulazione di interrogativi, indirizzi e riflessioni strategiche. Inoltre, i primi due punti sono anche oggetto di valutazione nell'ambito della scala di maturità presentata nel paragrafo III ed illustrata, nelle sue articolazioni, nell'Appendice 1.

### VI.1 In che modo il *top management* dimostra una solida cultura di controllo?

L'ambiente interno e la cultura del controllo sono elementi fondamentali per il funzionamento complessivo del sistema di controllo e possono essere misurati dai seguenti fattori:


- le iniziative ed i comportamenti che favoriscono una adeguata cultura del controllo parte integrante dell'ambiente interno nel modello ERM;
- l'intensità dei programmi di formazione dedicati alle tematiche di controllo interno;
- l'efficacia delle azioni disciplinari adottate in caso di comportamenti non conformi posti in essere da dipendenti o a seguito di eventi illeciti;
- le riunioni tenute dal top management per l'esame dei risultati di audit;

[31] *Cfr*. Art.7 Sistema di controllo interno e di gestione dei rischi, Commento del Codice di Autodisciplina. In particolare, il modello delle 'Tre Linee di Difesa' prevede i seguenti livelli di controllo: controlli di linea, controlli di monitoraggio di secondo livello e *assurance* fornita dalla terza linea indipendente. A riguardo, *cfr. par*. VII.4 del testo.

[32] Di recente pubblicazione anche da parte dell' Institute of Internal Auditors un position paper sull'argomento, The Three Lines of Defense in Effective Risk Management and Control, gennaio 2013.

- il livello di divulgazione del codice etico e di comportamento a tutti i dipendenti unitamente a programmi di sensibilizzazione;
- il livello di applicazione del codice etico alla gestione di fornitori e partner;
- la presenza di una politica e di un sistema di segnalazione c.d.'*whistleblowing*'[33];
- la presenza di iniziative di *survey* dei clienti e dei fornitori.

A tal riguardo giova rilevare che il 'Modello Organizzativo 231' appartiene al sistema di controllo interno in quanto parte integrante dell'assetto procedurale e di controllo dell'impresa ed è senz'altro un elemento fondamentale per consolidare la cultura etica; tuttavia, l'efficacia del modello stesso è supportata dall'azione di comunicazione dei valori svolta nel continuo e dall'efficacia dei sistemi incentivanti e/o disciplinari.

Si sottolinea infine, che il fattore umano ed i relativi rischi correlati di carattere etico o di conformità, influenzano l'ambiente interno di cui nell'organizzazione si può testare il clima a livello di:

- vertice e *top* management nel processo di trasmissione di valori aziendali e promozione di iniziative di carattere etico, di comunicazione e condivisione, ecc;
- *middle* - management e personale operativo nel monitoraggio di alcuni indicatori di criticità della cultura del controllo (per es. l'assenteismo);
- implementazione di procedure per la gestione delle informazioni (soprattutto quelle riservate);
- articolazione delle mappe di competenze e di valutazione del personale.

Tuttavia, quando si discute di cultura del controllo e degli elementi connessi alla gestione delle Risorse Umane, l'aspetto che forse non è sufficientemente enfatizzato si riferisce proprio alle modalità di selezione, formazione e gestione adottate dalla funzione Risorse Umane che dovrebbero considerare gli aspetti di etica del personale tra le competenze fondamentali oggetto di valutazione delle risorse stesse.

## VI.2 Il sistema delle deleghe, nei ruoli e nelle responsabilità, favorisce il sistema di controllo?

Il Consiglio di Amministrazione attribuisce deleghe di poteri agli Amministratori ed al top management sulla base della importanza e della tipologia delle operazioni gestite; mentre le deleghe di autorità a livelli più operativi possono essere evidenziate nelle procedure aziendali e in documenti separati.

In ogni caso, Il sistema delle deleghe non può prescindere dai controlli e dall'esame delle transazioni contabili su cui approvare operazioni con impatto finanziario/economico maggiore o minore rispetto a quanto pianificato. Rileva, peraltro, che la valutazione da parte degli Amministratori sulla correttezza della pianificazione delle spese e sulla precisazione dei relativi limiti, può implicare il coinvolgimento delle seguenti funzioni/ soggetti: Affari Legali e Societari, Risorse Umane, consulenti esterni, Dirigente Preposto e Internal Audit; quest'ultima con il ruolo di identificare eventuali disallineamenti.

In generale, alcuni principi fondamentali dovranno essere tenuti in considerazione nell'impostazione organizzativa delle deleghe e nella definizione delle responsabilità; in particolare:

- un'adeguata separazione di ruoli tra la gestione finanziaria, l'esecuzione o supervisione operativa, la gestione fisica dei beni e la gestione contabile;
- l'evidenza delle specifiche situazioni in cui il top management o il vertice aziendale possono superare le decisioni del management operativo senza seguire un'altra modalità di controllo compensativo (c.d. *management override*);

[33] Si fa riferimento alla pratica aziendale secondo la quale un soggetto durante l'attività lavorativa aziendale rileva e denuncia pubblicamente attività illecite.

- lo sviluppo di una mappa organizzativa formale che preveda anche la descrizione dei ruoli e sia regolarmente aggiornata nonché facilmente consultabile.

## VI.3 L'insieme delle politiche/ procedure è adeguato al fine di supportare il sistema dei controlli ed il *risk management*?


Le politiche, definite per consentire il raggiungimento degli obiettivi aziendali, sono i principi, le regole ed i controlli di cui l'organizzazione si è dotata. Le procedure sono declinazioni delle politiche, metodi usati nelle attività quotidiane che forniscono indicazioni operative dettagliate. Dunque, in termini di un modello di input-output le procedure sono sostanzialmente processi e devono essere conformi alle politiche adottate dalla organizzazione.

In ragione di quanto detto, per valutare l'adeguatezza delle procedure aziendali in termini di supporto al sistema di controllo e gestione dei rischi, è necessario che il Comitato controllo e rischi s'interroghi su alcune questioni prodromiche:

- quante attività aziendali possono essere effettivamente proceduralizzate;
- quali attività devono essere proceduralizzate in termini di priorità;
- le attività aziendali già proceduralizzate coprono le esigenze di regolamentazione interna ed esterna;
- in che misura le attività proceduralizzate sono sostenibili in termini di fattibilità, considerando gli eventuali vincoli tecnici ed economici;
- le procedure già attive sono di facile applicazione ed utilizzo.

Quanto premesso lascia intendere che la redazione e l'emissione di politiche e procedure per la copertura dei rischi aziendali più significativi è un'attività importante il cui coordinamento può essere affidato ad un unico ente, per esempio alla funzione Risorse Umane, che al fine di garantire la diffusione dei documenti e facilitarne la consultazione, utilizza specifiche metodologie e si avvale di sistemi tecnologici di supporto. Diversamente, le politiche e le procedure possono essere predisposte da più di una funzione o unità di business aziendale e, in tal caso, è opportuno che il Comitato controllo e rischi si accerti della strategia globale adottata per garantirne il corretto sviluppo. Inoltre, la tempestività degli aggiornamenti nelle procedure è importante quanto la loro definizione ed anche su tale aspetto il Comitato controllo e rischi, con il supporto delle funzioni di controllo, deve vigilare.

L'emissione delle procedure spesso comporta la contestuale programmazione di interventi formativi volti ad assicurare che, nell'ambito di ciascuna fase procedurale, ogni dipendente abbia adeguate conoscenze per svolgere il proprio ruolo.

Come si è già detto, le procedure redatte ai sensi del D.Lgs. 231/01 costituiscono un elemento basilare del sistema di controllo e dovrebbero costituire parte integrante dell'assetto procedurale aziendale. Tuttavia, talvolta tali procedure, a causa della necessità di accelerare la formalizzazione di quanto richiesto dal modello stesso ed in assenza di norme precise, nascono attraverso un processo autonomo che sfugge all'impianto procedurale aziendale. Il risultato di tale approccio è la presenza di procedure poco diffuse all'interno dell'organizzazione e spesso non aggiornate. A tal motivo, il Comitato controllo e rischi, nell'ottica di promuovere maggiore efficienza ed efficacia, dovrebbe approfondire il livello di integrazione dei sistemi.

Infine, con riferimento al disegno dei controlli interni si rileva che lo stesso dovrebbe essere, in linea generale, trasversale ai processi aziendali; pertanto, nelle organizzazioni di una certa dimensione, la funzione Risorse Umane o le funzioni di business sviluppano un'analisi interfunzionale che supporta il

modello di business ed i processi trasversali con l'obiettivo di garantire l'efficienza dei controlli e fornire le informazioni di base per la valutazione del rischio dell'interno del processo. Anche in questo contesto, il Comitato controllo e rischi, nell'ambito della sua attività di supervisione, può richiedere degli incontri mirati sugli aspetti organizzativi di tali processi.

