UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI SCIENZE ECONOMICHE E AZIENDALI "M.FANNO"

CORSO DI LAUREA IN ECONOMIA (TrEC)

PROVA FINALE

"INTERNAL AUDITING & RISK MANAGEMENT: IL CASO ASPIAG SERVICE"

RELATORE:

CH.MO PROF. Marco Ugo Paiola

LAUREANDO: Tommaso Rampazzo

MATRICOLA N. 1096184

ANNO ACCADEMICO 2017 – 2018

Alla mia famiglia

Indice

INTRODUZIONE 1

1. INTERNAL AUDITING

1.1. Evoluzione della professione 6

1.2. Governance e Sistema di Controllo Interno 8

1.2.1. I principi di Governance 9

1.2.2. Il Sistema di Controllo Interno (SCI) 11

1.3. International Professional Practices Framework (IPPF) 14

1.3.1. Il Codice Etico 16

1.3.2. Gli Standard di Connotazione 18

1.3.3. Gli Standard di Prestazione 23

1.3.4. Uno sguardo al domani 28

2. RISK MANAGEMENT

2.1. SCI & RISK MANAGEMENT: CoSo Report vs. ERM 31

2.1.1. Il CoSo Report 31

2.1.2. Il modello ERM 33

2.2. Il processo di Risk Assessment 37

2.3. Il Rischio Reputazionale 42

3. ASPIAG SERVICE: UN NUOVO PASSO VERSO L'EFFICIENZA ORGANIZZATIVA

3.1. Il Gruppo Aspiag 45

3.2. Il modello di governance 47

3.3. L'attività di Internal Auditing in Aspiag 49

CONCLUSIONI 54

Riferimenti bibliografici 56

Riferimenti normativi 58

RINGRAZIAMENTI

Desidero ringraziare tutti i collaboratori della Direzione Auditing e DPA, in particolar modo il Responsabile Daniele Pitassi, il cui aiuto è stato fonte di molteplici riflessioni ed ha fornito un grande stimolo alla realizzazione dell'opera.

INTRODUZIONE

Nell'ultimo decennio, una delle novità più importanti nella struttura organizzativa delle aziende italiane è stata l'inserimento della funzione di Internal Auditing, elemento fondamentale del sistema di controllo interno e risposta razionale al problema di come amministratori e manager possono far fronte alle loro pesanti responsabilità in materia di trasparenza informativa, correttezza gestionale, efficacia ed efficienza.

La presente trattazione si propone di analizzare l'attività di tale funzione, cercando di far comprendere chiaramente in che modo genera valore aggiunto per l'organizzazione. La scelta dell'argomento è frutto dell'esperienza personale da stagista vissuta nella Direzione Auditing e DPA di Aspiag Service S.r.l., operante nel settore della Grande Distribuzione Organizzata (GDO). L'attività svolta all'interno della funzione comprendeva il supporto alle risorse nella gestione dei fornitori di servizi di sicurezza e trasporto valori e, in particolare, l'affiancamento al Responsabile nell'esecuzione di specifici audit, compresa la raccolta ed analisi delle informazioni, le interviste alle funzioni interessate, la redazione dei relativi report e la comunicazione al Board.

L'elaborato è organizzato in tre capitoli. Nel primo capitolo si procederà ad un'analisi completa dell'attività di Internal Auditing, partendo dal processo evolutivo avvenuto nel corso degli anni, per poi esaminare i principi di governance e di controllo interno, identificando gli attori coinvolti. Esso si conclude con la descrizione degli IPPF (International Professional Practices Framework), approfondendo in particolar modo gli Standard internazionali per la pratica professionale dell'Internal Auditing (di connotazione e di prestazione). Nel secondo capitolo si prenderanno in esame le tematiche di Risk Management in relazione al sistema di controllo interno (SCI), ponendo in confronto CoSo Report e ERM (Enterprise Risk Management), modelli che permettono la risoluzione dei problemi di identificazione, valutazione e gestione dei rischi da un punto di vista integrato che coinvolge l'intera azienda. La seconda e terza parte del capitolo tratteranno rispettivamente il processo di valutazione del rischio ("risk assessment") ed il rischio reputazionale, entrambi oggetto dell'attività dell'internal auditor. Il terzo ed ultimo capitolo esaminerà il caso di studio dell'azienda Aspiag Service, descrivendo in particolare il modello di governance e come viene svolta l'attività di Internal Auditing.

1. INTERNAL AUDITING

Le attività di Internal Auditing (o revisione interna, d'ora in poi IA) sono effettuate in contesti giuridici e culturali differenti, all'interno di organizzazioni che variano per finalità, dimensione e struttura, e da persone interne od esterne ad esse. Tale circostanza condiziona la "pratica" di IA in ciascuna azienda. Tuttavia, i professionisti del settore, associati nell'IIA - Institute of Internal Auditors, di cui l'AIIA (Associazione Italiana Internal Auditors) è la sezione italiana, individuano gli elementi chiave che caratterizzano tale attività negli Standard Internazionali per la pratica professionale (International Professional Practices Framework – IPPF) periodicamente aggiornati.

L'IIA, appunto, ne fornisce una definizione chiara e concisa:

*"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." (Definizione di Internal Auditing, IPPF. AIIA, s.d.)*

Essa "**assiste l'organizzazione**" in quanto funzione di staff rispetto al vertice aziendale, fornendo valutazioni e raccomandazioni sul livello di rischio residuo, senza assumere però la responsabilità finale per le decisioni prese, che rimane a carico del management di linea interessato.

È una funzione "**indipendente**" e "**obiettiva**", caratteristiche necessarie per lo svolgimento di tale attività. La prima si determina, a livello organizzativo, tramite un riporto gerarchico ai massimi vertici dell'organizzazione, mentre la seconda trova fondamento nell'etica professionale dell'auditor e nella sua competenza. Egli deve essere imparziale, privo di preconcetti e scevro di potenziali conflitti di interesse.

L'ambito di riferimento dell'IA è definito nelle attività di "**assurance**" (Figura 1), intesa come l'insieme delle attività utili a migliorare la qualità dell'informazione (attendibilità, tempestività, economicità e rilevanza) a supporto delle decisioni del management, ovvero l'esame oggettivo delle evidenze allo scopo di ottenere una valutazione indipendente dei processi di gestione del rischio, di controllo o di governance (per esempio, la verifica

dell'effettivo rispetto delle normative vigenti interne ed esterne), e di "**consulenza**" (Figura 2), ossia servizi di supporto ed assistenza, la cui natura ed estensione sono concordate con il cliente, intesi a fornire valore aggiunto e migliorare i processi di governance, Risk Management e controllo di un'organizzazione, sempre senza assumere responsabilità manageriali.

Figura 1: *attività di assurance* (Materiale didattico AIIA, IPPF, *Assurance vs. Consulenza*, 2017)

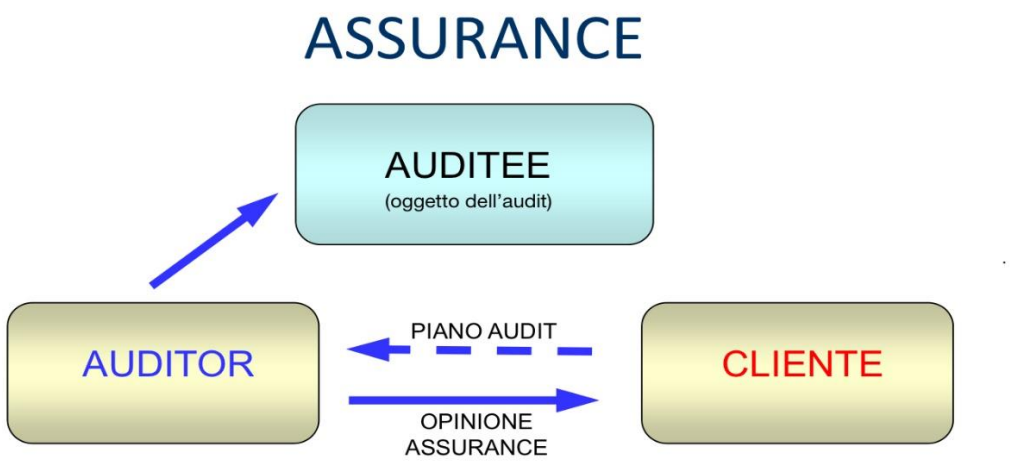


Figura 2: *attività di consulenza* (Materiale didattico AIIA, IPPF, *Assurance vs. Consulenza*, 2017)

L'Internal Auditor svolge la sua attività tramite un "**approccio professionale sistematico**", mettendo a disposizione dell'organizzazione la metodologia e gli strumenti necessari a condurre le analisi, le conoscenze, le capacità interpersonali e le competenze tipiche di tale professione.

Inoltre, secondo la definizione di IA, il metodo di audit applicato "**genera valore aggiunto**" e quindi è necessario che i benefici generati dallo svolgimento dell'attività siano superiori ai costi prodotti.

Il termine *internal auditor* si riferisce ai membri dell'Institute of Internal Auditors, ai detentori delle certificazioni professionali rilasciate dall'Institute, a coloro che si candidano a riceverle e a tutti i soggetti che svolgono attività di internal audit secondo la definizione di Internal Auditing.

In Italia, l'IA è una funzione giovane con risorse economiche e umane inferiori rispetto al mondo anglosassone e ancora poco presente all'interno delle Pubbliche Amministrazioni (Regioni, città metropolitane, ASL, Università) ma sviluppata nelle società quotate (soprattutto nei gruppi bancari), dove è obbligatoria, con ampie prospettive di crescita e miglioramento.

Stando ai risultati del sondaggio (denominato "Global Internal Audit Practitioner Survey") proposto dalla Research Foundation dell'IIA (IIARF) e condotto, nel corso del 2015, all'interno del progetto di ricerca internazionale CBOK (Common Body of Knowledge) allo scopo di analizzare lo status della professione confrontando l'Italia (164 Internal Auditor partecipanti) con i dati riferiti all'Europa Occidentale ed al resto del mondo (14mila partecipanti in 140 nazioni), si rileva che il 60% degli IA nel nostro Paese lavori per le società quotate in Borsa, mentre la diffusione risulta inferiore nel settore pubblico (6% circa). La percentuale di impiego nelle società private (non quotate), tra cui Aspiag Service S.r.l., è abbastanza importante, e si aggira intorno al 35% (come illustrato in Figura 3, D'Onza, 2016).

Figura 3: percentuale di impiego della funzione di IA in Italia, Europa e resto del mondo (dati CBOK).

Dal sondaggio emergono inoltre importanti constatazioni in termini di anzianità di servizio. Circa il 60% dei partecipanti, ha indicato che l'attività di Internal Audit è presente nella sua organizzazione da meno di 15 anni e ciò ne dimostra la giovinezza in Italia. Infatti, il ritardo con cui molte aziende di medio-grandi dimensioni hanno istituito la funzione di IA rispetto ai Paesi più industrializzati è abbastanza evidente.

Un'altra nota dolente riguarda le risorse. Molte funzioni di IA devono fare i conti con risorse umane e finanziarie limitate e si trovano a dover soddisfare richieste provenienti da numerosi attori della governance potendo avvalersi, anche in alcune società quotate, soltanto di poche unità di personale. La presenza in numerose aziende di unità organizzative di dimensioni ridotte pone diversi interrogativi sull'importanza che le figure apicali ed il CdA assegnano all'IA, nonché sulla sua capacità di riuscire ad essere percepita come una funzione che effettivamente crea valore. Si tratta di una sfida che i CAE (Chief Auditor Executive, ovvero il Responsabile dell'IA) quotidianamente si ritrovano a dover affrontare, in un contesto che, caratterizzato da una ripresa economica che procede a ritmi moderati, impone l'esigenza di puntare ad un'elevata produttività senza naturalmente perdere di vista la necessità di assicurare l'efficacia e la tempestività delle attività svolte. Per generare valore aggiunto è fondamentale che lo staff di IA sia composto da risorse qualificate.

1.1 EVOLUZIONE DELLA PROFESSIONE

Nel recente passato sono molteplici i fattori che hanno determinato l'evoluzione del contesto aziendale: lo sviluppo tecnologico, la pressione competitiva derivante dalla progressiva apertura e globalizzazione dei mercati, la complessità del contesto normativo e regolamentare, le ristrutturazioni aziendali, l'ottimizzazione dei processi alla ricerca di sempre maggiore efficienza e l'integrazione aziendale dovuta a sempre più frequenti fusioni e acquisizioni (Russo e Fraticelli, 2007).

