Il cambio di prospettiva nelle responsabilità e nella relazione tra funzioni di controllo dettato dal nuovo *Three lines model*

Carlo Regoliosi*
Dipartimento di Economia Aziendale Università degli Studi Roma Tre
Michele Variale
Responsabile Internal Auditing e Risk di Telepass SpA

ABSTRACT
L'ormai trentennale nutrito dibattito sulla natura, necessità e utilità dei cosiddetti "sistemi di controllo" ha prodotto negli anni diversi frutti, documentali e, diremmo noi, culturali che hanno dapprima posto all'attenzione collettiva e dappoi rafforzato e affinato metodi e processi di varia natura e calibro, aventi ad oggetto una corretta e consapevole gestione dei rischi, in un'ottica di controllo interno.
Tra i principali effetti dello sviluppo e della diffusione dei temi qui in discorso, uno dei più importanti pertiene l'ormai consolidato attuarsi di sistemi di controllo interno quale architrave portante di una gestione sostenibile e profittevole.
Il contributo esamina proprio il sistema di controllo interno, in quanto esso pur costituendo il pilastro di più antica trattazione (di lì parti la citata commissione Treadway, incaricata di produrre un *benchmark* di riferimento in materia) è parimenti quello che più di tutti ha vissuto evoluzioni ed affinamenti sino al più recente *Three lines model*, paradigma attuale di detti sistemi.
L'analisi di tale ultimo modello a nostro parere crea le giuste premesse per lo sviluppo di forme di *assurance* combinata tra soggetti diversi, storicamente anche distinti e distanti, e in tal senso dà avvio ad una feconda collaborazione tra diversi *layer* di controllo di sicuro interesse e di ampie prospettive.

RINGRAZIAMENTI
Uno speciale ringraziamento va indirizzato alla dott.ssa Marisa Zoppi, laureata magistrale in Economia Aziendale, oggi internal auditor nel gruppo Engie. Senza il suo prezioso lavoro di tesi, alcuni passaggi del presente lavoro sarebbero risultati più faticosi.

* Benché il contributo debba riferirsi integralmente ai due autori, i paragrafi 1, 2 e 5 debbono attribuirsi al prof. Regoliosi, mentre i paragrafi 3, 4 e 6 debbono attribuirsi al dott. Variale.

1 Introduzione

Dalla fine degli anni '80 del secolo scorso, si è sviluppato – dapprima oltre oceano – dappoi anche in Europa un ampio e nutrito dibattito su tematiche inerenti i cosiddetti "sistemi di controllo". All'apparire di una complessità crescente delle dinamiche economiche – si pensi, a titolo di mero esempio, al mutato scenario dell'ambiente di riferimento per le imprese legato all'avvento di internet ed al riemergere di tentazioni fraudolente (antiche come l'uomo, ma dagli impatti che si sono notevolmente ampliati nel tempo e nello spazio) – fece infatti da contraltare quasi coevo una profonda riflessione sulle modalità con cui le imprese potessero far fonte e ai nuovi ed agli antichi rischi. In tale dibattito – dalla commissione Treadway (1987) in avanti – sono scaturiti molteplici frutti, documentali e, diremmo noi, culturali che nel corso degli ultimi 30 anni hanno dapprima posto all'attenzione collettiva e dappoi rafforzato e affinato metodi e processi di varia natura e calibro, aventi ad oggetto una corretta e consapevole gestione dei rischi, in un'ottica di controllo interno.

Pur non essendo questa la sede per riferire anche in sintesi della feconda produzione sopra citata, è innegabile che alla vigilia del giro di boa del terzo di secolo dalla prima release del CoSO Report, alcuni elementi fondazionali sono stati ormai accolti a pieno titolo nel disciplinare giuridico ed organizzativo delle imprese. Si pensi, anche qui volendo esemplificare, (i) ai sistemi di amministrazione e controllo, nonché ai codici di governo delle imprese che hanno assai integrato e reso intelligibile la struttura di governance delle società di capitali di grandi dimensioni, (ii) ai modelli di *risk management* progressivamente evolutisi che – dal mondo finanziario sino a quello industriale – hanno contribuito ad un più rigoroso costruirsi dei processi decisionali e di feedback, sino (iii) al deciso istituzionalizzarsi dei sistemi di controllo interno quale architrave portante di una gestione sostenibile e profittevole.

Il contributo qui in proposta si rivolge proprio a quest'ultimo tassello dell'agire responsabile, il sistema di controllo interno, giacché paradossalmente costituisce il pilastro di più antica trattazione (di lì parti la citata commissione americana incaricata di produrre un *benchmark* cui riferirsi per ragionevolmente "evitare" frodi contabili e scandali finanziari) e perché il lungo corso della riflessione sul punto ha a nostro avviso prodotto nel tempo risultati di grande interesse, culminati nel *Three lines model*, paradigma attuale di detti sistemi.

2 Il sistema di controllo (e di gestione dei rischi): cenno e rinvio

Definizioni di sistema di controllo ne sono state fornite molteplici, sia sotto il profilo normativo che di prassi; esse sono tutte di grande interesse, ma riteniamo che in questa sede sia utile richiamare le due maggiormente autorevoli: il già citato CoSO Report e il Codice di Corporate governance.

Nel primo dei documenti citati, si legge che il Sistema di Controllo interno è un «*processo, svolto dal CdA, dai dirigenti e da tutto il personale aziendale, finalizzato a fornire una ragionevole certezza sul raggiungimento degli obiettivi aziendali che rientrano in particolare nelle seguenti categorie:*

– *efficacia ed efficienza delle attività operative;*
– *attendibilità delle informazioni di bilancio;*
– *conformità alle leggi e regolamenti in vigore*».

Nel secondo, viceversa, al par. XVIII di apertura del capitolo 6, si legge che il «*sistema di controllo interno e di gestione dei rischi è costituito dall'insieme delle regole, procedure e strutture organizzative finalizzate ad una effettiva ed efficace identificazione, misurazione, gestione e monitoraggio dei principali rischi, al fine di contribuire al successo sostenibile della società*».