## VI.4 Le informazioni necessarie per le decisioni e le attività di controllo sono disponibili in modo tempestivo e affidabile?


Gli Amministratori prima di valutare la disponibilità, la tempestività e l'affidabilità delle informazioni, dovrebbero verificarne l'esistenza e la fruibilità soprattutto con specifico riferimento alle informazioni qualitative di per sé poco strutturabili per il *reporting*.

Tutto ciò premesso, l'adeguatezza del processo di *reporting* non solo di carattere gestionale e finanziario ma anche per gli aspetti strategico operativi e commerciali, dipende molto dal livello di integrazione dei sistemi informativi, pertanto al riguardo il Comitato controllo e rischi deve essere informato dal relativo Responsabile.

Inoltre, il Comitato controllo e rischi può organizzare riunioni in merito alla gestione delle principali informazioni e dei relativi flussi di comunicazione all'interno dell'organizzazione; in tale contesto, per coordinare e sostenere un r*eporting* tempestivo e affidabile, è importante focalizzarsi sul ruolo svolto dalla funzione preposta al controllo di gestione ed al budgeting.

Una reportistica standard e non personalizzata nella tempistica e nei contenuti, prodotta da una funzione manageriale o da una funzione di controllo di secondo livello, rende finanche inefficace i controlli previsti per mitigare i rischi. Tale problematica può facilmente sfuggire al Comitato controllo e rischi mentre spesso emerge attraverso interventi di *self-assessment* condotti, in qualità di facilitatore, dalla funzione Internal Audit o da altra funzione indipendente che contribuisce appunto a valutare la maturità e l'adeguatezza del processo di comunicazione.

La comunicazione, l'informazione e l'informatizzazione costituiscono oggetto di valutazione anche nelle matrici della scala di maturità dove a livello 4[34] l'ottimizzazione dei sistemi evolve, attraverso l'integrazione, verso modelli di *governance* informatizzati e verso la declinazione personalizzata delle informazioni in base alle specifiche esigenze dei vari *stakeholder*.

## VI.5 Le attività di controllo interno sono definite in modo coerente con gli obiettivi dell'organizzazione e con gli aspetti connessi alla gestione del rischio?

Come si è già detto nel paragrafo IV, l'esplicita declinazione degli obiettivi in coerenza con i processi aziendali, consente un corretto bilanciamento dei controlli. Un esempio tipico di non corretto bilanciamento si può rintracciare nel processo di approvvigionamento dove la funzione acquisti pone maggiore priorità sul contenimento dei costi, mentre la funzione amministrativa valuta maggiormente l'accuratezza contabile; da tale disallineamento organizzativo si genera un processo poco tempestivo con impatti sulla soddisfazione del cliente.

Pertanto, risulta evidente che il Comitato controllo e rischi non può limitare il suo intervento a meri controlli di conformità o di bilancio, mentre è auspicabile che approfondisca, con approccio integrato e tramite l'Internal Auditing, la coerenza tra i controlli interni ed i diversi obiettivi di business e di *governance*, verificando peraltro l'effettiva copertura dei rischi identificati mediante le diverse strategie di risposta.

[34] *Cfr*. Appendice 1 -Matrice della scala di maturità dell'azienda in ambito di governance interno, tabella D.

## VI.6 In che modo sono monitorate le iniziative di miglioramento del *management* in risposta alle osservazioni dell'Internal Audit?

Il Consiglio di Amministrazione, il Comitato controllo e rischi ed il management evincono dalle relazioni della funzione Internal Audit il livello di funzionalità e affidabilità del sistema di controllo interno.

I Report dell'Internal Audit possono apportare veramente valore aggiunto all'azienda se i manager affrontano le problematiche, individuate nel corso delle attività di audit, condividendo decisioni consapevoli nell'accettazione dei rischi. Inoltre, un esplicito supporto alle attività di internal auditing promosso dall'Amministratore Delegato e dal Comitato controllo e rischi può contribuire a garantire il progressivo miglioramento del sistema di controllo.

I manager di linea, dal canto loro, devono acquisire informazioni in merito agli esiti delle attività di controllo interno e predisporre, prima o subito dopo l'emissione della relazione di audit, piani d'azione congrui, corredati delle tempistiche per l'attuazione delle stesse iniziative e assumersi, nel contempo, la responsabilità di monitorare e controllare la corretta implementazione di ciascuna azione correttiva. Inoltre, il responsabile della funzione di Internal Audit al fine di garantire l'effettiva realizzazione delle azioni pianificate gestisce un processo formale di *follow-up*.

Per quanto detto, uno degli strumenti utili per misurare il miglioramento continuo del sistema di controllo interno è il monitoraggio che in base al modello delle 'Tre Linee di Difesa', in qualità di controllo di secondo livello, si caratterizza per avere una gestione trasversale interfunzionale tra aree di responsabilità interdipendenti ma non necessariamente coordinate. In questo senso, la funzione di Audit, valutando l'efficacia dell'intero sistema dei controlli persegue anche l'efficienza complessiva del sistema, bilanciando le interrelazioni tra gli attori deputati all'esercizio del controllo.

Nel caso in cui il management ritenga di non dover adottare dei provvedimenti a fronte di rilievi presentati dalla funzione di Audit, la decisione di accettare il relativo rischio deve essere approvata ad un livello adeguato. Periodicamente infatti, il senior management, il Direttore Finanziario e l'Amministratore Delegato, nell'ambito del processo di *risk management*, analizzano le raccomandazioni ad alto rischio emerse dagli interventi di audit. Inoltre, in quest'ottica, l'Amministratore Delegato si riunisce periodicamente con il responsabile della funzione di Internal Audit per esaminare le relazioni e le raccomandazioni di audit in sospeso e raccogliere pareri su rischi e controlli. Infine, anche il Comitato controllo e rischi riceve dalla funzione di Audit, su aspetti non ancora affrontati dal management, periodiche relazioni in merito a raccomandazioni ad alto rischio di audit.

## VII - L'adeguatezza della funzione di Internal Audit

L'Internal Audit, per sua natura e missione, svolge un'attività finalizzata a fornire *assurance*[35] in merito all'adeguatezza complessiva del sistema di *governance* interno ed, in particolare, al grado con cui l'ambiente di controllo sostiene e promuove la realizzazione degli obiettivi aziendali. In questo senso, la funzione di Audit si interfaccia con tutte le dimensioni che compongono il modello *Enterprise Risk Management*, di cui si è parlato nei paragrafi precedenti, e con le relative interrelazioni.

Per quanto detto, una condizione necessaria per l'esercizio di una vigilanza completa ed efficace sul sistema di governo interno, è la presenza di un'attività indipendente di *assurance* sia per quanto riguarda l'architettura del sistema di controllo che per il suo effettivo funzionamento[36]; tale *assurance* integra le responsabilità primarie operative presenti ai vari livelli e garantisce la gestione del rischio globale, uniforme

[35] Per *assurance* si intende l'attività di valutazione oggettiva e indipendente svolta a supporto delle responsabilità di sorveglianza e vigilanza proprie del Consiglio di Amministrazione, dei suoi Comitati e del Collegio Sindacale.

[36] *Cfr*. Art.7 – Sistema di controllo interno e gestione dei rischi, Principi 7.P.3 punto *(b)* del Codice di Autodisciplina dove si precisa che il Responsabile della funzione Internal Audit verifica il funzionamento e l'adeguatezza del sistema di controllo interno e di gestione dei rischi.

ed efficiente, il livello di controllo interno e l'esercizio della *governance*. Da ciò si evince che se la funzione di Internal Audit non è stata istituita, è opportuno che il Consiglio di Amministrazione, tenendo conto delle proprie esigenze di *assurance,* rivaluti almeno con cadenza annuale tale scelta.

Il Comitato controllo e rischi e il Collegio Sindacale, nei rispettivi ruoli di supervisione e vigilanza, dovrebbero approfondire alcuni aspetti relativi alla *mission* della funzione di audit ed in particolare verificare che l'attività di audit sia svolta in modo corretto, completo ed efficiente.