In altre parole, questi fattori hanno portato ad una maggiore valorizzazione del concetto di rischio, nelle molteplici accezioni in cui è possibile percepirlo nell'ottica dell'impresa. Simmetricamente, si sono sviluppate e moltiplicate le opportunità, favorite dai processi di liberalizzazione degli scambi, dall'abbattimento delle barriere commerciali e finanziarie, dall'incremento dell'importanza della tecnologia e del know-how, dall'innovazione e differenziazione di prodotti, servizi e dei processi attraverso i quali vengono realizzati.

L'azienda è chiamata a reagire a tali cambiamenti (sia interni che esterni, sia positivi che negativi), perciò è importante che ogni funzione contribuisca alla creazione di valore. Anche l'*Internal Auditing*.

Nel corso del tempo tale funzione è stata caratterizzata da un'importante evoluzione storica, successiva all'introduzione negli anni '40, che vedeva gli auditor qualificati come area di "staff aziendale" principalmente rivolta all'osservazione e alla valutazione dei problemi aziendali aventi natura contabile e finanziaria. A partire dagli anni '80-'90, infatti, l'IA ha acquisito (o meglio, conquistato) una sempre crescente autonomia nell'esame ed analisi svolta a beneficio dell'alta direzione per la valutazione dell'insieme sistematico delle funzioni amministrative e gestionali dell'organizzazione (Aondio, Barbieri, Cassinari, Chiesa, Gutierrez, Marsecane e Micocci, 2014).

Questo processo evolutivo ha richiesto un rafforzamento degli *skills*, delle metodologie e degli strumenti di lavoro, ma soprattutto un cambiamento culturale della percezione del proprio ruolo e dei destinatari del proprio lavoro. In altre parole, oggi l'Internal Auditor deve calibrare la propria attività secondo un'ottica di "marketing interno", concentrando gli sforzi sulla soddisfazione dei propri "clienti" interni, ovvero preoccupandosi di come tutti gli stakeholder (dal board, al vertice aziendale, al management operativo) possano percepire e valorizzare il "prodotto" dell'audit (Rossi e Fraticelli, 2007).

Negli anni, infatti, l'accezione negativa di "watch-dog" (ispettore), il quale individuava un rischio già manifestato e ne imputava le responsabilità, si è ridimensionata a favore di un ruolo specializzato sull'individuazione di soluzioni coerenti con il contesto esterno di riferimento e con la propensione al rischio assunta dall'impresa.

Tutto ciò ha determinato una maggiore visibilità e credibilità della stessa funzione aziendale. Ma il processo evolutivo non finisce qui. La "*digital transformation*" interesserà anche la funzione di Internal Auditing e dipenderà in gran parte da come il top management saprà ripensare complessivamente l'organizzazione.

L'internal auditor del futuro non dovrà semplicemente essere un esperto di tecnologie digitali, ma dovrà saper esercitare il proprio ruolo in organizzazioni che il nuovo paradigma dell'economia digitale renderà più veloci nell'adattamento alle condizioni di mercato, più internalizzate, più connesse e attive nella comunicazione con gli stakeholder e, inevitabilmente molto più esposte al rischio. Quindi il valore della funzione sarà misurato soprattutto dalla capacità di anticiparli.

L'Italia ha investito molto meno di altri Paesi nell'innovazione tecnologica, accumulando un ritardo che ha pesato su crescita e produttività. I dati forniti dalla ricerca *Fattore ICT (2017)*, realizzata dal Politecnico di Milano e da Confindustria Digitale, evidenziano come il "Bel Paese" nel nuovo millennio abbia effettuato 20 miliardi di minori investimenti in tecnologia ogni anno rispetto alla media UE, raggiungendo un gap di oltre 300 miliardi a fine 2017 e, secondo una classifica stilata dalla Commissione Europea che misura il percorso dei Paesi verso un'economia e una società digitalizzate, si trovi agli ultimi posti (25esima su 28, nonché penultima nell'uso di internet).

Uno degli obiettivi del Convegno Nazionale dell'AIIA (Associazione Italiana Internal Auditors) 2017 "*Digital Transformation. L'Internal Auditing nell'Industry 4.0*" è stato appunto definire cosa manca per recuperare tale ritardo. Secondo il presidente Maurizio Bonzi, manca la piena consapevolezza di imprenditori e manager che è arrivato il momento di cambiare radicalmente il modo di progettare e organizzare il business, altrimenti saranno molte le aziende che non riusciranno a sopravvivere nel nuovo scenario. "Il passaggio dalla consapevolezza all'operatività", continua Bonzi, "sarà comunque difficile, perché la digital transformation interessa l'organizzazione nel suo complesso, a cominciare dalle competenze e attitudini richieste alle diverse figure aziendali, Internal Auditor compresi, naturalmente. Questo nuovo scenario sarà il banco di prova per l'IA, costretto a confrontarsi con fattori di rischio sempre maggiori." Le aree di rischio, che le nuove tecnologie hanno amplificato sono la cybersecurity, la protezione di dati sensibili e la reputazione (per esempio il malfunzionamento di un prodotto, se diffuso via social, può generare un rischio reputazionale enorme).

1.2 GOVERNANCE E SISTEMA DI CONTROLLO INTERNO

Le imprese italiane hanno fatto importanti passi avanti in materia di governance, adottando modelli più adeguati agli scenari in cui si muovono e più efficaci nella tutela degli stakeholder. Allo stesso modo, il sistema dei controlli e le figure che in azienda lo interpretano hanno conosciuto un'evoluzione rilevante. Nonostante ciò oggi si discute molto di organizzazioni troppo burocratizzate, di sovrapposizione nelle funzioni di controllo e, più in generale, di una scarsa efficacia a fronte di costi più elevati rispetto al passato (Fargion, 2014). Il bisogno di disciplinare le organizzazioni e di controllarne il funzionamento ha portato negli ultimi anni a costruire un sistema di norme molto pervasivo che, inevitabilmente, ha incrementato il grado di rigidità, mostrando limiti in termini di efficacia.

L'obiettivo sarà quindi superare questa tendenza formalista dei modelli di governance e controllo, rendendo il sistema più flessibile e maturo, lasciando alle organizzazioni un maggiore grado di discrezionalità nell'adattamento e agli interpreti (manager e professionisti) la responsabilità di compiere le scelte. Questo vale anche per gli internal auditor, i quali, con l'evoluzione dei modelli di governance, sono stati messi al centro del sistema di controllo interno e resi indipendenti dalle gerarchie, condizione necessaria per svolgere efficacemente il proprio ruolo.

1.2.1 I principi di Corporate Governance

Per "*Corporate Governance*" («governo d'impresa» o «governo societario») si intende l'insieme di regole, di ogni livello (leggi, regolamenti, ecc.) che disciplinano la gestione e la direzione di una società o di un ente, pubblico o privato (Materiale didattico AIIA, La Corporate Governance in Italia e nel Mondo*, I principi di Corporate Governance*, 2017). Essa include anche le relazioni tra i vari attori coinvolti, come i portatori di interesse (stakeholder, ossia chi detiene un qualunque interesse nella società), e gli obiettivi per cui l'impresa è amministrata. Gli attori principali sono gli azionisti (shareholders), il Consiglio di Amministrazione (Board of Directors, d'ora in poi CdA) e la direzione aziendale (management).

Nella progettazione del «governo societario» (approvato dal CdA) vengono definite le specifiche scelte attinenti agli assetti statutari (modelli di amministrazione e controllo) ed organizzativi interni (compiti, poteri e composizione degli organi aziendali), il sistema delle deleghe, il regime del controllo contabile, il sistema di incentivazione e remunerazione, i flussi informativi, la struttura finanziaria e le modalità di gestione dei conflitti di interesse.

Gli obiettivi sono principalmente quattro (Materiale didattico AIIA, La Corporate Governance in Italia e nel Mondo*, A cosa serve la Governance?*, 2017):

- Migliorare la qualità dell'azione strategica, per incrementare la creazione del valore attraverso l'ottimale rapporto rischio/rendimento;
- Assicurare la supervisione strategica e il controllo da parte del CdA (e dell'organo di controllo) sul top management;
- Assicurare l'esistenza di un contesto favorevole per lo sviluppo di un'efficace gestione dei rischi e del controllo interno;

- Assicurare l'affidabilità e la lealtà del management della società ed evitare che non ci siano operazioni contrarie all'oggetto sociale.

Nel corso degli anni l'attenzione al riguardo è cresciuta enormemente, in quanto inefficaci *sistemi di governance* riducono appunto l'efficacia del controllo (a tutti i livelli) sull'attività del top (e middle) management.

In Europa si possono trovare tre diversi sistemi di Corporate Governance, la cui adozione dipende in larga misura dalle disposizioni di legge locali. Essi sono: il sistema ordinario, il sistema monistico ed il sistema dualistico (Materiale didattico AIIA, La Corporate Governance in Italia e nel Mondo*, I principi di Corporate Governance*, 2017).

Il *sistema ordinario* fornisce il più alto livello di protezione, prevedendo la netta separazione tra le funzioni di gestione e di controllo. La gestione aziendale è assegnata ad un organo amministrativo, composto da più amministratori (CdA) o un singolo Director (Amministratore Unico). La funzione di controllo, invece, è assegnata ad un Collegio Sindacale composto da 3 o 5 membri effettivi e 2 supplenti. Questo modello risulta attualmente la forma più diffusa in Italia.

Il *sistema monistico* (modello anglosassone denominato «one-tier system») si differenzia dal sistema ordinario per l'assenza del Collegio Sindacale e permette una divisione flessibile di ambiti di responsabilità all'interno del CdA tra amministratori esecutivi (impegnati nella gestione quotidiana della società) e non esecutivi (Comitato di Controllo, eletto dal consiglio e avente il ruolo di supervisione). La responsabilità congiunta garantisce che le informazioni necessarie siano disponibili a tutti i membri del CdA, i quali vengono eletti dall'Assemblea dei Soci.

Il *sistema dualistico* (modello tedesco denominato «two-tier system») è composto sia dal Consiglio di Amministrazione (Management Board) sia da un Consiglio di Sorveglianza (Supervisory Board). Il primo gestisce la società e svolge le proprie funzioni come un organismo indipendente e può delegare alcuni dei suoi poteri di amministrazione ad uno o più dei suoi membri. Il secondo svolge la funzione di vigilanza e nomina i membri del CdA.

Tutte le parti coinvolte nel governo societario hanno un interesse, sia esso diretto o indiretto, nella performance della società: dipendenti e manager ricevono salari, benefit e reputazione; gli azionisti ricevono un ritorno monetario; i clienti ricevono beni e servizi; i fornitori ricevono compensi per i loro beni e servizi. In cambio, questi singoli individui apportano valore sotto forma di capitale economico, umano e sociale.

Per ridurre le inefficienze che nascono da situazioni avverse o potenzialmente pericolose, e quindi anche per "proteggere" i portatori d'interesse, vengono sviluppati meccanismi e controlli di governo societario. Essi possono essere *interni* o *esterni*. I primi monitorano le attività per poi intraprendere, se necessario, azioni correttive per raggiungere gli obiettivi aziendali. I secondi, invece, raccolgono una serie di controlli effettuati dagli stakeholder sull'impresa.

1.2.2 Il sistema di Controllo Interno

I principi di Corporate Governance definiscono il Sistema di Controllo Interno (SCI) come l'insieme delle regole, delle procedure e delle strutture organizzative volte ad assicurare il corretto funzionamento e il buon andamento dell'organizzazione, attraverso l'individuazione, valutazione, monitoraggio, misurazione e gestione di tutti i rischi d'impresa, coerentemente con il livello di rischio accettato dal vertice aziendale. È dunque un continuo processo di attività svolto da tutti gli organi dell'impresa che permea tutte le unità aziendali costituendo parte integrante dell'attività quotidiana.

Il Testo Unico delle disposizioni in materia di intermediazione finanziaria (D.Lgs. 24 febbraio 1998 n. 58, meglio noto come Testo Unico della Finanza - TUF) e la relativa disciplina di attuazione, individuano gli ambiti operativi degli organi preposti al controllo della gestione aziendale: il Collegio Sindacale, la società di Revisione e l'Internal Auditing.