Non sorprenderà il lettore la compresenza di due definizioni (*inter multa alia*) così distanti: da una parte vi è una spiccata enfasi sulla componente umana, che nell'altra statuizione non è nemmen citata. Nella seconda, tuttavia, vi è una esplicita attenzione al tema dei rischi, non casualmente riflessa nell'integrazione della definizione stessa "*Sistema di controllo interno e di gestione dei rischi*", taciuti dal CoSO Report nonché una menzione degli strumenti che da impiegare come forme di presidio.

Il connubio delle due definizioni – a ben vedere forse meno distanti di quanto sembri proprio per le differenti ottiche con cui affrontano il tema, facilmente combinabili a nostro giudizio – ha prodotto nel tempo soluzioni organizzative e di costrutto che hanno assurto a loro volta a *best practice* in materia. Su tutte, val la pena ricordare il *Three Lines Model* (2020), evoluzione non implicita di un precedente modello, cui dedichiamo il prossimo paragrafo.

3 Il *Three lines model* del 2020: di che si tratta?

Nel 2013, l'Institute of Internal Auditors, con l'obiettivo dichiarato di delineare a sua volta specifiche *best practices* volte alla creazione di una buona governance aziendale, elaborò il *Three Lines of Defense Model*. Si trat-

tava di un quadro di riferimento volto a supportare le aziende nell'organizzazione del SCIGR che dava enfasi al ruolo e all'indipendenza dell'internal auditor quale elemento decisivo per raggiungere gli intenti figurati dai modelli di controllo implementati.

Il modello in parola, in estrema sintesi, ritiene produttivo «*distinguere tre livelli in cui è articolato il presidio del Sistema di Controllo Interno nel suo complesso, sia con riferimento al suo disegno che al relativo funzionamento:*

– *il primo livello, consistente nei c.d. controlli di linea, pertiene al management operativo e agli stessi lavoratori, e riguarda i controlli e le attività di supervisione insite nei processi operativi e produttivi che richiedono competenze specifiche del business, dei rischi e delle normative pertinenti;*

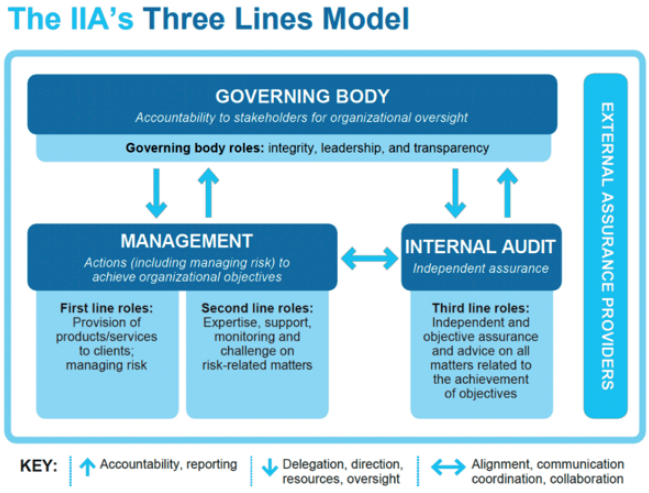
– *il secondo livello concerne le strutture aziendali che forniscono assurance su rischi specifici e presidia il processo di individuazione, valutazione, gestione e controllo dei rischi legati all'operatività, garantendone la coerenza rispetto agli obiettivi aziendali e rispondendo a criteri di segregazione che consentono un efficace monitoraggio;*

– *il terzo livello, infine, fornisce l'Assurance complessiva sul disegno e il funzionamento del Sistema di Controllo Interno attraverso valutazioni indipendenti. È insito nell'attività svolta dall'internal audit e dagli organi di controllo e di vigilanza*» (F. Accardi <www.riskcompliance.it>).

Nel corso del tempo, anche in considerazione dell'evoluzione della professione di *Internal Auditing* e della crescente maturità ed autorevolezza delle riflessioni dell'Institute internazionale, sono venute ad esistenza alcune possibili opportunità di miglioramento nel modello. da più parti, infatti, anche solo l'espressione "*defense*" fu ritenuta obsoleta, quando non *misleading*: il controllo e, più in generale, la gestione dei rischi siede a pieno titolo alla tavola degli strumenti del buon *manager* senza dover essere relegata a profili difensivi; per la creazione di valore occorre un buon mix di tutti gli attori e di tutti i punti di vista, non qualificando alcuni tra questi come attori ed altri come tutori o peggio "controllori".

In tale dibattito, l'IIA intraprese un percorso di aggiornamento del modello che portò, nel 2020, a dare vita ad una *release* più evoluta, chiamata *Three Lines Model* (rappresentato nella Figura 1).

Figura 1
Il *Three Lines Model* (2020)



Quest'ultimo modello vuole porsi quale *framework* avente l'obiettivo di:
– guidare le organizzazioni nell'identificazione di strutture e processi che consentano il raggiungimento degli obiettivi aziendali;
– strutturare un efficace ed efficiente Sistema di Controllo Interno e Gestione dei Rischi (SCIGR).

Il modello, come detto, sostituisce il precedente *Three Lines of Defense* del quale ne rappresenta una evoluzione (anche se, a parere di chi scrive, non una evoluzione "necessaria"), specie in considerazione delle nuove frontiere che orientano ormai da qualche anno la professione.

Il primo dei due principali elementi evolutivi del nuovo *framework* (il secondo "*Risk Management (including internal control)*" meriterebbe riflessioni a parte, fuori ambito nella presente dissertazione) è rappresentato, come cennato, dalla sua denominazione: l'eliminazione della parola "difesa" dal nome del modello, sintetizza e racchiude in sé il percorso seguito dalle riflessioni condotte in seno all'associazione – e più in generale tra gli addetti ai lavori – nell'aggiornamento dello stesso, ma soprattutto chiarisce in modo nuovo ciò che oggi ci si può e ci si deve attendere dal concetto di "controllo", nonché la professione di IA.