Se l'Internal Audit opera nel rispetto di tali criteri, è ragionevole sostenere che l'*assurance* fornita potrà apportare un forte impulso al miglioramento continuo della *governance* d'impresa, sostenere gli organi sociali mediante il supporto di fonti appropriate e garantire un completo, adeguato ed efficiente flusso di informazioni sulla gestione del rischio. In questo senso, l'Internal Audit sarà in grado di:

- valutare la coerenza tra gli obiettivi strategici e le attività operative, svolgendo analisi approfondite su eventuali disallineamenti;
- fornire supervisione sull'adeguatezza del sistema di identificazione, di misurazione e di gestione dei rischi;
- formulare una valutazione complessiva del sistema di controllo interno, in base ad un approccio sistematico e una copertura progressiva, garantendo criteri coerenti;
- favorire lo sviluppo di una maggiore efficacia nell'attività della 'prima e della seconda linea di difesa';
- esprimere pareri indipendenti su potenziali conflitti di interessi emergenti ai vari livelli operativi.

## VII.1 L'attività di Audit è svolta in modo corretto?


In linea generale, il Comitato controllo e rischi deve accertarsi che, coerentemente con quanto previsto dagli standard professionali internazionali, il mandato della funzione di Audit sia approvato dal Consiglio di Amministrazione. Tale mandato deve attribuire all'Internal Audit un livello adeguato di autorità al fine di garantire l'indipendenza e l'obiettività necessaria per lo svolgimento della sua *mission;* inoltre, chiarisce il suo ruolo nell'attività di *assurance* sulla adeguatezza complessiva del sistema controllo interno e della gestione dei rischi.

L'*Institute of Internal Auditors* (IIA) ha messo a punto una definizione di internal auditing[37] che, superando ampiamente il ruolo ispettivo attribuitole in passato, può essere utilmente consultata per illustrare l'incarico della funzione di Audit all'interno del proprio mandato. In passato infatti, la funzione di Audit era considerata come l'organo deputato al mero controllo della conformità delle attività operative aziendali rispetto alle politiche ed alle procedure interne, finalità raggiunta, peraltro, anche mediante attività di prevenzione e di individuazione di frodi e/o errori.

Attualmente, invece, le funzioni di Internal Audit affrontano in modo più ampio gli aspetti connessi al sistema di controllo interno svolgendo anche attività di supporto di tipo *advisory* al management; di qui l'importanza di chiarire l'ampiezza del ruolo ricoperto da tale funzione di controllo nell'ambito del proprio mandato.

Nel mandato di audit deve essere enfatizzato, inoltre, che tra il Comitato controllo e rischi e la funzione di Internal Audit esista una comunicazione diretta ed aperta; in questo senso, è sottolineata l'importanza del

[37] L'internal auditing è un'attività indipendente ed obiettiva di *assurance* e consulenza, finalizzata al miglioramento dell'efficacia e dell'efficienza dell'organizzazione; assiste l'organizzazione nel perseguimento dei propri obiettivi tramite un approccio professionale sistematico, che genera valore aggiunto, in quanto finalizzato a valutare e migliorare i processi di controllo, di gestione dei rischi e di corporate governance (*Cfr*. Standard Professionali IIA).

ruolo ricoperto dal Comitato controllo e rischi al fine di assicurare una vigilanza efficace sul quadro complessivo dei controlli interni e dei rischi. In particolare, il mandato dovrebbe comprendere precise disposizioni in merito a:

- la nomina del Responsabile Internal Audit in linea con quanto definito dal Codice di Autodisciplina[38];
- il completo accesso alle informazioni anche mediante il supporto di personale appropriato nel corso dello svolgimento di incarichi di audit;
- l'impossibilità di assumere responsabilità operative da parte dell'Internal Audit o svolgere funzioni che potrebbero ricondursi ad ambiti oggetto di successivi interventi di audit;
- i rapporti esistenti tra l'Internal Audit e gli altri organi o funzioni aziendali, al fine di consentire una corretta comunicazione senza compromettere l'indipendenza della stessa funzione di Audit;
- l'approvazione del piano di audit da parte del Consiglio di Amministrazione basato, in coerenza con il Codice di Autodisciplina[39], su un processo strutturato di analisi e prioritizzazione dei principali rischi;
- la previsione di corrette modalità per l'attivazione di incarichi ritenuti necessari a fronte di eventuali rischi emergenti e avviati su iniziativa del Responsabile di Internal Audit, dell'Amministratore incaricato del sistema di controllo interno e di gestione dei rischi, del Comitato controllo e rischi e/o del Collegio Sindacale, garantendo l'equilibrio delle scelte ritenute prioritarie;
- incontri periodici e riservati tra il Responsabile Internal Audit ed il Comitato controllo e rischi in assenza del management;
- l'ampiezza delle attività di audit in coerenza con le caratteristiche dell'azienda e del gruppo, ovvero con tutti i processi e le funzioni di riferimento;
- ogni forma di limitazione del mandato presentata ed approvata dal Comitato controllo e rischi.

Infine, poiché la comprensione degli obiettivi strategici e di *business* dell'impresa è essenziale per l'efficacia della funzione di Audit, è opportuno che il Responsabile Internal Audit sia invitato a partecipare ad alcuni incontri di pianificazione strategica e ad altre riunioni utili a tale finalità, senza che questo alteri, peraltro, l'indipendenza della funzione.

Si fa presente che l'Associazione Italiana Internal Auditors, anche in ambito del Chief Audit Executive Program, svolge in modo continuo un'attività di benchmarking al fine di individuare best practice di riferimento, pubblicando periodicamente dei paper al riguardo.


### *Monitoraggio della performance svolta dalla funzione di Internal Audit*

Una efficace funzione di Internal Audit è dotata di processi strutturati per valutare la propria performance; in particolare, essa utilizza i risultati di audit ed il parere dei revisori esterni o di altri soggetti interessati, per monitorare le evoluzioni delle problematiche nel tempo e raggiungere un miglioramento continuo nelle proprie prestazioni.

Gli standard professionali emessi dalla *Institute of Internal Auditors* (IIA) richiedono, almeno ogni cinque anni, un controllo della qualità indipendente dalla funzione di Audit. A tal riguardo, il Comitato controllo e rischi dovrebbe accertare che tale valutazione sia stata effettuata

[38] *Cfr*. Art.7 – Sistema di controllo interno e gestione dei rischi, Criteri applicativi 7.C.1 del Codice di Autodisciplina dove si precisa che 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'[…].

[39] *Cfr*. Art.7 – Sistema di controllo interno e gestione dei rischi, Criteri applicativi 7.C.1, punto *(c)* del Codice di Autodisciplina e par. VII.2 per alcuni orientamenti.

e prendere visione dei relativi risultati. L'attività di *Quality Assurance,* secondo quanto previsto dagli standard internazionali, è eseguita da personale competente.

Al fine di confrontare la propria operatività ed efficacia con le altre organizzazioni, l'Internal Audit utilizza anche strumenti di *benchmarking*. In ogni caso, il Responsabile Internal Audit sviluppa per la funzione di audit tecniche di misurazione specifiche della *performance* e le condivide con il Comitato controllo e rischi; si tratta, per esempio, di indagini di *customer satisfaction*, di *post audit debriefing*, di revisioni ed analisi interne di *Quality Assurance* i cui risultati sono, a loro volta, presentati al Comitato controllo e rischi.

### *Modalità di valutazione e di comunicazione dei risultati di audit*

Generalmente i risultati di audit sono comunicati in forma scritta mediante *Audit Report*; tali relazioni fanno riferimento agli obiettivi e all'ambito delle verifiche, alle evidenze di audit ed alle raccomandazioni per il miglioramento del sistema di controllo. I report comprendono commenti e proposte per azioni correttive formulate da parte del management della funzione/processo oggetto di audit.

I report di audit si caratterizzano per essere documenti oggettivi ed equilibrati che illustrano sia le aree di rischio adeguatamente gestite che le carenze osservate; inoltre, in linea di principio, presentano i risultati delle verifiche di audit separatamente dalle raccomandazioni facilitando il processo di comunicazione degli esiti degli interventi e supportando il management nella definizione delle priorità da assegnare alle azione di miglioramento formulate.

Con cadenza prestabilita, il Responsabile Internal Audit fornisce una sintesi delle relazioni di audit al Comitato controllo e rischi e all'Amministratore incaricato del sistema di controllo interno e di gestione dei rischi con un livello di dettaglio coerente con le dimensioni/complessità dell'organizzazione e, comunque, sufficiente a permettere al Comitato controllo e rischi di comprendere le tipologie e le quantità di problematiche di controllo riscontrate nell'attività di audit, nonché le iniziative promosse dal management per poterle risolvere/gestire.

Ad integrazione di tale flusso informativo, il Comitato controllo e rischi, periodicamente, prende anche visione di un *Audit Report* dettagliato al fine di comprenderne ed approfondire l'approccio metodologico e la qualità del processo di reporting.