Il **Collegio Sindacale**, ovvero l'Organo di Controllo, deve vigilare sull'osservanza della legge e dell'atto costitutivo, sul rispetto dei principi di corretta amministrazione e sull'adeguatezza della struttura organizzativa, del sistema di Controllo Interno e del sistema amministrativo-contabile. Esso però non svolge alcuna funzione di controllo contabile.

La **Società di Revisione** deve garantire la regolare tenuta della contabilità e la corretta rilevazione dei fatti di gestione nelle scritture contabili, la rispondenza del bilancio d'esercizio e del bilancio consolidato alle risultanze della contabilità e degli accertamenti eseguiti, nonché alle norme che li disciplinano. Essa, inoltre, esprime con apposite relazioni un giudizio sul bilancio d'esercizio e sul bilancio consolidato.

La **funzione di Controllo Interno** (Internal Auditing) deve verificare l'idoneità ed il rispetto delle procedure interne ad assicurare il rispetto delle disposizioni di legge, deve vigilare sul rispetto del codice interno di comportamento, deve gestire il registro dei reclami ed offrire un supporto consultivo ai settori dell'organizzazione aziendale in merito a specifiche

problematiche. Tale funzione è assegnata ad un responsabile (Responsabile Internal Auditing, d'ora in poi RIA), svincolato da rapporti gerarchici rispetto ai responsabili dei settori di attività controllati, che svolge la propria attività in modo autonomo e indipendente, riferendo gli esiti del proprio operato con obiettività e imparzialità.

A questi tre organi è necessario aggiungere il Consiglio di Amministrazione, il Comitato per il Controllo Interno (obbligatorio per le società quotate) e l'Alta Direzione (identificata nel presidente del CdA, nell'Amministratore Delegato o nel Direttore Generale).

Il **CdA** ha la responsabilità ultima del sistema dei controlli interni dei quali deve assicurarne la costante completezza, funzionalità ed efficacia, in coerenza con la specificità dell'impresa e la natura e l'intensità dei rischi aziendali. Tale mission si inquadra nell'ambito dei compiti di indirizzo strategico e organizzativo previsti dall'art. 2381 c.c..

In particolare, il CdA:

- approva la struttura organizzativa, l'attribuzione dei compiti, il sistema di deleghe di poteri e responsabilità, garantendo un'adeguata separazione di funzioni;
- definisce le strategie e le direttive in materia di sistema di controllo interni e di gestione dei rischi;
- viene informato sull'efficacia del sistema di controllo interno e di gestione dei rischi, avendo conto delle azioni correttive attuate a fronte di carenze appurate.

Le società quotate prevedono che il CdA si avvalga di un **Comitato per il Controllo Interno** (*Audit Committee*), costituito da Amministratori non esecutivi (la maggioranza dei quali indipendenti), il quale ha il compito di valutare l'attività dei preposti al Controllo interno, l'adeguatezza dei principi contabili utilizzati e l'attività della società di revisione.

L'**Alta Direzione**, invece, ha la responsabilità di attuare, mantenere e monitorare il sistema dei controlli interni e il sistema di gestione dei rischi, in conformità con le direttive dell'Organo Amministrativo. Si conferma come il sistema dei controlli interni sia elemento strutturale dell'impresa. In particolare:

- definisce in dettaglio la struttura organizzativa, i compiti e le responsabilità delle varie unità, concretizzando la separazione di funzioni;
- concretizza le strategie e le direttive in materia di sistema di controllo interni e di gestione dei rischi, procedendo a continuo monitoraggio;
- implementa le azioni migliorative del sistema di controllo interno e della gestione dei rischi, dandone conto al Consiglio di Amministrazione.

Dopo aver definito le competenze dei diversi organi di controllo ed al fine di garantire efficacia ed efficienza del SCI, è necessario che fra gli stessi vi sia *cooperazione*, soprattutto mediante lo scambio di informazioni.

Nel SCI esistono 3 diversi livelli (i c.d. "three lines of defense", figura 7), che ricoprono ruoli distinti all'interno del framework organizzativo (IIA, *The Three Lines of Defense in effective Risk Management and Control*, 2013):

- Il 1° livello consiste nei *controlli di linea (Operational Management)*, diretti ad assicurare la corretta esecuzione delle procedure di controllo delle operazioni ed effettuati dalle stesse strutture operative.
- Il 2° livello comprende i *controlli sui rischi e sulla conformità (Compliance and Risk Management)*, il cui obiettivo è assicurare la corretta attuazione del processo di gestione dei rischi ed il rispetto dei limiti operativi assegnati alle varie funzioni e garantire la conformità dell'operatività aziendale alle norme, incluse quelle di autoregolamentazione.
- Il 3° livello racchiude l'*attività di revisione interna (Internal Audit)*, volta ad individuare violazioni delle procedure nonché a valutare periodicamente la completezza, l'adeguatezza, la funzionalità (in termini di efficienza ed efficacia) e l'affidabilità del sistema di controllo interno e del sistema informativo (ICT audit).

Sebbene né il Senior Management né gli organi di governo siano considerati tra le tre "linee" di questo modello, nessuna discussione sui sistemi di controllo e di gestione dei rischi sarebbe completa senza prima considerare i ruoli essenziali che essi ricoprono. Entrambi rappresentano i principali stakeholder serviti dalle "tre linee di difesa"(o 3 livelli), e sono le parti meglio posizionate per garantire che esse siano rispecchiate nella gestione del rischio e nei processi di controllo dell'organizzazione.

Figura 7: *"the three lines of defense"* (Fonte: *The Three Lines of Defense in effective Risk Management and Control*, IIA, 2013).

1.3 INTERNATIONAL PROFESSIONAL PRACTICES FRAMEWORK (IPPF)

L'International Professional Practices Framework (IPPF) è lo schema concettuale che organizza le *Authoritative Guidance* emanate dall'Institute of Internal Auditors (IIA).

Le Authoritative Guidance sono suddivise in due categorie**: Vincolanti**, ovvero i *Principi Fondamentali per la pratica professionale di Internal Auditing*, la *Definizione di Internal Auditing*, il *Codice etico* e gli *Standard Internazionali per la pratica professionale dell'internal auditing* (Standard); e **Raccomandate**, ossia le *Guide Attuative* e le *Guide Supplementari* (IPPF, AIIA – Associazione Italiana Internal Auditors, s.d.).

Figura 8: *IPPF* (fonte: AIIA)

I fattori del mercato globale e la continua richiesta di elevati standard qualitativi in termini di buon governo aziendale, gestione del rischio e cultura del controllo interno hanno innalzato, in tutte le organizzazioni, le aspettative nei confronti del professionista dell'Internal Auditing. Per questa ragione, il 1° gennaio 2017 sono entrati in vigore i nuovi **Standard Internazionali per la pratica professionale** dell'attività di Internal Auditing. Tali standard sono il frutto del processo di revisione, coordinato dall'*International Internal Audit Standards Board* (IIASB) dell'Institute of Internal Auditors, culminato a inizio 2016 con la pubblicazione della proposta di cambiamenti e perseguito con la raccolta di feedback e la pubblicazione della versione definitiva a ottobre 2016. La nuova versione degli Standard, che sostituisce la precedente del 2013, completa la revisione effettuata a luglio 2015, la quale aveva introdotto alcuni

importanti elementi quali la *Mission dell'Internal Auditing*, i *Principi Fondamentali per la pratica della professione* e la riorganizzazione delle *Guide Interpretative e Pratiche*, sostituite dalle *Guide Attuative e Supplementari*.

Non si tratta di una vera e propria "rivoluzione", ma di una naturale evoluzione che riflette i cambiamenti nel contesto in cui operano ormai tutte le organizzazioni, le quali si trovano a dover affrontare una dinamicità senza precedenti alimentata anche dalle continue innovazioni nel campo dell'IT (Information Technology), facendo così aumentare le sfide ad operare sempre meglio con risorse limitate e le aspettative nei confronti della professione e di chi nelle organizzazioni è chiamato a dimostrare il valore dell'attività di Internal Auditing (Catani, 2017).

Insieme al **Codice Etico**, gli Standard trattano tutti gli elementi vincolanti dell'International Professional Practices Framework che l'Internal Auditor è tenuto a rispettare per essere qualificato come tale (infatti utilizzano la dizione "deve" per indicare un requisito vincolante) ed hanno uno scopo ben preciso: stabilire i *principi fondamentali* per la pratica della professione, fornire un *framework* per lo svolgimento e la promozione dell'attività di internal audit, stabilire *la base per valutare la prestazione dell'IA* e *migliorare* i processi e le operazioni dell'*organizzazione*.

Gli Standard comprendono due categorie principali, che si applicano a tutti i servizi di internal audit: **Standard di Connotazione** (attribute) e **Standard di Prestazione** (performance). I primi (1000, 1100, 1200 e 1300) precisano le caratteristiche che le organizzazioni e gli individui che effettuano attività di internal audit devono possedere, mentre i secondi (2000, 2100, 2200, 2300, 2400, 2500 e 2600) descrivono la natura dell'attività e forniscono criteri qualitativi in base ai quali è possibile valutarne la performance. Sono inoltre previsti gli Standard Applicativi, che dettagliano i contenuti delle due tipologie sopra citate, definendo i requisiti da applicare ai servizi di assurance (A) e di consulenza (C).

I servizi di assurance comportano un'obiettiva valutazione delle evidenze da parte degli internal auditor finalizzata alla formulazione di giudizi o conclusioni riferiti a un'organizzazione, attività, funzione, processo, sistema o altro. L'internal auditor definisce la natura e l'ampiezza dell'incarico di assurance. Tre sono le parti generalmente coinvolte nei servizi di assurance: (1) il *process owner*, cioè la persona o il gruppo direttamente coinvolti nell'organizzazione, attività, funzione, processo, sistema o altro, (2) l'*internal auditor*, cioè la persona o il gruppo che effettua la valutazione e (3) l'*utente*, cioè la persona o il gruppo che utilizzerà tale valutazione.

I servizi di consulenza sono attività di advisory e sono generalmente effettuati dietro specifica richiesta di un cliente committente. Natura e ampiezza dell'incarico di consulenza sono definiti in accordo con il cliente. Due sono, in genere, le parti coinvolte nei servizi di consulenza: (1) l'*internal auditor*, cioè la persona o il gruppo che offre il servizio, e (2) il *cliente*, cioè la persona o il gruppo che lo richiede e ne beneficia. Nello svolgimento dei servizi di consulenza, gli internal auditor dovrebbero mantenere l'obiettività e non assumere responsabilità di tipo manageriale.

Qualora leggi o regolamenti vietino agli internal auditor o all'attività di Internal Audit di operare in conformità con alcune parti degli Standard, essi dovranno tuttavia rispettarne tutte le altre parti e dare adeguata informativa.

Se gli Standard sono utilizzati congiuntamente con requisiti rilasciati da altri organismi riconosciuti, gli internal auditor possono comunicare nel modo più opportuno anche l'uso di altri requisiti. In tal caso, se l'attività di internal audit indica la conformità con gli Standard ed esistono differenze tra gli Standard e altri requisiti eventualmente adottati, gli internal auditor e l'attività di internal audit devono rispettare gli Standard e possono conformarsi ad altri requisiti solo se questi sono più restrittivi.

1.3.1 Il Codice Etico

Il Codice Etico dell'Institute of Internal Auditors ha lo scopo di promuovere la cultura etica nell'esercizio della professione di Internal Auditing e si estende oltre la definizione per includere due componenti essenziali: i *Principi*, fondamentali per la professione e la pratica dell'Internal Auditing sia a livello individuale che organizzativo, e le *Regole di Condotta*, ovvero norme comportamentali che gli internal auditor sono tenuti ad osservare con riferimento a ciascuno dei principi.

Il mancato rispetto del Codice Etico da parte dei membri dell'Institute, dei detentori delle certificazioni professionali e di coloro che si candidano a riceverle, sarà valutato e sanzionato secondo le norme previste nello Statuto e nelle "Administrative Directives" dell'Institute.

I principi che internal auditor è tenuto ad applicare sono quattro (Amato, 2017):

- *INTEGRITÀ*, che permette lo stabilirsi di un rapporto fiduciario e quindi costituisce il fondamento dell'affidabilità del suo giudizio professionale. Secondo tale principio, l'internal auditor:

a. deve operare con onestà, diligenza e senso di responsabilità.

b. deve rispettare le leggi e divulgare all'esterno solo se richiesto dalla legge e dai principi della professione.

c. non deve essere consapevolmente coinvolto in nessuna attività illegale, né intraprendere azioni che possano indurre discredito per la professione o l'organizzazione per cui opera.

d. deve rispettare e favorire il conseguimento degli obiettivi dell'organizzazione, quando etici e legittimi.