Al riguardo, Richard Chambers, presidente e CEO dell'*Institute of Internal Auditors* fino al 2021, riferendosi al modello in esame ha affermato: «*I think one of the things that we've been able to do with the new Three Lines Model*

is to emphasize that the role of management, the board and the internal auditors is to enhance the value to organizations, not just protect it. While as internal auditors we still have responsibilities for providing assurance on the effectiveness of risk management and controls, we also should be lending a hand in helping our organizations better understand the opportunities» (<https://www.accountingtoday.com/news/iia-updates-three-lines-model-to-stress-risk-management-and-governance>). Da queste parole emerge chiaramente e con forza la logica di fondo del nuovo modello e i principi che ogni professionista del rischio, tra cui vanno annoverati gli internal auditor *in primis*, dovrebbe osservare nello svolgimento del proprio lavoro.

Ogni internal auditor, infatti, è oggi chiamato ad adottare un approccio proattivo nella verifica della corretta e congrua gestione del rischio e quindi nelle attività tipiche di *assurance*, le quali, diversamente dal passato, non sono più finalizzate esclusivamente alla protezione del valore dell'organizzazione, bensì anche alla creazione dello stesso[1]. Ciò – a ben vedere – riflette il carattere per cui le aziende non sono più concepite come entità solo da proteggere, preservare, conservare attraverso l'identificazione delle potenziali minacce che, se non opportunamente gestite e mitigate, potrebbero compromettere il successo dell'organizzazione e, nei casi più gravi, la sua sopravvivenza. Al contrario, rispettando un percorso evolutivo in cui l'*assurance* è anche *advisory*, ci si attende che, al giorno d'oggi, l'IA contribuisca all'individuazione delle opportunità che il contesto presenta.

Del resto, già da una prima lettura del nuovo modello, risulta molto chiaro l'intendimento di N. Mouri (Chairman dell'IIA nel periodo 2018-19) che, durante il periodo in cui il documento era in consultazione pubblica (nel 2019), aveva dichiarato in modo esplicito lo scopo della revisione del *framework*: «*Garantire l'adattamento e la flessibilità alle organizzazioni e dinamiche delle diverse aziende, affinché le strutture dei livelli di controllo possano fare leva e imparare reciprocamente, in modo più efficace e strategico. Dobbiamo abbracciare il concetto che il rischio vada oltre la difesa. L'incertezza crea rischi e crea opportunità. Entrambe le parti devono essere prese in considerazione nel processo decisionale e nella pianificazione a tutti i livelli. Le organizzazioni devono decidere il modo più appropriato*

[1] Si consideri quanto riportato dall'IIA: «the Mission of Internal Audit articulates what internal audit aspires to accomplish within an organization. Its place in the IPPF is deliberate, demonstrating how practitioners should leverage the entire framework to facilitate their ability to achieve the Mission. The mission of internal audit is to **enhance and protect organizational value** by providing risk-based and objective assurance, advice, and insight» (enfasi nostra).

per allocare e strutturare le risorse e le responsabilità all'interno delle loro organizzazioni, utilizzando a loro vantaggio le Tre Linee di Difesa» (<https: //www.riskcompliance.it/news/il-nuovo-modello-delle-tre-linee-al-centro-la-creazione-di-valore-e-linterazione/>).

Il *Three Lines Model* consente, inoltre, di definire con maggiore chiarezza i ruoli e le responsabilità degli attori coinvolti a vario titolo nella *governance* societaria e le relazioni intercorrenti tra loro. Sul punto, è appena il caso di anticiparlo, si fondano novità di particolare interesse, cui nel prosieguo si darà conto ed argomento.

A riguardo, l'IIA ha scelto di mantenere la distinzione tra organi di prima, seconda e terza linea *esclusivamente* per differenziare i ruoli ricoperti da quest'ultimi e mantenere una certa familiarità col modello precedente. Le "linee" non intendono denotare elementi strutturali: gli organi di governo, il *management*, così come le strutture di controllo e gestione dei rischi e l'Internal Audit, non sono da interpretarsi come ruoli a sé stanti e statici. Il modello favorisce l'abbandono dell'approccio tradizionale di controllo cd. *a silos*, per abbracciare e incentivare il ricorso a forme di cooperazione più o meno intense tra i vari *assurance providers*, interni ed esterni all'organizzazione, in modo tale che gli organi di governo e gli altri *stakeholder* possano beneficiare di una visione completa, univoca e olistica sull'efficacia della *governance*, dei rischi e dei controlli aziendali.

A ben vedere, questo punto di visuale si affianca (talora superandolo) al requisito/pilastro della indipendenza (leggasi *segregation of duties*) convogliando il valore di questa nel più ampio obbiettivo di efficacia talora dimenticato per strada a vantaggio di miopi distanze. Detto connubio di forze è possibile (e fecondo) soltanto se i professionisti di prima, seconda e terza linea comunicano tra loro impiegando un linguaggio comune in materia di rischi e controlli, ferme restando le competenze specifiche e le responsabilità possedute da ciascuno, cercando di rimuovere le barriere esistenti, spesso dettate da limiti informativi derivanti dalla diversa collocazione nell'organigramma aziendale.

Occorre, in altre parole, che tutti gli attori del SCIGR siano allineati verso un obiettivo comune, ossia la creazione e la salvaguardia del valore aziendale nel rispetto delle aspettative e prerogative di tutte le parti interessate. I rischi diventano, quindi, (finalmente?) una questione collettiva e la responsabilità del miglior modo di fronteggiarli è condivisa: ciascuna linea risponde dei risultati derivanti dall'esercizio della propria funzione e nel rispetto delle proprie prerogative, ma tutte insieme, congiuntamente, in quanto "gruppo" sono responsabili del successo o insuccesso della ge-

stione del rischio e quindi, in via transitiva, dell'organizzazione

Va osservato inoltre come il *Three Lines Model* sia un modello *principle based*. Esso propone sei principi chiave che consentono alle organizzazioni di esaminare e valutare criticamente la propria complessiva struttura di *governance*, individuando i propri punti di forza ed eventuali aree di miglioramento.