La metodologia adottata dalla funzione Internal Audit, se evoluta, è in grado di fornire negli *Audit Report* anche una valutazione del sistema di controllo interno applicando un punteggio - giudizio predefinito ai processi/ strutture oggetto di audit; a titolo esemplificativo si riporta la seguente scala di possibili valutazioni:

1. Sistemi di controllo valutati insufficienti, sulla base della significatività delle problematiche riscontrate;
2. Sistemi di controllo valutati non adeguati, soggetti a significativi miglioramenti;
3. Sistemi di controllo valutati complessivamente adeguati, con l'evidenza di alcune aree critiche;
4. Sistemi di controllo valutati complessivamente positivi, con alcune aree di miglioramento;
5. Sistemi di controllo valutati positivi.

Dalla relazione di audit, inoltre, deve emergere che la valutazione del sistema di controllo interno si riferisce al:

- disegno inteso come architettura standard del controllo implementata dal management a presidio di determinati obiettivi di business/governo o di rischi,
- funzionamento dei controlli disegnati e pertanto aspetti riferiti alla mera conformità.

A tale proposito, si sottolinea l'importanza degli indirizzi formulati dall'Associazione Italiana Internal Auditors in merito ad un approccio metodologico professionale che supporta pienamente le attività di valutazione dei sistemi di controllo[40].

[40] *Cfr*. Disegno e funzionamento del Sistema Integrato di Controllo Interno, AIIA, aprile 2008.

## VII.2 L'attività di Audit è svolta in modo completo?

Il Comitato controllo e rischi nell'ambito della sua attività di supervisione, verifica che la funzione di Audit sia in grado di coprire l'universo aziendale dei rischi – controlli ed esprimere una valutazione sul sistema di controllo interno supportata da una adeguata metodologia, da una attività di pianificazione strutturata e da un team di risorse qualificate.

### *Il piano di internal auditing*

Il piano annuale della funzione di Audit è lo strumento fondamentale per mettere in relazione l'attività di internal auditing con le esigenze complessive di valutazione del sistema di controllo interno aziendale; inoltre, consente al Comitato controllo e rischi di verificare che i rischi e le priorità definite siano state adeguatamente considerate. A tal motivo, il piano di audit pur riferito ad un arco temporale di passo annuale, prevede anche una pianificazione strategica di medio termine.

Il Responsabile Internal Audit prepara un piano annuale di audit sulla base dell'analisi dei processi di business dell'organizzazione e dei relativi rischi ad essi associati; inoltre, se un processo di *Enterprise Risk Management* è già in atto, esso costituirà il punto di partenza per il processo di *risk assessment* finalizzato allo sviluppo di un piano di audit in linea con le valutazioni di rischio aziendale.

L'esame dei processi prende le mosse dall'universo di audit che generalmente riguarda i processi interfunzionali piuttosto che le singole funzioni; tuttavia, se è presente all'interno dell'organizzazione un *process model,* esso rappresenterà un valido riferimento per assicurare una pianificazione completa dell'attività di audit.

Il piano di audit deve illustrare i criteri di rischio utilizzati per definire le priorità. Tali criteri possono anche aver riguardo a fattori dimensionali e fattori di rischio qualitativi, tra cui a titolo esemplificativo si evidenzia:

- il contributo dei processi agli obiettivi strategici;
- il contributo dei processi ai risultati economici (*i.e.* ricavi, costi, margini di profitto);
- l'importanza del processo in relazione ad implicazioni legali;
- la rilevanza dell'impatto del processo sui sistemi IT;
- l'esperienza pregressa di audit.

In questo contesto, il Responsabile Internal Audit, nella fase preliminare della preparazione del piano, può consultare sia il management in merito alle evoluzioni di *business* in corso, sia i revisori esterni per acquisire informazioni relative alla attività di certificazione contabile; terrà inoltre conto delle informazioni a disposizione dell'evoluzione dei controlli di secondo livello.

Il Comitato controllo e rischi, dal canto suo, esamina il piano di audit e ne valuta l'adeguatezza in base all'approccio metodologico adottato dal Responsabile di Internal Audit e alla conoscenza del settore. Nel corso dell'esercizio, è compito della funzione Internal Audit monitorare il mantenimento di un equilibrio nel proprio piano di attività, tenendo conto delle richieste intervenute, della copertura dei rischi complessivi aziendali e riferendone al Comitato controllo e rischi qualora dovessero sorgere delle problematiche in merito.

Inoltre, nell'attività di predisposizione del documento programmatico di audit, è importante valutare i processi/attività esclusi dal piano. A tal motivo, il Responsabile Internal Audit deve esplicitare le aree di rischio escluse dal processo di pianificazione di audit, indicando la ragione delle scelte: carenze di competenze specifiche o risorse, ambiti gestiti direttamente dalle funzioni di controllo di secondo livello e oggetto di verifica periodica ecc.. Tale precisazione consente al Comitato controllo e rischi di valutare correttamente i rischi da accettare a seguito dell'esclusione di determinati processi dalle verifiche di audit.

Infine, in ragione della rilevanza del processo e delle responsabilità che ne derivano per gli Amministratori, è opportuno acquisire conoscenze adeguate sulle modalità di pianificazione delle attività di audit e sui criteri di *risk assessment*[41] trattati in diverse pubblicazioni dell'Associazione Italiana Internal Auditors.

### *Le risorse della funzione di audit*

Il dimensionamento della funzione di Internal Audit si basa su un congruo numero di persone qualificate, necessarie in un determinato arco temporale a coprire i principali processi dell'impresa nonché gli interventi attivati per rispondere ad eventuali rischi emergenti (es. sospetti di illecito, ecc).

Le funzioni di Internal Audit sono dotate di personale qualificato con adeguata esperienza nell'analisi dei rischi delle aree di business. Al personale di audit è richiesta, inoltre una formazione continua nelle discipline di loro competenza per rimanere al passo con i progressi tecnologici e con i cambiamenti della struttura organizzativa aziendale.

In linea di principio, le attività di Internal auditing possono essere condotte da:

- risorse *in-house*: la responsabilità delle attività di controllo è assegnata al Dipartimento di Audit oppure alcune attività sono incluse nelle responsabilità dirette delle funzioni di linea (per esempio per rischi legati alla sicurezza fisica o all'ambiente); d'altro canto, la Direzione Internal Audit, in caso di necessità può includere nel proprio organico, personale dotato di competenze specifiche proveniente da altre funzioni;
- risorse in *outsourcing*: una società esterna è incaricata di eseguire il complesso delle attività di controllo normalmente svolte dalla funzione di Internal Audit; in questi casi è tuttavia necessario la presenza di un referente interno qualificato in grado di monitorare e supervisionare il lavoro delle risorse esternalizzate.
- risorse interne ed esterne: attività distinte o progetti possono essere affidati ad una società di consulenza specializzata o uno o più esperti esterni affiancare il personale della funzione di Internal Audit in specifici team.

La funzione di Internal Audit richiede un ampio spettro di competenze e conoscenze; tra le competenze e le qualità più importanti per la professione di internal auditing si può citare la comunicazione, l'ascolto attivo, la persuasione, la *leadership*, il *problem solving*, l'integrità, l'innovazione, la conoscenza del settore economico, l'analisi dei processi ed il *project management*.

Il Responsabile Internal Audit non dovrebbe accettare incarichi se non dispone di personale con le necessarie competenze, ma, come si è detto, in caso di necessità può attingere anche le competenze da altro personale aziendale, coinvolgendo eventualmente esperti esterni o in *outsourcing*.

La competenza del personale applicato presso la funzione di Internal Audit può essere avvalorata anche mediante il conseguimento di alcuni importanti titoli professionali di seguito elencati:

- certificazione professionale internazionale: *Certified Internal Auditor* (CIA);
- certificazioni specialistiche: *Certified Risk Management Assurance* (CRMA), *Certified Information Systems Auditor* (CISA), *Certified Financial Sector Auditor* (CFSA), *Certified Control Self Assessor* (CCSA);
- altri titoli professionali relativi a *risk management*, processi contabili, qualità ecc.

In questo senso, la funzione di Internal Audit promuove lo sviluppo professionale e la certificazione del proprio personale e il Responsabile Internal Audit riferisce periodicamente al Comitato controllo e rischi sulle competenze degli internal auditor, sui titoli accademici e professionali da essi conseguiti e sull'esperienza di audit maturata specificatamente all'interno dell'organizzazione e/o nel settore industriale.