- *OBIETIVITÀ*, nel raccogliere, valutare e comunicare le informazioni attinenti l'attività o il processo in esame. Infatti, l'internal auditor:
  a. non deve accettare o partecipare ad alcuna attività o avere relazioni che pregiudichino o appaiano pregiudicare l'imparzialità della sua valutazione. In questo caso vanno incluse quelle attività o relazioni che possano essere in conflitto con gli interessi dell'organizzazione.
  b. deve riferire tutti i fatti significativi a lui noti, la cui omissione possa fornire un quadro alterato delle attività analizzate.
- *RISERVATEZZA*, rispettando il valore e la proprietà delle informazioni che riceve ed è tenuto a non divulgare senza autorizzazione, salvo che lo impongano motivi di ordine legale o deontologico. Egli:
  a. deve acquisire la dovuta cautela nell'uso e nella protezione delle informazioni acquisite nel corso dell'incarico.
  b. non deve usare le informazioni ottenute né per vantaggio personale, né secondo modalità che siano contrarie alla legge o di nocumento agli obiettivi etici e legittimi dell'organizzazione.
- *COMPETENZA*, nell'esercizio dei propri servizi professionali, utilizzando il bagaglio più appropriato di conoscenze, competenze ed esperienze. L'internal auditor:
  a. deve effettuare solo prestazioni per le quali abbia la necessaria conoscenza, competenza ed esperienza.
  b. deve prestare i propri servizi in pieno accordo con gli Standard Internazionali per la Pratica Professionale dell'Internal Auditing.
  c. deve continuamente migliorare la propria preparazione professionale (attraverso corsi di aggiornamento) nonché l'efficacia e la qualità dei servizi resi.

1.3.2 Gli Standard di Connotazione

Gli Standard di Connotazione raccolgono le caratteristiche richieste a singoli ed organizzazioni per lo svolgimento di servizi di internal audit (IIA, *Standard Professionali per la pratica professionale dell'Internal Auditing (Standard)*, 2016).

1000 – FINALITÀ, AUTORITÀ, RESPONSABILITÀ

"Le finalità, i poteri e le responsabilità dell'attività di internal audit devono essere formalmente definiti in un *Mandato di internal audit*, coerente con la Mission dell'Internal Auditing e con gli elementi vincolanti dell'International Professional Practices Framework (i Principi fondamentali per la pratica professionale dell'internal auditing, il Codice Etico, gli Standard e la Definizione di Internal Auditing). Il RIA deve verificare periodicamente il Mandato di internal audit e sottoporlo all'approvazione del senior management e del board."

Tale mandato è un documento formale che stabilisce la posizione dell'attività di internal audit nell'organizzazione, precisando la natura del riporto funzionale del RIA al Board, autorizza l'accesso ai dati, alle persone e ai beni aziendali che sono necessari per lo svolgimento degli incarichi e definisce l'ambito di copertura delle attività di internal audit. Deve inoltre essere predisposto in sede di costituzione della struttura della funzione ed approvato dal Vertice Aziendale e, nelle società ove presente (solitamente società quotate), dal Comitato del Controllo Interno.

Il mandato dovrebbe essere redatto in forma scritta, in quanto costituisce un veicolo formale per la revisione e l'approvazione del Vertice Aziendale, nonché per l'accettazione formale da parte del Consiglio di Amministrazione. Essa facilita la periodica valutazione dell'adeguatezza dell'attività di internal auditing quanto a finalità, poteri e responsabilità e consente, in caso contenzioso, di disporre di una prova formale dell'accordo con il management e il CdA. La mancanza del mandato definito ed approvato costituisce una rilevante carenza, che necessita di essere colmata con la massima priorità (Marcandalli, 2005).

1010 – Riconoscimento delle guidance vincolanti nel Mandato di internal audit

"Il carattere vincolante dei Principi fondamentali per la pratica professionale dell'internal auditing, del Codice Etico, degli Standard e della Definizione di Internal Auditing deve essere specificato nel Mandato di internal audit. Il RIA dovrebbe discutere la Mission dell'internal auditing e gli elementi vincolanti dell'International Professional Practices Framework con il senior management e il board."

1100 – INDIPENDENZA ED OBIETTIVITÀ

"L'attività di internal audit deve essere *indipendente* e gli internal auditor devono essere *obiettivi* nell'esecuzione del loro lavoro."

Indipendenza è la libertà da condizionamenti che minaccino la capacità dell'attività di internal audit di adempiere alle proprie responsabilità senza pregiudizi. Per raggiungere il livello di indipendenza necessario per adempiere efficacemente alle responsabilità di tale attività, il RIA ha diretto e libero accesso al senior management e al Board. Ciò può essere conseguito tramite un duplice riporto organizzativo ("dual reporting structure").

Obiettività è l'attitudine mentale di imparzialità che consente agli internal auditor di svolgere gli incarichi in un modo che consenta loro di credere nella validità del lavoro svolto e nell'assenza di compromessi sulla qualità. In materia di audit, l'obiettività richiede che gli internal auditor non subordinino il loro giudizio a quello di altri.

1110 – Indipendenza organizzativa

"Il RIA deve riportare a un livello dell'organizzazione che *consenta all'attività di internal audit il pieno adempimento delle proprie responsabilità*. Inoltre, deve *confermare al board*, *almeno una volta l'anno*, lo *stato di indipendenza organizzativa dell'attività di internal audit*."

L'indipendenza organizzativa si realizza con efficacia quando il RIA riferisce funzionalmente al Board. Ad esempio, il riporto funzionale al Board comporta che il esso:

- Approvi il Mandato di internal audit;
- Approvi il piano di audit risk based;
- Approvi il budget ed il piano delle risorse umane e finanziarie;
- Riceva comunicazioni sui risultati dell'attività e sulle materie rilevanti;
- Approvi la remunerazione del RIA;
- effettui opportune verifiche con il management e con il RIA per stabilire se sono presenti limitazioni non appropriate dell'ambito di copertura e delle risorse.

Nell'ultimo decennio molta strada è stata fatta per migliorare l'indipendenza della funzione di Internal Auditing, soprattutto sotto il punto di vista del corretto posizionamento organizzativo. Si è infatti passati da una situazione che prevedeva, fino agli anni '80, la dipendenza dalla struttura amministrativa, alla situazione attuale, in cui la funzione riporta generalmente al

Vertice Aziendale (Amministratore Delegato, Presidente e in alcuni casi Comitato di Controllo Interno).

In Italia, pare che la maggioranza delle funzioni di IA non operi ancora in una situazione che garantisca completamente la loro indipendenza, questo poichè i processi di definizione della retribuzione del RIA, di assunzione o rimozione dal ruolo e di assegnazione delle risorse non prevedono una sistematica valutazione e approvazione formale da parte di un organo di governo societario non esecutivo, come il Comitato di Controllo Interno o il Presidente (Paganini, 2007).

Le novità principali rispetto alla versione del 2013 sono rappresentate dall'introduzione dello Standard 1112, *Ruoli addizionali del RIA*, e dall'ampliamento dello Standard 1130, *Condizionamenti dell'indipendenza e dell'obiettività*.

Lo Standard 1112 cita:

"Laddove il RIA abbia, o si prevede abbia, ruoli e/o responsabilità che esulano dall'internal auditing, devono essere poste in essere opportune *misure di tutela* atte a *limitare i condizionamenti all'indipendenza o all'obiettività*."

Al RIA possono essere richiesti ruoli e responsabilità addizionali che esulano dall'internal auditing, come ad esempio la responsabilità per attività di Compliance o Risk Management. Tali ruoli e responsabilità possono condizionare, anche solo apparentemente, l'indipendenza organizzativa dell'attività di internal audit o l'obiettività individuale dell'internal auditor. Le misure di tutela sono quelle attività di supervisione, spesso intraprese dal Board, atte a indirizzare questi potenziali condizionamenti e possono comprendere attività come la valutazione periodica delle linee di riporto e delle responsabilità e lo sviluppo di processi alternativi per ottenere l'assurance sulle aree di responsabilità addizionali (Catani, 2017).

Lo Standard 1130, invece, sottolinea che, se indipendenza od obiettività sono compromesse o appaiono tali, le circostanze dei condizionamenti devono essere rese note ad appropriati interlocutori. Tra i fattori che possono di condizionamento si possono annoverare a titolo unicamente esemplificativo conflitti di interessi personali, limitazioni del campo di azione, restrizioni dell'accesso a dati, persone e beni e vincoli di risorse.

A questo standard è stato aggiunto il terzo punto (A3), che colma una lacuna precedente, fornendo indicazioni sul fatto che l'IA possa prestare servizi di assurance anche per quelle aree dove ha in precedenza svolto servizi di consulenza. Questo a patto che la natura della

consulenza non condizioni l'obiettività e che, nell'assegnazione delle risorse all'incarico, l'obiettività individuale sia salvaguardata.

1200 – COMPETENZA E DILIGENZA PROFESSIONALE

Gli incarichi devono essere effettuati con la dovuta competenza e diligenza professionale.

"Gli internal auditor devono possedere le *conoscenze*, *capacità* e *altre competenze* necessarie all'adempimento delle loro responsabilità individuali. L'attività di internal audit nel suo insieme deve possedere o dotarsi delle conoscenze, capacità e altre competenze necessarie all'esercizio delle proprie responsabilità." (Standard 1210)

Tra le capacità risultano la valutazione della situazione attuale, dei trend e delle tematiche emergenti, allo scopo di consentire la formulazione di pareri e raccomandazioni pertinenti. Essi sono incoraggiati a dimostrare la propria competenza conseguendo le opportune certificazioni e qualifiche professionali, come quella di "Certified Internal Auditor" (CIA) e altre certificazioni rilasciate da "The Institute of Internal Auditors" (IIA, sezione italiana AIIA) e da altri organismi professionali riconosciuti.

Inoltre, secondo lo Standard 1220, gli internal auditor devono applicare la *diligenza* e le *capacità* che ci si attende da un internal auditor ragionevolmente prudente e competente. Diligenza professionale non implica infallibilità.

1300 – QUALITY ASSURANCE and IMPROVEMENT PROGRAMM (QAIP)

La qualità è la formula magica per conquistare gli stakeholder.

"Il RIA deve sviluppare e sostenere un *programma di assurance e miglioramento della qualità* che copra tutti gli aspetti dell'attività di internal audit e ne verifichi continuamente l'efficacia."

Un *programma di assurance e miglioramento della qualità* adeguatamente implementato consente di effettuare una periodica valutazione di conformità dell'attività di internal audit agli Standard e per consentire di verificare se gli internal auditor rispettano il Codice Etico. Tale programma valuta l'efficienza e l'efficacia dell'attività di internal audit e consente di cogliere le opportunità per il miglioramento delle prestazioni, di far emergere e/o consolidare leading practice e di individuare nuove sorgenti per generare valore. Inoltre, il QAIP si compone di *valutazioni interne* e di *valutazioni esterne* indipendenti (Taralli, 2015).

Lo *Standard 1311* chiarisce che "le *valutazioni interne* devono includere (i) il monitoraggio continuo della prestazione dell'attività di IA, (ii) periodiche autovalutazioni o valutazioni condotte da altre persone interne all'organizzazione che abbiano conoscenze adeguate della pratica professionale di internal audit". Il monitoraggio continuo deve risultare concretamente attuato nella quotidiana attività di supervisione, verifica e misurazione dell'attività di IA e dovrebbe essere formalmente definito nei manuali o nelle procedure adottate internamente alla funzione. A seconda degli obiettivi strategici, delle dimensioni e del grado di informatizzazione della funzione di IA, possono essere variamente implementati utili strumenti di supporto al monitoraggio continuo, quali per esempio *checklist di conformità*, *key performance indicators (KPI)*, *timesheets* per la rilevazione dell'effettivo assorbimento delle risorse assegnate alle attività di audit, *skill inventories* per assicurare la corretta pianificazione delle risorse e per un'efficiente individuazione dei fabbisogni formativi dello staff ed infine *questionari* per intercettare le aspettative degli stakeholder e per misurare la *customer satisfaction*.