L'articolazione per principi conferisce elasticità e flessibilità al modello, il quale è applicabile, pur con ampi correttivi e gradualità, a qualsiasi azienda, indipendentemente dalla natura o dimensione. Tali principi, unitamente ai ruoli svolti dagli attori del SCIGR, saranno affrontati nel paragrafo successivo.

4 Il *Three lines model* del 2020: principi e ruoli del modello

Il *Three Lines Model* identifica 6 principi chiave (riportati nella Figura 2.

Figura 2
I principi chiave del *Three Lines Model*

- **Principio 1 – Governance**

Il primo principio individua nella creazione di un SCIGR – di qui innanzi SGR - *Sistema di gestione dei rischi (incluso controllo interno)* – efficiente ed efficace il fondamento del successo sostenibile dell'organizzazione (si rinvia *supra* al già citato art. 6 del codice di Corporate Governance). A tal

fine, l'organo di governo (Consiglio di Amministrazione o Consiglio di Sorveglianza, a seconda del modello di *governance* adottato) è chiamato ad improntare la propria *leadership* sui valori dell'integrità e della trasparenza, così da essere percepito dagli *stakeholder* (ad esempio azionisti, dipendenti o clienti) come un *partner* affidabile poiché dotato di un elevato livello di responsabilità (*Accountabilty*). Si sottolinea in questo passaggio – pur incidentalmente – l'importanza dei c.d. stakeholders perché, in un'ottica *risk based*, il perimetro dell'azienda contemporanea risulta marcatamente più ampio di quanto la tradizione, anche scientifica, ha nel tempo delineato. Laddove, infatti, il successo sostenibile di un'organizzazione dipenda fortemente dagli effetti di componenti "esogene" (*partnership*, *supply chain*, reti, ecc.), il successo aziendale origina anche nell'assunzione consapevole (e gestione *in parte qua*) di rischi esterni al perimetro di responsabilità istituzionale, ma *de facto* capaci di generare conseguenze importanti per l'impresa, e dunque meritevoli di essere appuntati all'evidenza.

Il *management*, inoltre, deve sempre agire (*Actions*) in modo efficiente, ottimizzando cioè le risorse disponibili e secondo processi decisionali basati sul rischio. In altre parole, le "azioni", nonché la stessa attività di *risk management*, dovrebbero essere l'esito di un processo ponderato, il quale prevede (i) una preventiva analisi delle iniziative da intraprendere per il conseguimento di determinati obiettivi (di *business* e di governo), (ii) una pianificazione delle stesse e (iii) un successivo *follow-up*, che tenga conto dei potenziali impatti derivanti dal mancato raggiungimento dei traguardi prefissati.

In tale scenario, l'*internal auditor* si colloca nel ruolo di facilitatore[2] a supporto del vertice aziendale nel miglioramento continuo del SGR, fornendo servizi di *assurance* e consulenza indipendenti e obiettivi e riportando eventuali carenze riscontrate direttamente al board (*Assurance and Advice*), secondo standard, ma anche verso le linee coinvolte, monitorando con attenzione il procedere delle azioni correttive.

- **Principio 2 – Ruolo dell'organo di governo**

Il secondo principio prevede che l'organo di governo garantisca l'esistenza di strutture e processi adeguati per una *governance* efficace e, al contempo, l'allineamento degli obiettivi e delle attività aziendali con gli interessi prioritari degli *stakeholder*. Esso inoltre:

– delega le responsabilità specifiche e fornisce risorse al *management*

[2] Secondo un'interpretazione del ruolo che da tempo lo vede quale fluidificatore indipendente di relazioni lavorative talora complesse in materia di gestione del rischio e controllo.

per raggiungere gli obiettivi aziendali, garantendo al tempo stesso il rispetto delle aspettative legali, normative ed etiche;
– istituisce e supervisiona una funzione di *internal audit* indipendente, obiettiva e competente per fornire chiarezza e fiducia sui progressi realizzati verso il raggiungimento degli obiettivi.

Allineare gli obiettivi in un quadro di forze sovente centrifughe e individualistiche, per di più nel rispetto di molteplici *layer"* normativi" è attività complessa, di qui la necessità di un salto di qualità in tutti coloro che, pur a diverso titolo, mirano al raggiungimento degli obiettivi olistici dell'organizzazione.

• **Principio 3 – Management e ruoli della prima e seconda linea**

In generale, in coerenza con quanto descritto in precedenza, il terzo principio prevede anzitutto che i responsabili delle singole funzioni aziendali debbano indirizzare le varie attività al perseguimento degli obiettivi dell'organizzazione.

Nella prima linea sono ricomprese tutte le *business units* e le attività principali della catena del valore, ossia quelle che riguardano direttamente la produzione, la fornitura e la consegna di prodotti o servizi al cliente. Inoltre, rientrano nella prima linea anche tutte le funzioni di supporto, quali ad esempio l'ufficio acquisti o la logistica. La prima linea, pertanto, è rappresentata dal *management* operativo al quale è affidata, oltre che l'esecuzione delle attività anzidette, la prima responsabilità e titolarità della gestione dei rischi: in questo non casualmente vengono definiti *risk owner*.

I controlli di primo livello (o di linea) sono i controlli effettuati all'interno dei processi operativi da parte dei relativi responsabili[3] e sono finalizzati ad assicurare il corretto svolgimento delle operazioni aziendali.

Nella seconda linea, invece, troviamo funzioni organizzative maggiormente focalizzate su indirizzo e controllo in ottica di coordinamento e supervisione al presidio di rischi specifici; esse forniscono competenze complementari e supportano il *management* di linea nell'implementazione e nel monitoraggio del sistema di gestione del rischio.