[41] *Cfr*. anche Internal Auditing - Chiave per la Corporate Governance, C. Dittmeier, EGEA, marzo 2011- Capitolo 10: Il piano di internal auditing.

## VII.3 L'attività di Audit è svolta in modo efficiente?

### *Coordinamento ed integrazione[42]: i revisori esterni e la funzione di Internal Audit*

Nell'ambito della rete dei controlli svolti dagli organi che non partecipano alla gestione dell'impresa, è importante sottolineare il ruolo dei revisori esterni[43]; tuttavia essi, ai fini dell'esame e della certificazione del bilancio di periodo, svolgono una attività strettamente limitata alla valutazione dell'ambiente di controllo interno e dei processi contabili afferenti il *financial reporting*.

Il ruolo della funzione Internal Audit è invece più ampio, e coinvolge tutti i processi aziendali per i quali, mediante attività di audit, si fornisce *assurance* al Comitato controllo e rischi ed al Consiglio d'Amministrazione. Pertanto, l'attività di internal auditing garantisce, l'affidabilità della comunicazione interna e dell'informativa che, come rappresentato nell'immagine riportata di lato, è pervasiva e fondamentale per le decisioni strategiche ed operative del Consiglio di Amministrazione e di tutti i livelli aziendali.


L'*assurance* di audit può riguardare aspetti connessi con:

- il reporting finanziario;
- il reporting sui rischi;
- il reporting sui processi operativi;
- i processi operativi alimentanti la contabilità ed il reporting;
- i processi IT che, in ambienti complessi, devono garantire un'adeguata integrazione dei database e dei diversi sistemi.

In ambienti in cui i processi di reporting finanziario non sono dotati di sistemi operativi integrati con i processi di controllo, può accadere che le relazioni finanziarie, predisposte dai revisori esterni e dirette agli azionisti e agli investitori, esprimano pareri positivi mentre il sistema di reporting interno presenti comunque delle debolezze o manchi di tempestività.

A tal motivo, gli standard e le linee guida esistenti sottolineano l'importanza dell'attività di internal auditing anche per i revisori esterni. Infatti, l'*assurance* fornita sull'ambiente di controllo, sui singoli presidi interni e sul *risk management* costituisce una importante base di riferimento per la certificazione contabile rilasciata dai revisori esterni che in tal modo, possono apprezzare i punti di forza dell'organizzazione ed individuare le aree di debolezza che potrebbero avere impatto sui processi di *financial reporting*.

In questo senso, per rafforzare il processo di *assurance*, è auspicabile che il dialogo tra i revisori esterni, il Comitato controllo e rischi e l'Internal Audit, in merito all'attività di audit ed alle relative risultanze, abbia cadenza regolare.

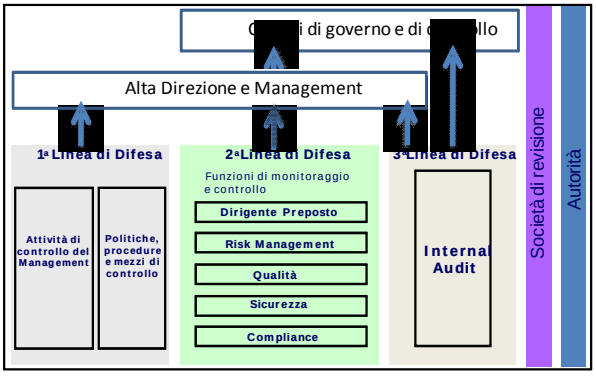
### *Coordinamento ed integrazione: le funzioni aziendali di controllo di secondo livello e l'Internal Audit[44]*

Il Codice di Autodisciplina evidenzia che il sistema di controllo interno e quello di gestione dei rischi devono essere considerati come un sistema unitario ed integrato le cui componenti sono tra loro coordinate in modo interdipendente ed il sistema, nel suo complesso, è inserito nell'assetto organizzativo, amministrativo e

[42] *Cfr*. Corporate Governance Insights, ECIIA, maggio 2012; Making the most of the internal audit function: recommendations for Directors and Board Committees, EcoDa e ECIIA, dicembre 2012.
[43] *Cfr*. Il sistema dei controlli, Nedcommunity, 2005 e *Board evaluation*: regole, principi, *best practice*, Nedcommunity, 2008.
[44] *Cfr*. Corporate Governance Paper, Approccio Integrato al Sistema di Controllo Interno ai fini di un efficace ed efficiente governo d'impresa, AIIA, febbraio 2008.

contabile della società[45].

A tal riguardo, si richiama il modello delle 'Tre Linee di Difesa', a cui si è già fatto cenno nel corso della trattazione, che considera tra le funzioni di controllo di secondo livello:




- il *Risk Management* e la Funzione *Compliance* (prevalenti nel settore finanziario[46]);
- il Dirigente Preposto alla redazione dei documenti contabili societari e le Funzioni aziendali che lo supportano direttamente (es. il Controllo di Gestione);
- le altre funzioni di controllo di secondo livello (es. la Qualità, la Sicurezza, ecc.);
- le altre forme di audit svolte sui sistemi di gestione in base alle normative internazionali (BSI, ISO[47], ecc.); In generale la seconda linea di difesa, presidia il processo di valutazione e controllo dei rischi garantendo la coerenza con gli obiettivi aziendali e rispondendo a criteri di segregazione organizzativa in modo da assicurare un efficace monitoraggio.

L'Internal Audit invece, in qualità di terza linea di difesa, assolve al compito di valutare l'efficacia dell'intero sistema dei controlli, compresi i processi sottoposti a revisione dalle funzioni appartenenti alla seconda linea di difesa; identifica eventuali disallineamenti in ottica di *risk management* e persegue l'obiettivo di efficienza complessiva del sistema, facilitando, peraltro, le interrelazioni tra gli attori deputati all'esercizio del controllo.

In particolare, l'attività di *assurance* condotta dall'Internal Audit in base al piano *risk based* può fornire un importante contributo al Dirigente Preposto in relazione alla responsabilità attribuitagli per la valutazione dell'adeguatezza del sistema di controllo interno in ambito amministrativo-contabile, alla funzione *Risk Management* in merito alla misurazione dell'entità del rischio residuo e alle altre funzioni di controllo nel monitoraggio dell'effettivo funzionamento e dell'adeguatezza dei controlli da loro presidiati.

In tale contesto, il Dirigente Preposto, la funzione di *Compliance* e le altre funzioni di controllo possono rappresentare all'Internal Audit la necessità di specifiche attività di verifica che saranno svolte compatibilmente con i compiti complessivi della funzione.

Nell'ottica dell'efficienza e dell'evoluzione continua dei processi, l'Internal Audit può formulare specifici suggerimenti per le altre funzioni di controllo finalizzati al miglioramento dei presidi. Ad esempio, l'Internal Audit può fornire supporto consulenziale nel corso della definizione delle procedure operative, sviluppate in relazione al rischio di *compliance*, a cui prendono parte il Dirigente Preposto, la funzione *Compliance* e le altre funzioni di controllo.

Sulla base di quanto sopra, l'Internal Audit assicura un idoneo flusso informativo verso il Dirigente Preposto, la funzione *Compliance* e le altre funzioni di controllo di secondo livello; inoltre, acquisisce, nell'ambito del processo di pianificazione di audit ai fini del *risk assessment*, tutti gli elementi di valutazione sulle aree maggiormente a rischio. In particolare, la parte del piano di audit dedicata ai processi contabili, considera i rischi percepiti dal Dirigente Preposto ma deve essere opportunamente bilanciata rispetto all'universo dei processi e dei rischi, favorendo un approccio di audit che consideri la contabilità come parte integrante dell'intera rete dei processi aziendali.

---

[45] *Cfr*. Art.7 – Sistema di controllo interno e gestione dei rischi, Commento del Codice di Autodisciplina.

[46] *Cfr*. Comunicazione congiunta Banca d'Italia - CONSOB dell'8 marzo 2011 in materia di ripartizione delle competenze tra Compliance e Internal Audit nella prestazione dei servizi di investimento e di gestione collettiva del risparmio.

[47] Si fa riferimento a *standard* che assicurano la sicurezza, la qualità, l'affidabilità di beni e servizi e la riduzione dei rischi, emessi da *International Organization for Standardization* (ISO) e da *British Standards Institution* (BSI).