Per quanto concerne le autovalutazioni, il QAIP rappresenta un punto di riferimento fondamentale. Esso richiede un approccio sistematico e disciplinato al processo di autovalutazione e una review documentata di conformità per ciascuna area obbligatoria dell'IPPF. Le "*best practices*" dell'IIA prevedono che l'autovalutazione abbia almeno cadenza annuale e che "il RIA condivida i risultati, i piani d'azione necessari e la loro attuazione con il Senior Management ed il Board".

La fase più delicata del ciclo di quality assurance è rappresentata dalle *valutazioni esterne* "che devono essere effettuate una volta ogni cinque anni da parte di un valutatore o di un team di valutatori, qualificato e indipendente, esterno all'organizzazione", come stabilito dallo *Standard 1312*. Esse rappresentano una grande occasione di benchmarking, nonché un volano per lo sviluppo della funzione di IA in termini di miglioramento delle performance, identificazione di nuove opportunità di creazione di valore, incremento di visibilità all'interno dell'organizzazione e implementazione della customer experience. Terminata la valutazione, i valutatori esprimono un giudizio, formulato secondo il c.d. "Quality Assessment Manual" definito dall'IIA. Esso è espresso in funzione dell'applicazione e della conformità alla definizione di Internal Auditing, al Codice Etico e agli Standard, attraverso le seguenti modalità: *Generally Conforms*, *Partially Conforms* e *Does Not Conform* (Taralli, 2015).

1.3.3 Gli Standard di Prestazione

Gli Standard di Prestazione descrivono la natura dell'attività, forniscono criteri qualitativi in base ai quali è possibile valutarne la prestazione e identificano gli elementi fondamentali del processo di Internal Auditing (IIA, *Standard Professionali per la pratica professionale dell'Internal Auditing (Standard)*, 2016).

GRUPPO 2000 – GESTIONE DELL'ATTIVITÀ DI INTERNAL AUDIT

"Il RIA deve gestire efficacemente l'attività al fine di assicurare che essa *aggiunga valore all'organizzazione*." (Standard 2000)

L'attività di internal audit è gestita efficacemente quando:

- raggiunge le finalità e le responsabilità indicate nel *Mandato di internal audit*;
- è conforme agli *Standard*;
- i suoi singoli membri rispettano il *Codice Etico* e gli *Standard*;
- tiene in considerazione i trend e le tematiche emergenti che potrebbero influire sull'organizzazione.

L'IA aggiunge valore all'organizzazione e ai suoi stakeholder, invece, quando tiene in considerazione le strategie, gli obiettivi e i rischi, si adopera per fornire soluzioni per migliorare i processi di governance, di gestione del rischio e di controllo e fornisce in via oggettiva assurance rilevante.

Secondo lo Standard 2010, "il RIA deve predisporre un *piano* (c.d. Piano di Audit) basato sulla *valutazione dei rischi* al fine di determinare le priorità dell'attività di internal audit in linea con gli obiettivi dell'organizzazione."

Per predisporre il piano *risk based*, il RIA si consulta con il Senior Management e il Board per comprendere le strategie, i principali obiettivi di business, i rischi associati e i processi di Risk Management dell'organizzazione. Egli deve rivedere e adeguare opportunamente il piano, in risposta ad eventuali cambiamenti intervenuti a livello di attività, rischi, operatività, programmi, sistemi e controlli dell'organizzazione. Inoltre, deve definire un "tempo di copertura" dei rischi ritenuti prioritari, la cui stima può essere effettuata sulla base delle indicazioni raccolte in fase di valutazione e/o sulla base delle informazioni relative ad attività pregresse e deve tener conto dell'ambito di copertura dell'audit da effettuare e delle risorse a disposizione della funzione.

Tale piano deve basarsi su una documentata valutazione del rischio (Risk Assessment), effettuata almeno una volta l'anno, e deve contenere (Mancini, 2017):

- ✓ gli obiettivi ed i criteri di redazione;
- ✓ la programmazione delle attività (natura, periodo);
- ✓ il budget annuale;
- ✓ le modalità di reporting.

Perché il piano sia valido, una volta predisposto, deve essere sottoposto all'esame e all'approvazione del Senior Management e del Board (Standard 2020).

Il RIA, inoltre, ha il compito di assicurare che le risorse disponibili siano *adeguate*, ovvero che siano in possesso delle conoscenze e competenze, *sufficienti* ed *efficacemente impiegate* per ottimizzare l'esecuzione del piano approvato (Standard 2030) e di definire *direttive* e *procedure*, necessarie a guidare l'attività di internal audit (Standard 2040).

Nel coordinamento dell'attività, il RIA ha la possibilità di fare affidamento su terzi per i servizi di assurance e consulenza, dovendo però preventivamente valutarne la competenza, l'obiettività e la diligenza professionale e definire congiuntamente obiettivi e risultati attesi.

Un elemento fondamentale è rappresentato dalla *comunicazione con il Board ed il Senior Management* (Standard 2060), i quali non solo sono attivamente coinvolti nell'approvazione del piano, ma devono anche essere periodicamente informati sul suo stato di avanzamento e sulla conformità dell'attività al Codice Etico e agli Standard. Tale comunicazione deve comprendere i rischi significativi, inclusi quelli di frode, i problemi di controllo e governance e ogni altra questione che necessita di essere sottoposta alla loro attenzione. Frequenza e tipologia dei contenuti delle comunicazioni sono definiti in maniera condivisa dal RIA, dal Senior Management e dal Board e variano a seconda della rilevanza delle informazioni che devono essere comunicate e dall'urgenza delle azioni correlate.

GRUPPO 2100 – Natura dell'attività

L'attività di internal audit deve valutare e contribuire al miglioramento dei *processi di governance*, per esempio attraverso la promozione dei valori e dei principi etici all'interno dell'organizzazione, la consulenza nelle decisioni di natura strategica ed operativa e la proposta di procedure e direttive che possano rendere efficiente il coordinamento delle attività e dei processi di scambio delle informazioni; *di gestione del rischio*, monitorando la coerenza degli obiettivi con la mission dell'organizzazione ed identificando i rischi significativi, per i quali devono essere individuati opportuni piani d'azione; e *di controllo dell'organizzazione*,

mantenendoli efficaci ed efficienti, tutto ciò tramite un approccio sistematico, rigoroso e risk based. La credibilità e il valore dell'IA sono rafforzati quando gli auditor agiscono in maniera proattiva (e non reattiva) e le loro valutazioni offrono nuove riflessioni e tengono in considerazione gli impatti futuri.

GRUPPO 2200 – PIANIFICAZIONE DELL'INCARICO

Il Gruppo 2200 è composto dagli Standard che definiscono la pianificazione dell'attività di internal audit, integrando importanti elementi allo Standard 2010 (Piano di Audit). A tal proposito lo Standard 2200 cita: "Per ciascun incarico gli internal auditor devono predisporre e documentare un *piano* che comprenda gli *obiettivi dell'incarico*, l'*ambito di copertura*, la *tempistica* e l'*assegnazione delle risorse*. Il piano deve tenere in considerazione le strategie e gli obiettivi dell'organizzazione nonché i rischi attinenti l'incarico".

Precedentemente alla pianificazione, l'attività oggetto di revisione deve essere valutata in termini di rischio e gli obiettivi dell'incarico devono rispecchiare i risultati di tale valutazione, per la quale sono necessari adeguati criteri stabiliti dal Board e/o dal Senior Management (Standard 2210). Una volta definiti gli obiettivi, il RIA deve considerare il grado di probabilità che esistano errori significativi, frodi, non conformità e altre situazioni pregiudizievoli. Esistono varie tipologie di criteri: *interni* (ad esempio direttive e procedure dell'organizzazione), *esterni* (ad esempio leggi e regolamenti imposti dagli organismi competenti) e *prassi esistenti* (ad esempio linee guida di settore e professionali).

Il RIA deve inoltre notificare con un certo anticipo l'intervento, evitando ogni tipo di "sorpresa", attraverso la comunicazione dell'*Avviso di Audit*, che sarà indirizzata a tutti i soggetti interessati (come ad esempio il Responsabile della funzione interessata). La notifica dell'intervento deve comprendere gli obiettivi della verifica, la composizione del team che effettuerà l'attività di audit, il "tempo di copertura" ed il modus operandi (Mancini, 2017).

Una volta condiviso l'avviso, è necessario definire un *programma di audit*, ovvero la lista dei controlli e delle verifiche che dovranno essere svolte in funzione degli obiettivi e dell'estensione dell'incarico, definiti in base alle "best practices", ai precedenti audit oppure all'esperienza del RIA (Standard 2240).

GRUPPO 2300 – ESECUZIONE DELL'INCARICO

Al fine di raggiungere gli obiettivi dell'incarico, il RIA deve raccogliere informazioni sufficienti, le quali devono essere affidabili, pertinenti e utili in modo tale da favorire ogni

tipo di analisi e valutazione. Vi sono molteplici modalità di ottenimento di tali informazione, tra cui:

- *interviste*, dove l'auditor deve sia saper far parlare i soggetti coinvolti nell'audit (principalmente attraverso domande aperte), sia saper ascoltare;
- *questionari*, i quali possono essere vantaggiosi in quanto standardizzabili, ma potrebbero non portare a risultati veritieri;
- *workshop*, utili per ottenere informazioni dal management operativo;
- *campionamento*, il quale fornisce una rappresentazione della realtà dell'universo con un grado misurabile di affidabilità;
- *procedimenti analitici di audit*, basati sul confronto o relazione fra grandezze per identificare eventuali andamenti anomali.

Il RIA deve però ricordare, durante le valutazioni, di non saltare a conclusioni affrettate sulla base di sole interviste o senza adeguata documentazione a supporto. Ciò rappresenta una "trappola" da evitare (Mancini, 2017).

Ogni tipo di controllo, valutazione effettuata o informazione ottenuta deve essere documentata all'interno delle c.d. "*carte di lavoro*", le quali facilitano la supervisione del RIA e possono rappresentare una fonte per lo svolgimento di futuri audit.

GRUPPO 2400 – COMUNICAZIONE DEI RISULTATI

Il RIA è tenuto a comunicare i risultati dell'incarico, che devono contenere il relativo esito della valutazione, le anomalie o criticità, la causa che ha portato ad esse, l'effetto che potrebbero causare ed infine i suggerimenti e/o i piani d'azione. Laddove appropriato, il egli dovrebbe esprimere un giudizio, tenendo però in considerazione le aspettative del Senior Management, del Board e degli altri stakeholder. Tale giudizio deve essere accompagnato da adeguata documentazione a supporto.