Facendo riferimento agli attori del SGR in tema di *data security risk*, costituiscono un esempio di professionisti di secondo livello il *Chief Risk Officer* (CRO) e il *Chief Information Security Officer* (CISO) e, più in generale,

[3] Non a caso chi scrive ritiene vi siano anche controlli di livello *zero* appannaggio dei materiali operatori, attori delle azioni elementari. Non esiste logicamente alcuna attività, infatti, che sia agita senza controllo.

le funzioni di *compliance*, controllo della qualità, ma anche etica e sostenibilità ambientale. In generale, i controlli di seconda linea hanno l'obiettivo di assicurare – nell'ambito del perimetro oggettivo cui la loro attività è rivolta – la corretta attuazione del processo di *risk management*, il rispetto dei limiti operativi assegnati ai responsabili di area, nonché la conformità dell'operatività aziendale alla normativa vigente.

- **Principio 4 – Ruoli di terza linea**

Il quarto principio è specificamente dedicato all'internal audit, che rappresenta la funzione cardine della terza e ultima linea di controllo interno prevista dal modello. Il principio in esame ricalca essenzialmente la definizione di IA, secondo la quale ogni internal auditor fornisce *assurance* e *advisory* indipendente ed obiettiva sull'adeguatezza e l'efficacia della governance[4] e del sistema di controllo interno e di gestione del rischio.

L'IA mediante l'impiego di un approccio sistematico, grazie alle sue competenze e all'esperienza maturata sul campo, aiuta le funzioni di prima e seconda linea a trovare un equilibrio in termini di costi/benefici del controllo, promuovendo un sistema di *risk management* e controllo interno che consenta all'organizzazione di giungere ai propri traguardi, strategici e operativi, tenendo conto delle risorse necessarie per conseguirli e ottemperando alle politiche di assunzione del rischio adottate. Egli, inoltre, espone i risultati della propria attività agli organi di governo dai quali dipende funzionalmente pur mantenendo la propria indipendenza da quest'ultimi.

- **Principio 5 – Indipendenza della terza linea**

Il quinto principio è strettamente correlato al precedente e ribadisce, ancora una volta in modo esplicito, l'indipendenza dell'internal auditing, intesa come prerequisito obbligatorio di qualsiasi mandato di *assurance* e consulenza, così come previsto dagli standard professionali IPPF. L'indipendenza dell'IA, infatti, si pone quale pilastro fondamentale per la sua obiettività, credibilità e autorità.

Come già accennato, l'esigenza di combinare le *expertise* dell'IA in materia di SGR, con le competenze già verticali dei diversi detentori di responsabilità di controllo (leggasi 2ª linea) reclama una rivalutazione del por-

[4] Occorre notare che detto passaggio è ben lungi dal considerarsi pacificamente attuato, in quanto l'adeguatezza e l'efficacia della *corporate governance* sono sovente appannaggio degli azionisti o del Consiglio di Amministrazione, con ovvi problemi di circolarità.

tato del requisito di indipendenza per evitare formali *non expedit* o pericolose circolarità. Da una parte infatti un'eccessiva rigidità formale nell'interpretazione del requisito può portare ad effetti di inefficienza nei controlli e di intralcio non necessario alle operatività, oggetto di molteplici "disturbi" da parte dei diversi addetti al controllo; mentre una eccessiva flessibilità interpretativa potrebbe generare l'effetto opposto di mancanza di presidi obiettivi reciproci e l'indebolirsi della *constructive challenge* tra linee diverse, che è il principale elemento abilitante del miglioramento continuo del sistema di controllo.

- **Principio 6 – Creazione e protezione di valore**

Il sesto principio si concentra sulla creazione e sulla protezione del valore generato dall'organizzazione, elemento come già detto di assoluto rilievo nel novero degli argomenti qui in trattazione. A tal fine, tutti i ruoli coinvolti sono portati a **collaborare** in modo **coordinato** per contribuire alla creazione di valore e alla protezione degli *asset* aziendali, salvaguardando così gli obiettivi dell'organizzazione e gli interessi dei suoi *stakeholder*.

Il coordinamento e l'armonizzazione di tutte le attività e funzioni di *governance* possono essere garantiti attraverso la comunicazione, la cooperazione e altre forme di collaborazione. Tale ultimo principio sarà oggetto di maggiore attenzione nel prossimo paragrafo.

Come detto in precedenza, l'approccio *principle based* offerto dal modello in esame è stato ideato per fornire agli utenti una maggiore flessibilità. Tale elasticità si riflette anche sui ruoli che il *board*, il *management* e *l'audit* interno sono chiamati a svolgere nel più ampio quadro della *corporate governance*.

In particolare, l'organo di governo:

– è responsabile nei confronti degli *stakeholder* (all'interno dei quali annoveriamo gli azionisti *in primis*) della supervisione generale dell'organizzazione e della guida di quest'ultima, definendone vision e mission;
– si assume l'impegno di monitorare e tutelare gli interessi delle parti interessate, nonché comunicare in modo trasparente il raggiungimento degli obiettivi;
– è il principale promotore della cultura del controllo in azienda e, per tale ragione, è chiamato a comportarsi in modo virtuoso, secondo elevati canoni di etica e responsabilità;
– istituisce strutture, processi e comitati ausiliari volti alla realizzazione di un buon governo societario;
– delega responsabilità e fornisce risorse al *management* per raggiun-

gere gli obiettivi (di *business* e di governo) aziendali;
– determina i livelli di *risk appetite* dell'organizzazione e valuta l'adeguatezza del Sistema di Controllo Interno e di Gestione dei Rischi, nonché sulla *compliance* alle aspettative legali, normative ed etiche dell'azienda;
– istituisce e sovrintende a una funzione di *internal audit* indipendente, obiettiva e competente.