## Appendici

1. Matrice della scala di maturità dell'azienda relativa al livello di *governance* interna
2. Interrelazioni tra il modello *Enterprise Risk Management* (ERM) ed il Modello Organizzativo D.Lgs. 231/01
3. Temi da inserire nell'agenda del Comitato controllo e rischi

# Appendice 1. Matrice della scala di maturità dell'azienda relativa al livello di *governance* interna

Come si è visto nel corso della trattazione, l'approccio metodologico della scala di maturità, in coerenza con il modello *Enterprise Risk Management* (*cfr*. immagine riportata di lato), valuta il livello di adeguatezza e di efficacia della *governance* aziendale, la gestione del rischio ed i controlli interni; a tal fine, le matrici di seguito articolate, rappresentano per gli amministratori uno strumento utile al fine di stabilire il grado di maturità aziendale per gli ambiti descritti e gli eventuali piani di evoluzione/rafforzamento.


Si rileva tuttavia, che trattandosi di modelli concettuali qualitativi non sempre è possibile riscontrare nella loro effettiva applicazione una perfetta omogeneità in ciascun ambito valutato; in pratica, rispetto a ciascuna classe di valutazione per certi aspetti l'azienda può posizionarsi a livelli iniziali, per altri può presentare un livello ben definito e per altri ancora potrebbe addirittura far rilevare un livello ottimizzato. Inoltre, essendo gli ambiti oggetto di valutazione riconducibili al modello ERM, gli stessi sono tra di loro interdipendenti e correlati. Da ciò si evince che ciascun ambito risulta condizionato dal livello di valutazione conseguito dal precedente; per esempio l'ambito relativo agli strumenti di misurazione e monitoraggio non potrà godere di una valutazione ottimale se le persone, le competenze, le responsabilità, le deleghe ed i comportamenti sono valutati ad un livello iniziale.

## Appendice 1:
## Matrice della scala di maturità dell'azienda relativa al livello di *governance* interna

| **A. Persone, competenze, responsabilità, deleghe, comportamenti** | | | | |
|---|---|---|---|---|
| Livello 1<br>**Iniziale** | Livello 2<br>**Semi-Strutturato** | Livello 3<br>**Definito** | Livello 4<br>**Gestito** | Livello 5<br>**Ottimizzato** |
| • Le informazioni sulle competenze sono limitate e di natura informale<br>• E' sentita l'esigenza di maggiori competenze manageriali e di *leadership*.<br>• I ruoli e le responsabilità non sono definiti.<br>• La formazione ed i programmi di sviluppo non sono attivi.<br>• I sistemi di incentivazione o disincentivazione non sono implementati<br>• Il management vede la *governance* come un impedimento. | • Le competenze di base necessarie per la direzione sono identificate.<br>• I ruoli e le responsabilità sono poco strutturati e non raggiungano un livello corretto.<br>• La formalizzazione dei ruoli chiave, dei programmi di sviluppo e rotazione delle risorse è attuata in modo limitato.<br>• Le responsabilità esistono ma non sono formalmente assegnate o documentate.<br>• I sistemi di incentivazione o disincentivazione non sono strutturati | • L'organo di governo definisce i ruoli ed esistono responsabilità formalmente assegnate.<br>• L'organo di governo monitora gli investimenti nelle risorse.<br>• I ruoli chiave ed i piani di sviluppo e rotazione delle risorse sono definiti e formalizzati.<br>• Le responsabilità, le deleghe ed i poteri sono definiti e documenti appieno.<br>• I *gap* identificati nelle competenze delle risorse sono in fase di superamento.<br>• Esistono azioni collettive che creano sporadiche tensioni. | • Le responsabilità alle prime linee organizzative sono assegnate<br>• La formazione continua è assicurata a tutti i dipendenti.<br>• Le deleghe ed i poteri sono comunicati e conosciuti.<br>• Le azioni collettive sono superate mediante una maggiore coesione. | • L'organo di governo e il top management dimostrano un forte interesse per la *governance* d'impresa<br>• Più livelli di *accountabilty* esistono in ciascun ambito organizzativo.<br>• Le decisioni sono chiare con idonei strumenti di *empowerment*.<br>• Il management vede la *governance* come un vantaggio competitivo. |

## Appendice 1:
## Matrice della scala di maturità dell'azienda relativa al livello di *governance* interna

| B. Definizione di obiettivi, piani strategici, risk management | | | | |
|---|---|---|---|---|
| Livello 1<br>**Iniziale** | Livello 2<br>**Semi-Strutturato** | Livello 3<br>**Definito** | Livello 4<br>**Gestito** | Livello 5<br>**Ottimizzato** |
| • La *mission* e gli obiettivi aziendali sono informali.<br>• Il processo di gestione del rischio non esiste.<br>• I rischi non sono percepiti.<br>• La valutazione dei rischi è informale e limitata.<br>• I piani a breve e medio termine sono informali.<br>• Le situazioni inattese sono frequenti e gestite con modalità di emergenza. | • Gli obiettivi aziendali generali sono molto ampi e le connessioni con le attività aziendali sono peraltro poco chiare.<br>• Le strategie ed i piani a breve e medio termine esistono ma hanno un utilizzo limitato.<br>• La gestione del rischio è parziale o limitata ed informale<br>• I rischi sono spesso sottovalutati.<br>• Un sistema per l'identificazione e la classificazione di rischi è impostato, con parziale implementazione e/o con misurazione qualitativa.<br>• *Risk assessment* sono svolti tramite *workshop* occasionali di autodiagnosi (*Control Risk Self Assessment* -CRSA) | • La *mission* ed gli obiettivi aziendali definiti e correlate alle attività aziendali.<br>• L'organo di governo approva obiettivi, piani, strategie e budget.<br>• I processi relativi alla gestione del rischio sono impiantati.<br>• Le responsabilità sulla gestione del rischio sono assegnate.<br>• L'organo di governo approva alcune politiche su rischi rilevanti o strategici.<br>• Un sistema per l'identificazione, la classificazione e la misurazione dei rischi è stato implementato.<br>• I programmi formativi in merito al *risk assessment* ed al *risk management* sono implementati. | • Gli obiettivi organizzativi e individuali sono definiti a cascata attraverso l'organizzazione.<br>• I piani operativi ed i budget sono rivisti annualmente e modificati se necessario.<br>• La valutazione formale dei rischi è completata ed è stata comunicata al Consiglio di Amministrazione.<br>• I rischi specifici sono mitigati con le azioni in atto di cui l'organo di governo monitora gli andamenti.<br>• Il sistema per l'identificazione, la classificazione e la misurazione di rischi è declinato fino ai livelli più operativi.<br>• Gli indicatori di rischio ad integrazione di *performance indicator* sono pienamente utilizzati. | • Tutto il personale opera in base ad obiettivi aziendali declinati sulle singole attività operative.<br>• I rischi sono conosciuti e gestiti dal management ad ogni livello<br>• I piani sono continuamente oggetto di aggiornamento per l'evoluzione dei rischi.<br>• Le strategie ed i piani comprendono idonee analisi di rischio integrate con il sistema di *risk management*.<br>• Il sistema di *risk management* è '*embedded*' nell'operatività dell'impresa. I progressi relativi al raggiungimento degli obiettivi della organizzazione ed alle modalità di gestione del rischio sono appropriatamente comunicati agli *stakeholder*. |

## Appendice 1:
## Matrice della scala di maturità dell'azienda relativa al livello di *governance* interna

| C. Definizione di processi e procedure operative ai vari livelli organizzativi | | | | |
|---|---|---|---|---|
| Livello 1<br>**Iniziale** | Livello 2<br>**Semi-Strutturato** | Livello 3<br>**Definito** | Livello 4<br>**Gestito** | Livello 5<br>**Ottimizzato** |
| • Le politiche sono assenti.<br>• Le prassi e le procedure sono gestite in modo non documentato.<br>• Le procedure sono elaborate *ad hoc.*<br>• Le responsabilità non sono assegnate.<br>• I dipendenti agiscono in modo intuitivo anche nell'esecuzione dei controlli | • Le politiche sono definite e formalizzate solo al livello alto.<br>• Un codice etico è emanato<br>• Qualche procedura formale è applicata.<br>• Alcuni controlli formalmente previsti sono adottati.<br>• Le responsabilità sono stabilite. | • Le politiche di *governance* sono stabilite dall'organo di governo.<br>• Una buona conoscenza dei principi di *governance* è diffusa ed i progetti e le attività relative sono avviati.<br>• L'impianto procedurale è definito.<br>• Le procedure di controllo sono definite.<br>• La documentazione è prontamente disponibile.<br>• Responsabilità stabilite e formalizzate | • La vigilanza sulle politiche di *governance* è attiva da parte dell'organo di governo.<br>• L'impianto procedurale è definito e pienamente attuato.<br>• La conoscenza delle politiche e delle procedure è ampiamente diffusa.<br>• Le informazioni correlate alla rete procedurale sono conformi agli standard.<br>• La garanzia della qualità è raggiunta attraverso auto-valutazioni e controlli. | • Le procedure operative ed i protocolli/ procedure 231 sono integrate tra di loro.<br>• I controllo integrati esistono anche nell'ambito dello sviluppo di nuove attività e progetti.<br>• I risultati delle attività di internal auditing con valutazioni adeguate o positivi sono molto frequenti<br>• Il miglioramento continuo è perseguito tramite procedure di diagnosi e valutazione. |