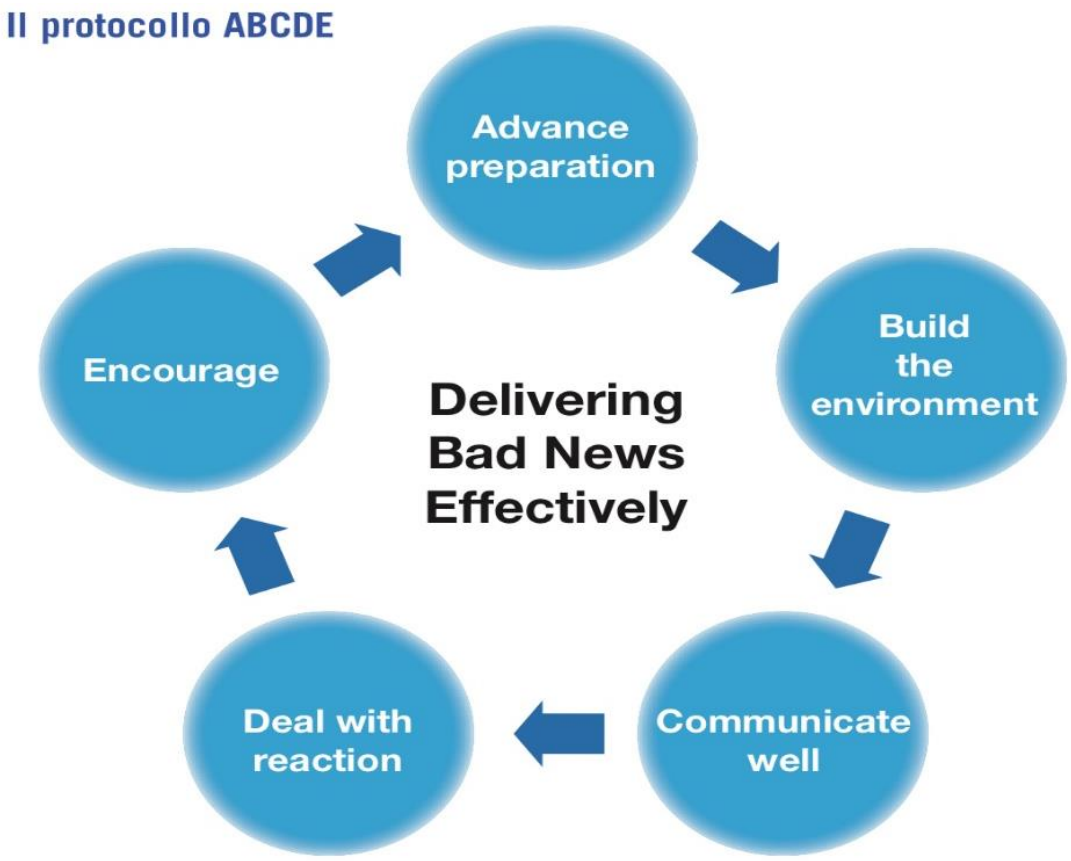
La comunicazione dei risultati inoltre deve essere *accurata*, priva di errori e distorsioni, *obiettiva*, corretta, imparziale e scevra da pregiudizi, *chiara*, facilmente comprensibile, *concisa*, che evita formulazioni non necessarie o dettagli superflui, *costruttiva*, che induce miglioramenti laddove necessari, *completa*, che contiene tutti gli elementi essenziali per i destinatari, e *tempestiva*, ovvero puntuale e opportuna nei tempi, che consente al management di intraprendere le necessarie azioni correttive (Standard 2420). La divulgazione dei risultati, soprattutto quando essi sono negativi, rappresenta un impegno delicato che un approccio consapevole può rendere efficace e costruttivo. La necessità di comunicare informazioni che

possono essere percepite come negative non è esclusiva degli auditor, ma abbraccia professionisti di qualsiasi disciplina, i quali hanno sviluppato protocolli basati su principi applicabili a qualsiasi tipo di comunicazione (Archabeault e Rose, 2010).

La comunicazione *face to face* con il management diviene sicuramente la più indicata per la divulgazione di risultati negativi ed uno dei protocolli più utilizzati viene definito con l'acronimo "*ABCDE*", il quale riassume la seguente strategia:

1. "*Advance preparation*": consiste in un'adeguata preparazione preliminare. Gli internal auditor possono evitare perdite di tempo ed errori analizzando accuratamente i fatti e le evidenze in proprio possesso prima di divulgarli e dovrebbero sforzarsi di immaginare e prefigurare quali potranno essere le reazioni e le richieste di approfondimento dei soggetti a cui l'audit è rivolto. È molto meglio scoprire prima le possibili difficoltà che possono sorgere e risolverle da soli o con i propri colleghi, piuttosto che nel bel mezzo di una riunione con l'Alta Direzione.
2. "*Build the environment*": creare l'ambiente giusto può essere un fattore determinante, in quanto dovrebbe consentire al RIA di mantenere il controllo della situazione e degli eventuali sviluppi. Egli dovrebbe scegliere il luogo adatto, evitando distrazioni che possano nuocere la produttività dell'incontro.
3. "*Communicate well*": il RIA dovrebbe utilizzare un linguaggio chiaro e diretto per comunicare le cattive notizie, conservando tuttavia un'attenta sensibilità rispetto alle possibili reazioni. Infatti, sarebbe opportuno evitare parole troppo esplicite (per esempio "*frode*") o che possano essere ritenute in qualche modo offensive. Inoltre, è necessario presentare prove e dati oggettivi emersi nel corso della verifica che accompagnino i risultati comunicati per rendere più comprensibile e condivisibile il messaggio.
4. "*Deal with reactions*": il RIA deve saper gestire ed essere pronto a rispondere alle richieste, preparandosi preventivamente sulle possibili domande e avendo sottomano tutta la documentazione di supporto.
5. "*Encourage*": una volta comunicati i risultati, il Board deve prendere le decisioni necessarie a mitigare o eliminare definitivamente le criticità riscontrate. In questo contesto, il RIA può offrire supporto e suggerimenti costruttivi. Ciò rappresenta il contributo più grande all'intero processo.

Figura 9: *protocollo "ABCDE"* (*The ABCs of Communicating Results*, The IIA, 2010)



GRUPPO 2500/2600 – FOLLOW-UP

Il *follow-up* è il processo, stabilito dal RIA, mediante il quale viene determinata l'adeguatezza, l'efficacia e la tempestività delle azioni correttive intraprese dal management in risposta a suggerimenti e raccomandazioni ed include l'accettazione del rischio da parte del management di non intraprendere alcuna azione. Se quest'ultima situazione si dovesse presentare ed il RIA valutasse tale rischio come inaccettabile per l'organizzazione, egli deve capire su quale base il management ha fondato la propria decisione e stabilire se abbia l'autorità per accettare il rischio in questione. È preferibile che il RIA risolva l'eventuale disaccordo e qualora non riuscisse, è tenuto ad informare il Board.

1.3.4 Uno sguardo al domani

Negli ultimi anni, grazie anche alla revisione degli Standard che ha trasformato i concetti in regole pratiche, le competenze che determinano il successo dell'IA si sono evolute. In particolare, l'internal auditor, oltre a possedere le competenze tecniche e una vasta gamma di soft skills, deve essere proattivo (*proactive*) ed orientato al futuro (*future-focused*).

Infatti, al fine di creare valore aggiunto per l'organizzazione, l'analisi svolta dalla funzione di IA deve essere *lungimirante*, deve ossia tenere in considerazione non solo i rischi attuali, ma soprattutto quelli derivanti da potenziali cambiamenti ed eventi che, in un futuro prossimo, potrebbero coinvolgere l'organizzazione. Perciò, è necessario un continuo e costante aggiornamento tanto sull'attività e sui cambiamenti del contesto interno, quanto sull'ambiente socio-economico nazionale ed internazionale. In un momento storico come quello attuale, ricco di grandi e veloci cambiamenti, la caratteristica principale che l'internal auditor deve possedere è la *curiosità*, ovvero la volontà di capire ed interessarsi a quegli aspetti che vanno oltre la semplice pratica professionale (Cianfarani, 2017).

Ciò significa agire proattivamente, anticipando l'incertezza, attrezzarsi con nuove conoscenze e competenze ed essere flessibili in modo tale da poter adattare il proprio Piano di Audit. Essere "*future-focused*" implica l'adozione di adeguati strumenti informatici ed un ulteriore cambiamento metodologico: l'internal auditor deve evitare di concentrarsi sul passato e focalizzarsi sull'organizzazione di oggi e di domani.

2. RISK MANAGEMENT

Negli ultimi anni, in un contesto macroeconomico in cui la vulnerabilità delle imprese è aumentata costantemente, si è assistito ad una costante crescita del bisogno di gestire il rischio in modo sempre più efficace e rigoroso, ponendo appunto tale bisogno sempre più al centro dell'attenzione di amministratori e manager, i quali continuano ad interrogarsi sulle modalità di individuazione, misurazione e trattamento dei rischi aziendali in un'ottica sistematica. Le aziende, infatti, hanno la necessità di comprendere il livello complessivo di rischio insito nei loro processi e nelle loro attività. Ciò implica il riconoscere e dare priorità ai rischi più significativi, individuare le criticità, riconoscere le debolezze dei controlli, arrivando ad attuare un efficace processo di Risk Management. Tali esigenze hanno portato alla ricerca e all'adozione di processi sempre più strutturati, in grado di contribuire ad assicurare che il rischio sia gestito efficacemente e in maniera coerente rispetto all'organizzazione nel suo complesso (ANRA, 2011).

Con il termine Risk Management (gestione del rischio) si intende l'insieme di processi attraverso cui un'azienda identifica, analizza, quantifica, elimina e/o monitora i rischi legati ad un determinato processo produttivo con l'obiettivo di minimizzare le perdite e massimizzare l'efficacia e l'efficienza dei processi produttivi (Amato, 2017). In realtà si tratta, più che di un singolo processo, di un insieme articolato di processi attraverso cui le aziende valutano dapprima la probabilità che si verifichi una determinata situazione e successivamente valutano il modo di evitarla, ridurne gli effetti, trasferirla a terzi o infine in molti casi accettarne in parte o totalmente le conseguenze minimizzando gli impatti sull'attività di impresa.

Secondo lo Standard 2120 (Standard Professionali per la pratica professionale dell'Internal Auditing), anche l'IA detiene un ruolo importante all'interno del Risk Management, infatti egli "deve valutare l'efficacia e contribuire al miglioramento dei processi di gestione dei rischi".

Nell'espressione di tale giudizio l'internal auditor deve valutare se gli obiettivi aziendali supportano o sono coerenti con la mission dell'organizzazione, se i rischi significativi sono identificati e valutati adeguatamente, se le c.d. "risk response" vengono individuate ed in seguito applicate, ed infine se le informazioni sui rischi vengono diffuse tempestivamente all'interno dell'organizzazione consentendo a Board e Management di adempiere alle rispettive responsabilità.

Inoltre, l'IA ha il compito di sviluppare un Piano di Audit "*Risk Based*" (in quanto tiene conto dei rischi aziendali), considerando il framework utilizzato per la gestione del rischio ed il "risk appetite" (propensione al rischio) stabilito dal Management per le diverse attività.

2.1 SCI & RISK MANAGEMENT: COSO Report vs. ERM

Alla fine degli anni '80, sull'onda emotiva creata da una serie di fallimenti e malversazioni che interessarono gli Stati Uniti, il mondo professionale concentrò la propria attenzione sulle carenze dei sistemi di corporate governance esistenti. Pochi anni dopo, analoghe problematiche si manifestarono anche in Regno Unito ed in altri paesi occidentali.

La risposta a questa situazione fu lo sviluppo di modelli attraverso i quali si cercò di razionalizzare e mettere a fattor comune le conoscenze dei sistemi di controllo interno a favore dei diversi portatori di interesse. Negli USA tale istanza di rinnovamento si concretizzò nella pubblicazione, nel 1992, del modello denominato "Internal Control Integrated Framework – CoSo Report". Anche negli altri paesi, soprattutto quelli europei, grazie all'armonizzazione dei sistemi di governance nell'ambito della Unione Europea, furono sviluppati tali modelli più o meno negli stessi anni, i quali nel corso del tempo sono stati oggetto di modifiche ed integrazioni (Casana, 2005).

Nei primi anni del XXI secolo, la necessità delle organizzazioni di affrontare e gestire sempre di più eventi incerti per sopravvivere, diede vita alla pubblicazione del modello Enterprise Risk Management (ERM), il quale incorpora totalmente il CoSo Report, ampliandone la portata. Ciò portò il Management ad adattare le decisioni in termini di rischio in modo tale da massimizzare il valore per gli stakeholder, determinando un livello di incertezza considerato accettabile. Tale massimizzazione si ottiene una volta raggiunto l'equilibrio ottimale tra redditività e rischi e quando le risorse vengono impiegate in modo efficace ed efficiente.

2.1.1 Il CoSo Report

"*CoSo*" è l'acronimo del "Committee of Sponsoring Organisations of the Treadway Commission". Tale comitato fu formato nel 1985 per supportare la *National Commission on Fraudulent Financial Reporting*, un'iniziativa indipendente voluta da privati per analizzare le condizioni che possono portare a frodi finanziarie celate in false comunicazioni sociali. Di

fatto tale organismo ha acquistato nel tempo il ruolo di principale referente in tema di sistemi di controllo interno.

Il *Coso Report* (1992) definisce il controllo interno come "un processo, svolto dal Consiglio di Amministrazione, dai dirigenti e dagli operatori della struttura aziendale, che si prefigge di fornire una ragionevole sicurezza sulla realizzazione degli obiettivi rientranti nelle seguenti categorie: efficacia ed efficienza delle attività operative (*operations*), affidabilità delle informazioni di bilancio (*reporting*) e conformità alle leggi e ai regolamenti in vigore (*compliance*)".