Il *management di linea*, invece, è responsabile delle azioni (inclusa la gestione del rischio per ciascuna porzione aziendale di competenza) tese al raggiungimento delle finalità aziendali e risponde delle risorse a lui affidate per il loro conseguimento.

I responsabili di linea dipendono gerarchicamente dal *board* e riportano direttamente a quest'ultimo i risultati ottenuti nel perseguimento dei traguardi organizzativi pianificati, nonché eventuali scostamenti tra gli uni e gli altri. Essi, inoltre, debbono garantire la conformità alle aspettative legali, normative ed etiche.

Gli specialisti di seconda linea, come già osservato, apportano competenze complementari su obiettivi specifici della gestione del rischio e, in particolare:
– promuovono lo sviluppo, l'implementazione e il miglioramento continuo delle pratiche di risk *management* e di controllo interno a livello di processi, sistemi ed entità;
– monitorano il raggiungimento degli obiettivi più basici del SGR, quali ad esempio il rispetto di leggi, regolamenti e comportamenti etici accettabili, *IT security*, sostenibilità e *quality assurance* e riportano i risultati raggiunti al *board*.

L'internal auditor, invece, come già più volte trattato all'interno di questo elaborato, riporta funzionalmente al *board* e amministrativamente al *senior management* i risultati della propria attività di *assurance* e consulenza, supportando l'organizzazione nel raggiungimento dei propri obiettivi con un approccio professionale sistematico volto a generare valore aggiunto, in quanto finalizzato al miglioramento dell'efficienza e dell'efficacia del quadro complessivo di *corporate governance*.

5 La responsabilità condivisa delle funzioni di controllo nell'indirizzo dei rischi: allineamento, comunicazione, coordinamento e collaborazione

Il sesto e ultimo principio proposto dal *Three Lines Model*, dedicato alla creazione e alla protezione del valore aziendale, recita testualmente: «*tutti i ruoli, lavorando insieme, contribuiscono collettivamente alla creazione e alla protezione del valore quando sono allineati tra loro e con gli interessi prioritari degli stakeholder. L'allineamento delle attività si ottiene attraverso la comunicazione, la cooperazione e la collaborazione. Ciò garantisce l'affidabilità, la coerenza e la trasparenza delle informazioni necessarie ad assumere decisioni basate sul rischio*».

Tale principio, nonostante sia enunciato a chiusura del modello, è probabilmente tra i più importanti ed innovativi di quelli offerti, in quanto sintetizza gli anni di lavoro e di riflessione da parte dell'IIA nella stesura del *framework* e ne evidenzia la complessità nel momento in cui questo deve essere applicato.

Esso è graficamente rappresentato dalla freccia bidirezionale che collega la funzione di internal audit con il *management* di prima e seconda linea (si torni *infra* alla Figura 1): quest'ultima rappresenta un elemento del tutto innovativo e caratteristico del modello, non riscontrabile nelle precedenti versioni, e testimonia la necessità di trasformazione ed evoluzione delle relazioni tra gli attori del SGR.

Per comprendere il principio in esame, pare opportuno interrogarsi anzitutto sul significato delle parole chiave in esso contenute.

L'allineamento a cui il modello fa riferimento è prima di tutto un allineamento a livello informativo, ma anche di intenti e di processi. I vari attori del SGR sono invitati, cioè, a condividere le stesse priorità di controllo fondate su un set informativo, anche in termini di rischiosità, comune e completo e, al contempo, le attività di verifica effettuate da ciascuno sono ipotizzate omogenee sul piano della metodologia tecnica e delle *technicality* impiegate (ad esempio, prevedendo la stessa numerosità campionaria); diversamente i risultati non sarebbero tra loro comparabili. L'allineamento di processo, è opportuno sottolinearlo, implica l'adozione di un'unica tassonomia allorquando si parla di rischi.

Ragionando in termini di rischi, è giudizio di chi scrive che il modello intenda spingere gli attori del SGR a rimuovere asimmetrie informative. Il disallineamento è un fenomeno progressivo e, spesso, poco visibile, soprattutto al *management* impegnato "a testa bassa" nel perseguimento di individuali agende di lavoro a fronte di sfidanti obiettivi funzionali. Il

disallineamento è anche un fenomeno fisiologico: i processi mutano in forza della vitalità dell'azienda nel mercato, così come le organizzazioni, che devono adattarsi ai cambiamenti sia in termini prettamente ri-organizzativi, sia in termini di nuove *skill* richieste. Ciò nonostante, non da ogni parte dell'organizzazione la capacità di adattamento alle novità della realtà è omogenea per modi e per tempi.

Ecco perché, nell'opinione di chi scrive, il Three Lines Model oggi incentiva le varie funzioni di controllo all'adozione di un linguaggio univoco e condiviso in materia di rischi e controlli. Sovente, infatti, negli ormai oltre 30 anni di tempo trascorsi dalle prime elaborazioni, le direzioni comuni osservabili tra porzioni di rischio-controllo sono state poche (si pensi al proliferare di modelli di gestione connessi a normative in materia di Health, Safety, alla 231, alla 262, all'Anticorruzione, alla privacy, ecc. sovente attivatrici di mappature di rischi, evidenza di *gap* ed elaborazione di azioni da implementare sconnesse tra loro) a stretto vantaggio degli attori impegnati in autopromozione e a sicuro nocumento dell'efficacia e dell'efficienza dei controlli.

Inoltre, il termine "allineare" letteralmente, significa "disporre sulla stessa linea cose o persone". Nello spirito del modello, dunque, allineamento è soprattutto da intendersi in senso molto ampio, di allineamento delle sensibilità ai rischi.