## Appendice 1:
## Matrice della scala di maturità dell'azienda relativa al livello di *governance* interna

| D. Sistemi di comunicazione, informazione, informatizzazione | | | | |
|---|---|---|---|---|
| Livello 1<br>**Iniziale** | Livello 2<br>**Semi-Strutturato** | Livello 3<br>**Definito** | Livello 4<br>**Gestito** | Livello 5<br>**Ottimizzato** |
| • La comunicazione è informale<br>• Le informazioni incomplete e non disponibili per tutti gli interessati.<br>• I principi di trasparenza non sono riconosciuti.<br>• La documentazione non sempre disponibile.<br>• I controlli che assicurino la coerenza e la completezza dell'informativa non sono stati implementati<br>• La tempestività nella comunicazione non è richiesta.<br>• Le soluzioni tecnologiche adottate sono limitate o isolate | • L'importanza della disponibilità delle informazioni è riconosciuta.<br>• La comunicazione è focalizzata sulla reportistica.<br>• Il *reporting* è solo parzialmente strutturato, non è scadenzato ed è pianificato per singolo destinatario.<br>• L'uso della tecnologia è limitato;<br>• Solo alcune soluzioni tecnologiche sono adottate ed i relativi progetti di sviluppo sono avviati. | • La comunicazione interna presenta un'ampia diffusione.<br>• La reportistica è scadenzata con informazioni standardizzate.<br>• Le soluzioni tecnologiche supportano una informativa effettiva sulla *governance*.<br>• L'uso di sistemi informatici è diffuso a diversi livelli anche se gli stessi sistemi non sempre sono integrati. | • L'informazione e la trasparenza sono un importante aspetto della cultura organizzativa.<br>• La tecnologia é utilizzata per la automazione di buona parte della reportistica.<br>• La reportistica è gestita con informazioni e tempistiche differenziate per ciascun utente.<br>• È previsto uno standard sulla reportistica che copre gli aspetti chiave.<br>• La tecnologia è implementata per fornire una informativa a tutti i livelli. | • La comunicazione a tutti gli *stakeholder* è completa.<br>• La trasparenza é vista come un elemento chiave della *governance.*<br>• Una reportistica complessiva sulla sostenibilità esiste ed è regolarmente predisposta.<br>• La tecnologia nella compilazione della reportistica è ampiamente adottata.<br>• Sono stabiliti standard che coprono tutti gli aspetti del reporting.<br>• La comunicazione è ritenuta una *best practice.*<br>• La tecnologia è pienamente integrata ed è considerata un vantaggio competitivo nelle *governance.* |

## Appendice 1:
## Matrice della scala di maturità dell'azienda relativa al livello di *governance* interna

| **E. Strumenti di misurazione e monitoraggio** | | | | |
|---|---|---|---|---|
| Livello 1<br>**Iniziale** | Livello 2<br>**Semi-Strutturato** | Livello 3<br>**Definito** | Livello 4<br>**Gestito** | Livello 5<br>**Ottimizzato** |
| • Esistono pochi strumenti di misura.<br>• Non esiste un processo di monitoraggio. | • Alcuni strumenti di misura sono stati adottati.<br>• I monitoraggi cominciano ad essere più reattivi.<br>• Alcune ricognizioni indipendenti sono svolte a livello informale. | • I processi di monitoraggio o sorveglianza sono definiti per le prime linee e per l'organo di governo.<br>• Gli strumenti di misura sono implementati per tutti gli obiettivi aziendali e le relative misurazioni globali sono in atto.<br>• Le forme di monitoraggio svolte da strutture di controllo di secondo livello esistono in ogni struttura aziendale.<br>• L'*assurance* indipendente è fornita al organo di governo dalla funzione Internal Audit. | • Gli strumenti di misura sono implementati per tutti gli obiettivi aziendali ed i risultati sono comunicati.<br>• Le misurazioni sono riviste annualmente.<br>• Tra i diversi gruppi di monitoraggio esistono alcune forme di coordinamento.<br>• L'Internal Audit applica il programma di *Quality Assurance Review* con cadenza annuale e con validazione esterna almeno ogni 5 anni. | • Gli obiettivi di *governance* sono ricompresi nel sistema di incentivazione.<br>• Esiste un sistema di controllo integrato ed i flussi tra tutte le strutture di controllo di primo, secondo e terzo livello sono efficienti e scambiati regolarmente.<br>• Le rilevazioni sono parte integrante di un sistema di *perfomance management*.<br>• Le rilevazioni coprono i *key driver*.<br>• E' adottata una *balance score card*. aziendale o sono implementati strumenti di rilevazione a 360° gradi. |

## Appendice 2. Interrelazioni tra il modello *Enterprise Risk Management* (ERM) ed il Modello Organizzativo D.Lgs. 231/01

Nell'ottica integrata della *governance* aziendale si evidenzia che i punti cardine del Modello Organizzativo ex D.Lgs. 231/01 anche se mirati ad aree definite come reati dalla legislazione vigente, costituiscono un vero e proprio sistema di controllo interno e di gestione dei rischi.

A tal proposito si riportano di seguito alcuni elementi chiave dei modelli organizzativi D.Lgs. 231/01, ampiamente trattati nelle linee guida delle associazioni di categoria quali Confindustria e ABI:

- analisi dei rischi potenziali (oggetto di potenziale reato);
- analisi dei relativi presidi;
- attribuzione delle responsabilità;
- costituzione di adeguati protocolli e procedure;
- diffusione del modello e attività di formazione del personale;
- controllo da parte di un Organismo di Vigilanza indipendente al fine di vigilare su attuazione ed effettivo funzionamento del modello;
- flussi informativi, tra cui segnalazioni di anomalie, verso l'Organismo di Vigilanza;
- previsione di un sistema sanzionatorio aziendale in caso di mancata ottemperanza ai regolamenti interni.

E' interessante osservare come tali elementi convergano perfettamente nel modello ERM che, se correttamente applicato, può fornire un'idonea copertura anche rispetto alle esigenze di presidio previste dal D.Lgs. 231/01.

Come illustrato nella figura riportata di fianco, è possibile rilevare una perfetta simmetria funzionale tra gli otto presidi del Modello Organizzativo 231 e gli otto elementi dell'*Enterprise Risk Management*. In particolare:


- la comunicazione degli obiettivi prevista nel *framework* internazionale si traduce nel Modello Organizzativo stesso che richiede, con inconfutabile chiarezza, la definizione degli obiettivi di prevenzione dei rischi previsti dalla norma legislativa;
- l'ambiente interno, quale fondamento generale di controllo, prevede tra l'altro, un codice etico di impresa e il relativo sistema disciplinare come standard di riferimento per una cultura del controllo e una gestione aziendale impostata sul rispetto di tale rigore etico. In questo senso, la diffusione delle prescrizioni del Modello 231, soprattutto tramite una costante attività formativa, contribuisce a rafforzare un ambiente aziendale più consapevole dei rischi da affrontare e dei presidi necessari a contenerli. Inoltre, il sistema di procedure e di deleghe aziendali costituisce il quadro di riferimento per l'assegnazione di responsabilità, garantendo l'*accountability* di tutti i processi aziendali, compresi quelli rilevanti ai fini 231;
- la identificazione degli eventi di rischio e la relativa valutazione richiedono una continua analisi integrata delle aree potenzialmente esposte anche ai rischi di reato ex 231 e delle relative modalità di realizzazione per valutarne l'effettivo grado di esposizione; tutto questo si svolge in modo integrato al sistema di *risk assessment* complessivo dell'impresa;

- le scelte strategiche operate dall'azienda per fornire una risposta ai rischi al fine di evitarli, contenerli o accettarli, richiedono spesso la revisione dei processi di controllo e conseguentemente l'adozione di idonee procedure aziendali che, sempre con approccio integrato, presidiano anche le aree ritenute sensibili in ottica 231;
- oltre ai presidi di primo livello, previsti dalle procedure e di competenza del management operativo, l'attività di controllo implica necessariamente un'attività di audit e di *compliance* svolte con indipendenza anche ai fini 231;
- l'informazione e la comunicazione richiamano l'esigenza di sistemi e modalità di informazione tra loro integrati nonché di una gestione strutturata dei flussi informativi e delle segnalazioni verso l'Organismo di Vigilanza, anche al fine di individuare situazioni potenzialmente a rischio;
- il monitoraggio rappresenta una componente centrale dello schema complessivo che comprende la necessaria supervisione da parte dell'Organismo di Vigilanza sull'adeguatezza e sul funzionamento del Modello, nonché sul suo continuo aggiornamento. All'attività di monitoraggio gli organi di controllo e il Consiglio di amministrazione partecipano ciascuno in base ai propri compiti e ruoli.