Questa definizione racchiude dei concetti fondamentali, quali il fatto che il controllo interno sia un processo, ovvero un mezzo per raggiungere un fine, e che sia svolto da persone, e quindi non si tratti solamente di un insieme di procedure raccolte in manuali o altri documenti. In particolare, è necessario sottolineare come le responsabilità non siano assegnate esclusivamente ad alcune specifiche funzioni (per esempio l'IA), ma a tutti i membri dell'organizzazione a qualunque livello gerarchico. Inoltre, dalla definizione si evince che il sistema di controllo interno garantisce solamente una ragionevole sicurezza di raggiungimento degli obiettivi e non una sicurezza assoluta.

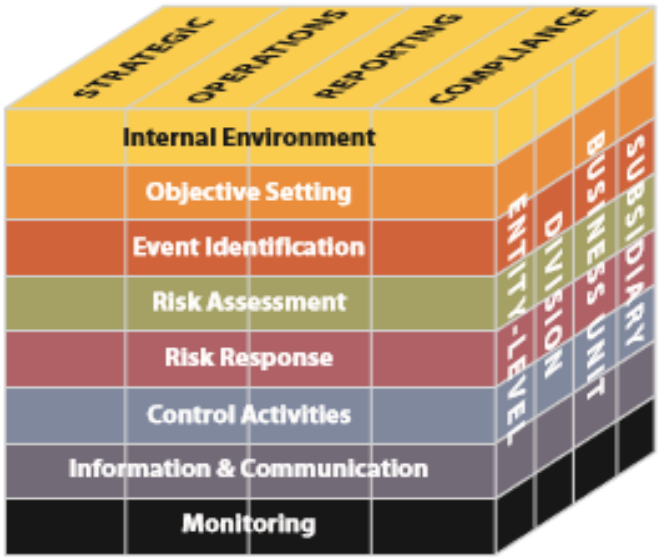
Secondo il CoSo Report, un efficace sistema di controllo nasce dall'interazione di cinque componenti (Control Envirorment, Risk Assessment, Control Activities, Information & Communication, Monitoring), i quali lavorano congiuntamente per il conseguimento degli obiettivi dell'organizzazione. Tali componenti (Figura 10) trovano una logica integrazione ed evoluzione nelle novità proposte dal ERM.

Figura 10: *CoSo Report* (Materiale Didattico AIIA, Sistema di Controllo Interno e di Gestione dei Rischi, *Diploma in Controllo e Internal Auditing*, 2017)

2.1.2 Il modello ERM

L'*Enterprise Risk Management* (Figura 11) è sempre più presente nelle diverse realtà aziendali, nel senso che sempre più attori del sistema economico si sono posti il problema dell'identificazione, valutazione e gestione dei rischi da un punto di vista integrato che coinvolga l'intera azienda. Tale modello, presentato ufficialmente il 29 settembre 2004 a New York, consente alle organizzazioni un confronto per valutare ed eventualmente migliorare il proprio processo di Risk Management. Per fare ciò, all'ERM Framework è stato associato un ulteriore documento, denominato "Application Techniques", il quale appunto offre modalità per l'applicazione delle tecniche di ERM alla propria azienda (Casana, 2015).

Figura 11: *il modello ERM* (ERM – Integrated Framework, *Executive Summary*, CoSo, 2004).



La definizione fornita dal Committee of Sponsoring Organizations of the Treadway Commission (CoSo, 2004) è la seguente:

"Enterprise Risk Management is a process, effected by an entity's board of directors, management and other personnel, *applied in strategy setting* and *across the enterprise*, designed to identify potential events that may affect the entity, and manage risk to be within its *risk appetite*, to provide reasonable assurance regarding the achievement of entity objectives".

Si tratta di un processo, svolto dal Board, dal Management e da altro personale, utilizzato per fissare le strategie all'interno dell'organizzazione, disegnato per identificare gli eventi

potenziali che potrebbero influenzarla e per gestire i rischi riconducendoli nell'ambito del "risk appetite", in modo tale da fornire una ragionevole sicurezza circa il raggiungimento degli obiettivi aziendali. Come si può notare, i concetti chiave presenti nel CoSo Report si ritrovano in tale definizione, ma di maggior interesse sono i cambiamenti che l'ERM introduce:

- "***Applied in strategy setting***": una delle principali novità è rappresentata dal diverso livello cui il modello si rivolge, viene infatti ampliato il range degli obiettivi interessati, comprendendo quelli strategici. Con il CoSo Report il rischio veniva identificato esclusivamente come un evento incerto, da cui potevano scaturire effetti negativi o positivi (opportunità). Ora invece, tali opportunità, in caso dovessero emergere dall'analisi, vengono valutate e fatte risalire tra gli obiettivi strategici.
- "***Across the enterprise***": le diverse componenti di un'organizzazione affrontano una molteplicità di rischi tra loro variamente correlati. Un aspetto innovativo del framework risiede proprio nel porre in evidenza la necessità di affrontare i rischi ed i loro potenziali impatti in modo integrato, analizzando le relazioni tra loro esistenti e non solo valutandoli singolarmente. Tale approccio viene definito "portfolio views of risk" e rende possibile la definizione di risposte efficaci ed efficienti.
- "***Risk appetite***": tale concetto non è del tutto nuovo, ma il suo inserimento all'interno del modello lo fa apparire come tale. Si tratta del *livello di rischio che un'organizzazione è disposta ad accettare nel perseguimento dei propri obiettivi*, ovvero la c.d. "propensione al rischio". Esso costituisce un elemento che permea l'intera organizzazione, dalla valutazione delle alternative strategiche alla definizione degli obiettivi allineati alle scelte fatte e che, infine, deve condizionare la definizione dei processi operativi di gestione dei rischi connessi a tali obiettivi.

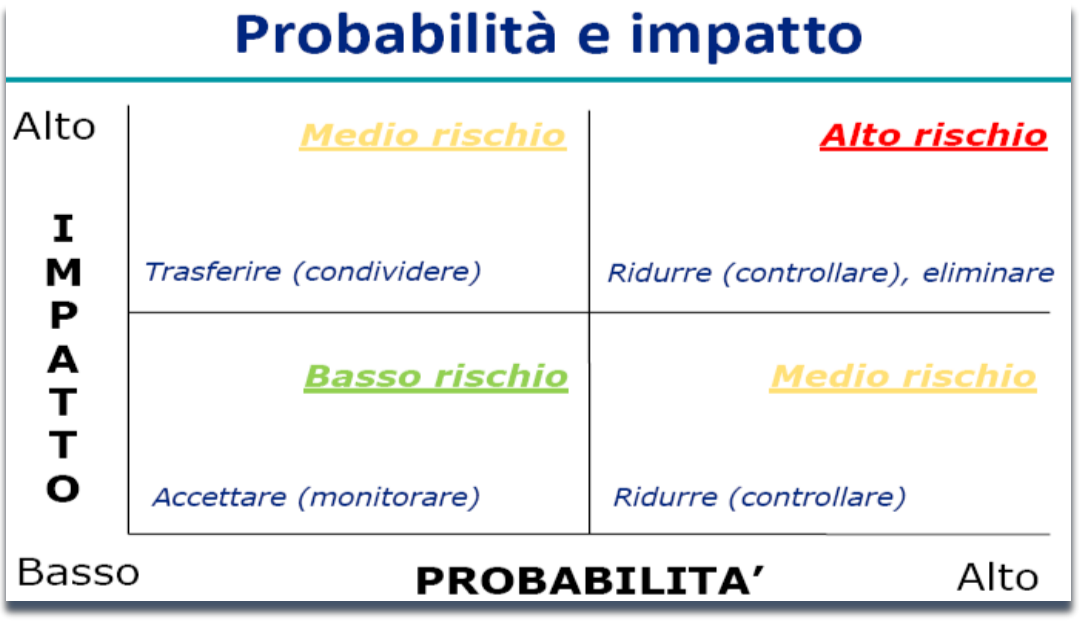
L'ERM incorpora di fatto il suo predecessore, il CoSo Report, ribaltando la logica con la quale il modello stesso era stato costruito. Infatti, l'attenzione non si concentra più sul controllo, bensì sul rischio. La stessa validità del controllo dipende dalla sua capacità di mantenere il rischio entro un certo livello predefinito (risk appetite). La relazione tra CoSo Report ed ERM è sinteticamente individuata nelle parole di Andrew J. Jackson, uno dei membri del Project Advisory Council del CoSo: "Possiamo considerare l'ERM Framework come una versione "turbo" o "extra lusso" dell'Internal Control – Integrated Framework. Esso non solo annovera tre componenti aggiuntive, *objective setting*, *event identification* e *risk*

response, ma le cinque componenti che derivano dal modello precedente sono di più vasta portata in termini sia di descrizione sia di guide applicative".

Infatti, come illustrato in Figura 11, le componenti del modello ERM sono precisamente otto (Executive Summary, CoSo, 2004):

1. *Internal Envirorment* (ambiente interno), il quale racchiude l'identità essenziale dell'organizzazione e pone le basi per il modo in cui il rischio viene visto ed indirizzato dagli stakeholder interni, inclusi la filosofia di Risk Management ed il "risk appetite", l'integrità, i valori etici e l'ambiente di riferimento in cui l'organizzazione opera.
2. *Objective Setting* (definizione degli obiettivi), che devono essere posti in essere prima che il Management possa identificare gli eventi che potrebbero influenzare i risultati aziendali. È necessario che tali obiettivi siano allineati alle strategie, espressi in modo chiaro e misurabile e coerenti con il "risk appetite".
3. *Event Identification* (identificazione degli eventi), necessaria per rispondere ad accadimenti interni ed esterni all'azienda che possono influenzare le strategie ed il raggiungimento degli obiettivi. Tali eventi possono rappresentare dei rischi (eventi negativi) o delle opportunità (eventi positivi).
4. *Risk Assessment* (valutazione del rischio), ossia l'analisi dei rischi, considerando probabilità ed impatto, per determinare come essi dovrebbero essere gestiti (Figura 12).

Figura 12: *Risk Assessment e Risk Response* (Materiale didattico AIIA, Sistema di Controllo Interno e di Gestione dei Rischi, *Diploma in Controllo e Internal Auditing*, 2017)



5. *Risk Response* (risposta al rischio), selezionata dal Management – evitarlo, accettarlo, gestirlo, trasferirlo – e valutata in relazione alla "risk tolerance" ed al "risk appetite" dell'organizzazione.
6. *Control Activities* (attività di controllo), fase in cui vengono stabilite ed implementate le policies e le procedure in modo tale da assicurare che le risposte al rischio e le direttive aziendali siano messe in pratica.
7. *Information & Communication* (informazione e comunicazione), in cui il Management identifica, raccoglie e comunica le informazioni pertinenti con modalità e tempistiche che rendono possibile l'adempimento delle diverse responsabilità. La comunicazione deve fluire in tutta l'azienda ed in tutte le direzioni (orizzontalmente, top-down, bottom-up).
8. *Monitoring* (monitoraggio) nel tempo dell'efficacia delle altre componenti del modello, le cui modalità sono scelte dal Management (self assessment, checklist, questionari, diagrammi, benchmarking, …).

L'ERM non consiste in un processo "in serie", dove un componente influenza solamente il successivo, ma si tratta di un processo multidirezionale ed interattivo, nel quale quasi ogni componente può influenzarne un altro.

Sebbene tale modello porti importanti benefici, esistono alcune limitazioni. Esse derivano da possibili errori di giudizio nel processo decisionale, dalla necessità di considerare il rapporto costi – benefici per le decisioni in termini di "risk response" e per l'instaurazione di controlli, dalla possibilità di aggirare i controlli da parte di due o più persone in collusione e dalla facoltà del Management di eludere le decisioni inerenti alla gestione del rischio. A causa di tali limitazioni non è possibile ottenere una *sicurezza assoluta* sul conseguimento degli obiettivi aziendali.

Nell'anno precedente, più precisamente il 6 settembre 2017, il CoSo ha emesso il nuovo framework, denominato "ERM – Aligning Risk with Strategy and Performance", con l'obiettivo di definire come l'allineamento di rischio, strategia e performance possano generare opportunità per migliorare le prestazioni del business e per creare, salvaguardare e realizzare valore (Cregut, 2017).