Sul piano organizzativo è evidente che le funzioni di prima, seconda e terza linea osservino l'organizzazione, i suoi rischi e le sue opportunità da prospettive differenti. Infatti, se è vero che l'*internal auditor* gode di una posizione privilegiata di osservazione rispetto al *management*, avendo una visione a 360 gradi dell'azienda ed anche perché, in virtù del ruolo svolto, ha accesso illimitato e incondizionato a qualsiasi risorsa dell'organizzazione, è altresì vero che il *management* di linea (da una parte) e le funzioni di secondo livello (dall'altra, pur se in misura minore) osservano le operazioni di *business* ad un livello di granularità che *l'auditor* difficilmente potrebbe maneggiare. Questo fa sì che l'IA sia una figura professionale normalmente competente e preparata in materia di rischi e controlli generali e generici, che di contro, il *management* di linea abbia un *set* di conoscenze approfondito, pur se focalizzato alla propria area funzionale di appartenenza, e che le conoscenze degli specialisti di secondo livello siano focalizzate su determinati ambiti del rischio/controllo. Il CISO, ad esempio, è certamente competente in materia di rischi collegati alla sicurezza delle informazioni in azienda, ma potrebbe non essere altrettanto preparato in tema di *compliance* normativa e procedurale, disciplina nella quale risulta

maggiormente qualificata l'area legale e, talvolta, lo stesso internal auditor.

Resta quindi da chiedersi: come allineare i ruoli dei diversi attori del SGR data la loro diversa collocazione nell'organigramma aziendale, l'eterogeneità di competenze e sovente il differente bagaglio culturale? Una possibile risposta a questa domanda viene offerta dallo stesso principio: *"l'allineamento delle attività si ottiene attraverso la comunicazione, la cooperazione e la collaborazione"*.

La **comunicazione** è il primo strumento che il *framework* individua per attenuare le differenze esistenti tra i protagonisti del SGR. Comunicare significa rendere comune la conoscenza, condividere le proprie esperienze e competenze su un determinato argomento (in questo caso la gestione dei rischi) e ciò naturalmente presuppone l'esistenza di un vivo dialogo tra le funzioni in esame, compresa quella di IA. A riguardo – come osservato – si potrebbe obiettare che l'interazione dell'IA con il *management* potrebbe minare l'indipendenza e, quindi, l'obiettività della funzione, essendo le due dimensioni intimamente correlate tra loro. In realtà, l'idea per la quale l'internal auditor, al fine di conservare la propria integrità professionale, debba isolarsi dal resto dell'organizzazione è ormai osservazione anacronistica e priva di coerenza (G. Troina, 2005), specie alla luce dei nuovi sentieri che sta percorrendo la professione e degli attributi che l'Internal Audit 4.0 deve possedere per operare in contesti così dinamici quanto incerti.

Nel tempo presente è ormai pacifico ritenere che l'*internal audit* possa dialogare e confrontarsi col *management* senza che per questo risulti pregiudicata la propria indipendenza ed obiettività. Lo stesso *framework* ribadisce che l'internal auditor non debba operare isolato. D'altronde, la stessa attività di *assurance* e consulenza costituisce un servizio reso dal professionista a supporto del *management*, presupponendo quindi un dialogo tra i due.

La comunicazione così intesa consente di realizzare due forme di relazione: la cooperazione e la collaborazione. Questi due termini spesso vengono erroneamente considerati sinonimi, in realtà assumono significati diversi.

La **cooperazione** è un processo attraverso il quale un gruppo di persone agisce o lavora sullo stesso progetto con l'obiettivo di conseguire un vantaggio reciproco dalla realizzazione di quest'ultimo, anziché competere a beneficio esclusivo di ogni individuo. I partecipanti condividono lo stesso obiettivo, ma restano portatori di interessi individuali.

È del tutto evidente che il richiamo alla cooperazione presuppone alcuni elementi la cui comprensione previa aiuta a capire quanto la sfida sia ardua, aldilà delle intenzioni teoretiche sulle necessarie segregazioni, che riteniamo in via di superamento *de facto*.

In primo luogo, cooperare è un termine che nel tempo presente ha visto ridurre la sua comprensione e la sua portata ad ambiti di rado economici, piuttosto sociali, etici, caratterizzati in una da interessi individuali convergenti. La riduzione della capacità stessa di cooperare a quei soggetti che condividono un'uniformità di pensiero, ne ha quasi snaturato la portata in quanto cooperare presuppone tanto l'unità di direzione, quanto la diversità di origine (diversamente dalla collaborazione, di cui si dirà dopo).

In secondo luogo, anche quando il punto precedente si ritenga teorico, non vi è dubbio che occorra per cooperare la presenza evidente di un interesse comune, e terzo dagli interessi individuali, cui sacrificare ove del caso questi, quando in conflitto. Sul tema del sovraordinato e preordinato interesse delle organizzazioni rispetto a quelli pur legittimi individuali, autorevole dottrina (E. Di Carlo, 2017) ha fornito un panorama degli approcci epistemologici maggiormente in voga nell'ultimo cinquantennio, concludendo per la necessità di esso, non solo in virtù di un confuso presupposto etico, quanto di un'auspicabile razionalità e capacità di «*orientare le diverse classi di aziende verso un modello di sviluppo sostenibile orientato al bene comune*».

È peraltro vero che una simile chiarezza teorica, come sovente accade nelle faccende aziendali, non sempre si sposa con una coerente traduzione pratica, ed è pertanto un cammino lungo e – per certi aspetti – controcorrente quello di chi suggerisce cooperazione in luogo di competizione. A supporto, come anche qui sovente deve essere registrato, soccorre la realtà di fatto di imprese che consapevoli del fatto che "nessuno (o pochi) si salva da solo" hanno intrapreso sia all'esterno che all'interno la via dell'unità tra diversi (costruzione di solide partnership, rafforzamento dei messaggi e dei meccanismi di *supply chain*, ecc.), utile viatico per indirizzare lo stile direzionale a logiche di tal genere.

La **collaborazione**, invece, significa non solo lavorare insieme verso un obiettivo, ma anche condividere gli stessi interessi. Collaborando si mettono a fattor comune conoscenze, competenze, esperienze, informazioni, risorse e tempo al fine di raggiungere un determinato obiettivo comune. La collaborazione, pertanto, presuppone un legame più profondo tra gli attori del SGR e, sotto questo profilo, la realizzazione di progetti di *combined assurance* ne rappresenta una delle più alte espressioni.