La correlazione appena descritta tra gli elementi dei due modelli mostra tutta la valenza di un *framework* integrato dei sistemi di controllo che può quindi essere efficacemente declinato in ogni ambito in cui sono strutturati presidi aziendali.

Inoltre, con l'introduzione di un numero crescente di reati, tra cui quelli informatici, è essenziale per l'efficacia del Modello Organizzativo 231 che tutte le attività insite nello stesso, dall'analisi dei rischi all'attuazione delle procedure aziendali, siano realizzate in modo integrato con il complessivo sistema di controllo e di gestione dei rischi. Tuttavia, attualmente, spesso si rileva che le prassi e le procedure aziendali risultano ancora separate e realizzate in modo a sé stante.

Si ribadisce invece, che proprio il notevole ampliamento dello spettro legislativo rende sempre più necessaria la correlazione dei presidi esistenti con quelli previsti in altri ambiti legislativi, quali, ad esempio, quelli stabiliti da:

- D.Lgs. 81/08[1] - Tutela della salute e sicurezza nei luoghi di lavoro;
- Legge 18 aprile 2005, n. 62[2] (*market abuse*); D.lgs. 21/11/2007 n. 231[3] (antiriciclaggio);
- Legge 28 dicembre 2005, n. 262[4] (tutela del risparmio), per gli aspetti di comunicazione sociale del bilancio.

Infine, si sottolinea ancora una volta che l'integrazione dei sistemi di controllo e di gestione dei rischi, è un aspetto essenziale per la valutazione dell'efficacia e dell'efficienza del sistema di controllo interno dal quale la funzione Internal Auditing non può prescindere.

[1] Decreto legislativo 9 aprile 2008, n. 81 Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro.

[2] Legge 18 aprile 2005, n. 62 Disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee. Legge comunitaria 2004.

[3] Decreto Legislativo 21 novembre 2007, n. 231 Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione.

[4] Legge 28 dicembre 2005, n. 262, Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari.

## Appendice 3. Temi da inserire nell'agenda del Comitato controllo e rischi

Gli argomenti di seguito presentati rappresentano alcuni dei punti che sarebbe opportuno portare all'ordine del giorno nelle riunioni del Comitato controllo e rischi; tale *check list* pur non avendo carattere esaustivo, fornisce un riferimento pratico per affrontare gli aspetti di *governance* già illustrati nel testo ed oggetto di valutazione per il Comitato controllo e rischi.

| Argomento | Informative/ aspetti da approfondire | Cadenza | Riferimento nel testo/ paragrafo |
|---|---|---|---|
| **Rivisitazione del Modello di *governance* complessivo** | •Modello di riferimento (ERM, COSO, ecc.)<br>•Modello Organizzativo D.Lgs. 231/01<br>•Ultima relazione approvata della corporate governance<br>•Aggiornamenti sugli orientamenti in merito | Annuale | II. |
| **Valutazione del processo di pianificazione strategica** | •Tassonomia rischi<br>•Mappatura rischi<br>•Modalità quantitative/qualitative di misurazione dei rischi e metodi di correlazione<br>•Organigramma, ruoli, sistema delle deleghe<br>•Progetti formativi<br>•Modello adottato per l'esplicitazione degli obiettivi<br>•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<br>•Aspetti implementativi del Modello organizzativo 231<br>•Scala di Maturità | Annuale, prima della approvazione del Piano Strategico | IV.,V. Appendice 1-B |
| **Proposta Piano Strategico oggetto di approvazione da parte del CdA** | •Tutte le analisi sviluppate in ottica rischi<br>•Modalità per l'esplicazione degli obiettivi<br>•Livello di esplicitazione della propensione al rischio | Annuale | V. |

| Argomento | Informative/ aspetti da approfondire | Cadenza | Riferimento nel testo/ paragrafo |
|---|---|---|---|
| **Analisi dell'evoluzione dei rischi significativi** | •Agenda del CdA<br>•Analisi dei flussi informativi per il CdA<br>•Informazioni sui rischi operativi raccolte dai dirigenti responsabili delle funzioni aziendali coinvolte o dalle funzioni di controllo di secondo livello<br>•Operazioni societarie avvenute o in corso<br>•Eventi imprevisti<br>•Analisi dell'Internal Audit | Trimestrale | V. |
| **Valutazione dell'ambiente interno** | •Informazioni fornite dall'Amministratore incaricato di vigilare sul sistema di controllo e di gestione dei rischi<br>•Sistema delle deleghe<br>•Sistemi di incentivazione<br>•Sistema disciplinare<br>•Sistemi di aggiornamento organizzativo<br>•Iniziative formative<br>•Codici etici e deontologici e modalità di raccolta delle segnalazioni<br>•Risultati dell'attività di Internal Audit<br>•Eventuali *survey*<br>•Scala di Maturità | Annuale | VI.<br>Appendice 1-A |
| **Valutazione del sistema aziendale di comunicazione e di declinazione degli obiettivi** | •Adeguatezza dei flussi informativi al CdA<br>•Adeguatezza dei flussi informativi dal CdA<br>•Informazioni fornite dall'Amministratore incaricato di vigilare sul sistema di controllo e di gestione dei rischi e dai Responsabili delle funzioni di Risorse Umane/ Organizzazione e dal Responsabile ICT<br>•Sistemi di incentivazione<br>•Strutturazione del management reporting<br>•Informazioni fornite dai responsabili di controllo della seconda e terza linea<br>•Scala di Maturità | Semestrale o trimestrale | IV,VI<br>Appendice 1-B,D |

| Argomento | Informative/ aspetti da approfondire | Cadenza | Riferimento nel testo/ paragrafo |
|---|---|---|---|
| **Valutazione andamento sistema di controllo interno** | •Adeguatezza dei flussi informativi al CdA<br>•Fonti informative fornite dall'Amministratore incaricato di vigilare sul sistema di controllo e di gestione dei rischi<br>•Relazioni dell'Internal Audit<br>•Risultati dei Follow up audit sui piani di rafforzamento<br>•Flussi informativi provenienti dalle funzioni di controllo di secondo livello<br>•Evoluzione delle politiche e linee guida di *governance*<br>•Evoluzione impianto procedurale<br>•Informazioni fornite dalla Società di Revisione<br>•Informazioni fornite dal Collegio Sindacale<br>•Scala di Maturità | Almeno trimestrale, anche in base ad una reportistica strutturata | VI. Appendice 1-C,E |
| **Valutazione della funzione di Internal Audit** | •*Quality Assurance Review* (QAR) interna o esterna<br>•Mandato della funzione di Audit<br>•Risorse, competenze, titoli professionali e certificazioni<br>•Dimensionamento delle risorse<br>•Copertura dell'attività pregressa svolta dalla funzione di Audit<br>•Approccio metodologico adottato per le valutazioni di audit | Annuale | VII. |
| **Approvazione del Piano annuale e di medio termine di Internal Audit** | • Proposta di Piano annuale e pluriennale di Internal Audit<br>• Piano di verifiche rilevanti ai sensi del D.Lgs. 231/01<br>• Informative fornite dal Collegio Sindacale<br>• Universo audit<br>• Criteri di risk assessment<br>• Revisioni della copertura di medio termine | Annuale | VII. |

La redazione del documento è stata curata da Carolyn Dittmeier – membro Executive Board IIA, Responsabile Controllo Interno di Poste Italiane, Past President ECIIA e AIIA, membro Audit Committee della FAO.

Hanno collaborato allo studio Paolo Casati, Marta Fraganza e Francesco Fuscà, professionisti che si dedicano all'approfondimento di temi legati ai rischi e controlli con l'obiettivo di contribuire alla cultura di controllo dell'organizzazione cui appartengono e alla diffusione della stessa agli stakeholder in generale.

Si esprime un sincero ringraziamento a Rosalba Casiraghi, Carmine di Noia e Emma Marcandalli, costantemente impegnati nello sviluppo della governance aziendale, che hanno fornito preziosi contributi.