Il sesto principio del *Three Lines Model* si rivela quindi quanto mai audace: non solo cooperazione (come si è detto merce rara), ma anche quando occorre collaborazione quale strumento operativo per allineare le funzioni di prima, seconda e terza linea, nel rispetto delle loro differenze e peculiarità. Esse si relazionano attraverso un dialogo continuo e costante

col fine ultimo di creare e proteggere il valore dell'organizzazione. Il *framework*, infatti, non intende eliminare la diversità dei ruoli ricoperti dai vari professionisti del rischio e del controllo, anzi, è proprio la diversità nelle conoscenze e competenze possedute da ciascuno che consente di colmare eventuali carenze nei controlli o duplicazioni di copertura. Per giungere a questo risultato, tuttavia, è necessario armonizzare e coordinare attività, processi, conoscenza ed etica, così da poter fornire una garanzia olistica in tema di *risk management* e controllo interno. La responsabilità del rischio diventa quindi condivisa, in quanto la gestione di quest'ultimo è l'esito di una strategia che vede la partecipazione a vario titolo di tutte le funzioni di controllo aziendale.

Al termine dell'ampia dissertazione, è possibile concludere che il valore del modello in discorso derivi dalla collaborazione dell'IA con gli altri attori del SGR e che la *combined assurance* sia uno degli strumenti operativi che meglio rispondono alla visione suggerita dal modello in esame.

6 La combined assurance come strumento operativo per implementare la visione suggerita dal *Three Lines Model*

La progettazione di un'adeguata *corporate governance* rappresenta una delle sfide principali cui sono oggi chiamate le aziende moderne. Per competere in contesti e mercati sempre più incerti, volatili, interconnessi si richiede alle aziende sempre più uno sforzo organizzativo ed operativo elevato, nonché la presenza in azienda di figure professionali che abbiano competenze multidisciplinari e avanzate per gestire un grande numero di rischi.

Come noto, sono diverse le funzioni di controllo, ognuna con ambiti di competenza ben definiti, che risultano fondamentali per l'organizzazione per gestire in maniera efficace ed efficiente i molteplici rischi cui l'attività è soggetta.

La mera esistenza di varie funzioni responsabili in vario modo di rischi e di controlli, tuttavia, non è sufficiente affinché queste possano contribuire attivamente al processo di creazione di valore. Per farlo è importante che questi attori accettino l'allineamento dei loro intenti, una visione armonica e organica dei processi di controllo e che le loro azioni siano coordinate, ma soprattutto condivise in un programma di lavoro. In questo modo, è possibile ridurre la probabilità di accadimento e la *magnitudo* degli eventuali impatti delle "carenze" nei controlli, evitare sovrapposizioni nei perimetri di analisi, ridondanze nel disegno del sistema di controllo interno

e duplicazioni di attività di *assurance*.

Sotto questo profilo, è nostro convincimento che la *combined assurance* (di seguito "CA") possa rappresentare – sotto determinate condizioni – lo strumento operativo ideale per implementare i principi enunciati dal *Three Lines Model* e, in particolare, il principio numero 6 – "Creazione e protezione di valore".

Come già osservato, la *combined assurance* trova fondamento nell'esigenza degli *stakeholder* di una garanzia olistica in tema di rischi e controlli che consenta di superare l'*assurance fatigue* derivante dall'effettuazione di molteplici verifiche, aventi ognuna una finalità diversa, ma spesso ripetitive per quanto riguarda le modalità di indagine e la raccolta di evidenze.

È nostro convincimento che la *combined assurance* sia uno dei modelli di conduzione delle attività di audit visibili nelle aziende che aderiscono profondamente allo spirito ed alla *mission* del *Three Lines Model*.

Se a giudizio di chi scrive risulta chiaro ed evidente come l'*assurance* combinata possa essere una diretta applicazione del modello in esame, quasi la sua adozione sia richiesta dallo stesso modello, nel mondo della professione e in quello accademico, molteplici sono i dibattiti sulla sua applicazione pratica. A riguardo, come più volte ripetuto, la principale critica che viene mossa alla *combined assurance* è quella di compromettere l'indipendenza dell'internal auditor, essendo quest'ultimo una funzione di terzo livello. In realtà, lo Standard IIA 2050 – Coordinamento e Affidamento **impone** al Responsabile di IA la condivisione delle informazioni con gli altri attori del SGR, il coordinamento delle attività di verifica da questi realizzate, ma soprattutto di «*considerare la possibilità di affidarsi all'operato di altri prestatori, esterni e interni, di servizi di assurance e consulenza, al fine di assicurare un'adeguata copertura e minimizzare le possibili duplicazioni*» (Standard IIA 2050 – Coordinamento e Affidamento).

A ciò si aggiunga che il concetto di indipendenza della funzione di IA è, a nostro parere, decisamente più profondo, non potendosi ricondurre esclusivamente alle linee di riporto organizzativo. L'indipendenza è, anzitutto, uno stato mentale grazie al quale l'internal auditor è in grado di esprimere il proprio giudizio professionale libero da qualsiasi *bias* interfunzionale e condizionamento psicologico o emotivo.

Al tempo stesso però, va osservato come la *combined assurance* massimizzi la sua utilità allorquando ricorrono due requisiti (vere e proprie condizioni di efficacia):

– una funzione di internal audit che creda fermamente nelle potenzialità e benefici della CA per le attività di verifica e gestione del rischio e

vede nella cooperazione un'opportunità per generare valore aggiunto;
– una cultura aziendale che promuova l'inclusione e il dialogo tra funzioni aziendali: qualsiasi progetto di *assurance* combinata richiede il pieno appoggio del vertice aziendale, diversamente sarà di difficile applicazione pratica.