2.2 IL PROCESSO DI RISK ASSESSMENT

Il "Risk Assessment" o "valutazione del rischio" è uno specifico processo del Risk Management di fondamentale importanza, tanto da esser divenuta una disciplina a sé stante. Essa consiste nella valutazione dei potenziali eventi (o pericoli, c.d. "*hazards*") e nella determinazione dei rischi inerenti che possono avere un impatto negativo sugli obiettivi dell'organizzazione. Tale analisi non dovrebbe solamente identificare i pericoli ed i loro potenziale effetti, bensì fornire appropriate misure e processi di controllo necessari a ridurne o eliminarne l'impatto sulle attività. Talvolta il Risk Manager richiede l'intervento di professionisti particolarmente esperti nella valutazione di specifici rischi.

Tale disciplina può essere applicata ai più svariati settori di attività e promossa nell'ambito dei processi generali richiesti dai manager volti al miglioramento dell'organizzazione, alla qualità ed alla protezione degli assets, e, in taluni casi, può essere imposta dall'autorità a seguito dell'entrata in vigore di leggi speciali.

Il processo di "Risk Assessment" è suddiviso in tre fasi principali (Amato, 2017):

1. *Analisi preliminare*
2. *Identificazione e classificazione del rischio*
3. *Misurazione del rischio e Risk Scoring*

1. Analisi preliminare

Come primo step della valutazione del rischio è necessario ottenere un approfondito grado di conoscenza della realtà in analisi, considerandone il contesto socio-economico e normativo, assieme al mercato in cui l'organizzazione opera ed ai relativi obiettivi strategici ed operativi. Partendo da ciò, viene analizzata non solo la catena del valore aziendale, ma anche la totalità dei processi di ogni funzione, verificando prima di tutto che gli obiettivi siano coerenti con quelli dell'organizzazione.

2. Identificazione e classificazione dei rischi

La fase successiva è inizialmente dedicata all'organizzazione di incontri e meeting con i vari responsabili aziendali, reali conoscitori dei rischi associabili alla propria funzione. Questo approccio consente di ottenere un quadro ampio della rischiosità aziendale, focalizzando l'attenzione sui rischi che ci si è prefissati di analizzare. Poiché l'identificazione dei rischi è multidisciplinare e trasversale all'intera azienda, il processo può risultare complesso e

pertanto va affrontato con una metodologia di indagine sistematica e rigorosa. In linea generale viene posta l'attenzione su due aspetti principali: la *raccolta di informazioni*, volta a raccogliere ed analizzare gli aspetti chiave per gli specifici rischi oggetto dell'analisi, e le *tecniche di identificazione*, da decidere in funzione dell'obiettivo, dei tempi e delle risorse a disposizione, come ad esempio la revisione documentale, i workshop, le interviste ed il CRSA (Control & Risk Self Assessment).

L'aspetto fondamentale da decidere iniziando ad implementare un processo di identificazione consiste nell'individuare la tipologia dei rischi che si vogliono mappare, definita come "classificazione dei rischi". L'insieme dei rischi a cui una realtà può essere esposta consiste di molteplici elementi, che possono infatti essere classificati in base al perimetro in cui emergono (internamente o esternamente all'azienda), al contesto a cui si riferiscono (Figura 13, categorie: *strategici*, *operativi*, *financial reporting* e *di conformità*) o a diverse classificazioni omogenee in base alla necessità.

Figura 13: *Risk Model per categoria* (Materiale didattico AIIA, Risk Management. *La definizione del Piano di Audit ed il processo di Audit*, 2017)

RISK MODEL	
Categoria	*Sottocategoria*
Strategici	Concorrenza Regolamentare/Normativo Reputazione Evoluzione del mercato e della tecnologia Fornitori e clienti Eventi naturali o accidentali Situazione politica
Operativi	Risorse Umane Legale Finanziari Processi e procedure Sistemi IT Salute, ambiente e sicurezza Atti illeciti Sistemi infrastrutturali Delega dei poteri

Financial Reporting	Schemi di bilancio Situazioni trimestrali Sistema di reporting, KPI
Conformità	D.Lgs. 231, 262, *privacy*, SOX, ecc. Antitrust, riciclaggio Trasparenza e anticorruzione Normativa di settore

3. Misurazione dei rischi e Risk Scoring

La valutazione del rischio aziendale viene solitamente effettuata combinando tecniche qualitative e quantitative.

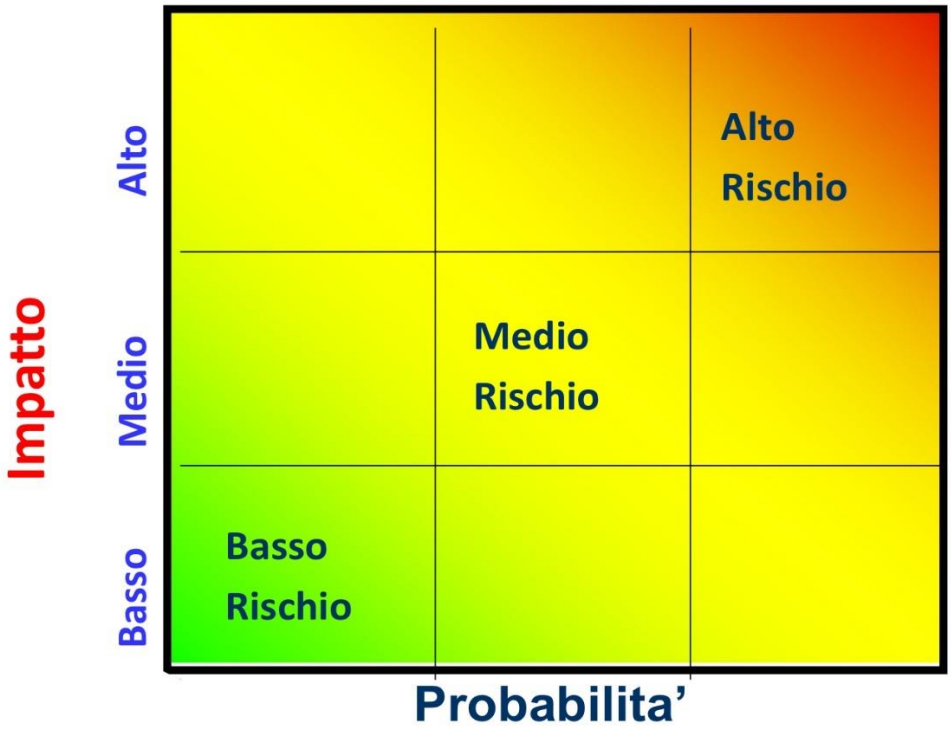
Le *tecniche qualitative* sono utilizzate quando la tipologia dei rischi da valutare non può essere quantificata, quando i dati necessari per una corretta quantificazione non sono disponibili e/o quando la ricerca e l'analisi dei dati risulta molto onerosa. L'obiettivo di tali tecniche è di classificare in ordine decrescente le attività oggetto di rischio in base a scale di valutazione (ad esempio rischio alto, medio, basso, vedi figura 14) o numeriche (per esempio assegnando un punteggio da 1 a 10).

In tal caso i rischi vengono valutati secondo due «direttrici»:

- ***Impatto*** ("impact"), ovvero il danno economico potenziale (perdita o mancato guadagno) patito al seguito del verificarsi dell'evento negativo (ad esempio sui ricavi, sul risultato operativo, ecc.)
- ***Probabilità*** ("likelihood"), ossia la frequenza del possibile realizzazione dell'evento in grado di influire negativamente sul raggiungimento degli obiettivi. Rappresenta una grandezza per definizione non conosciuta e quindi determinabile per proiezione delle esperienze passate o in base alla presenza di elementi che possono influenzarla.

Rischio = impatto * probabilità

Figura 14: *matrice di rischio* (Materiale didattico AIIA, Il Sistema di Controllo Interno e di Gestione dei Rischi, *Diploma in Controllo e Internal Auditing*, 2017)



Le *tecniche quantitative* invece, fondate su modelli matematici, sono più precise ed oggettive, e la loro validità dipende dall'affidabilità dei dati e dalle assunzioni di base. Esse sono solitamente utilizzate quando è necessario differenziare in modo più specifico le aree oggetto di audit, ovvero quelle in cui l'IA deve intervenire. Una di queste tecniche è il *risk scoring*.

Per pervenire al calcolo di un "risk score" che determini delle priorità di intervento è necessario passare attraverso le seguenti fasi:

1. ***Selezione dei fattori di rischio***: essi possono essere classificati come *fattori dimensionali* (esempio: valore monetario del processo), *di controllo* (esempio: complessità delle operazioni, sviluppo dei sistemi informativi, modifiche nel personale e nella struttura organizzativa, ambiente di controllo) o *di audit* (esempio: tempo trascorso dall'ultimo audit, risultati dei precedenti audit).
2. ***Valorizzazione dei fattori di rischio***: viene conferito un valore numerico (ad esempio da 1 a 5, dove 1 indica un fattore di rischio poco rilevante, mentre 5 molto rilevante, Tabella 1).

Tabella 1: *valorizzazione dei fattori di rischio* (Materiale didattico AIIA, Il Sistema di Controllo Interno e di Gestione dei Rischi, *Diploma in Controllo e Internal Auditing*, 2017*)*

FATTORI	***VALORE***	
	1	***5***
Valore monetario del processo	< 1 M €	> 20 M €
Complessità delle operazioni	Limitata	Estrema
Sviluppo dei sistemi informativi	Attività automatizzate	Attività manuali
Modifiche nel personale o struttura organizzativa	Turnover scarso	Turnover elevato
Ambiente di controllo	Cultura di controllo diffusa	Cultura di controllo scarsa
Tempo trascorso dall'ultimo audit	Meno di 1 anno	Più di 3 anni
Risultati ultimo audit	Nessun rilievo	Più di 3 criticità rilevate

3. ***Assegnazione del peso indicante la rilevanza dei fattori di rischio***: tali fattori di rischio potrebbero non assumere eguale rilevanza nella valutazione delle diverse aree di audit, perciò ad ognuno di essi viene attribuito un peso diverso, assegnando un valore più alto al fattore più significativo. Nell'esempio sopra riportato si considerano sette fattori, quindi i valori indicanti la rispettiva rilevanza saranno compresi tra 1 e 7.
4. ***Calcolo del "risk score"***: il "risk score" di ogni fattori di rischio è uguale al risultato della moltiplicazione tra valore e rilevanza (peso) assegnata (Tabella 2).

Tabella 2: *calcolo del "risk score"* (Materiale didattico AIIA, Il Sistema di Controllo Interno e di Gestione dei Rischi, *Diploma in Controllo e Internal Auditing*, 2017)

		PROCESSO XYZ		
		Valore fattore	Peso	Risk Score
1	Valore monetario processo	5	2	10
2	Complessità delle operazioni	3	5	15
3	Sviluppo dei sistemi informativi	3	7	21
4	Modifiche nel personale e struttura organizzativa	2	3	6
5	Ambiente di controllo	4	1	4
6	Tempo trascorso dall'ultimo Audit	2	6	12
7	Risultati dei precedenti Audit	3	4	12
	RISK SCORE			80

Il "risk score" ottenuto fornisce una misura del rischio relativo all'oggetto di audit preso in esame, ma non permette il confronto con altri oggetti. È necessario perciò "normalizzare" i valori dei fattori di rischio (**REF: Risk Evaluator Factor**). Tale operazione si ottiene esprimendo il "risk score" in funzione del suo valore massimo (nell'esempio corrisponde a 140).

REF = 80/max = 80/140 = 0,571

È possibile così classificare i progetti di audit in ordine decrescente in base ai Fattori di Valutazione del Rischio (REF), in modo tale da organizzare di conseguenza i relativi interventi.

È importante che, una volta terminato il processo di valutazione del rischio, i risultati siano registrati dall'azienda ed archiviati in modo da renderli accessibili per le fasi successive di Risk Management e per ulteriori future valutazioni.

2.3 IL RISCHIO REPUTAZIONALE

"*Per costruire una reputazione servono anni, per distruggerla basta poco…*".

Questa frase di vecchia data esprime la natura precaria della reputazione ed il suo essere, per definizione, continuamente a rischio.

In termini generali, la reputazione può essere definita come il risultato dell'interazione tra:

1. le *aspettative* degli stakeholder sui comportamenti dell'azienda,
2. le *azioni* compiute dall'azienda che incidono in termini più o meno forti secondo l'impatto che hanno sulle percezioni degli stakeholder e la deviazione delle loro aspettative,
3. la *reazione* del sistema degli stakeholder di cui l'azienda è parte.

Essendo un elemento raro, difficile (o costoso) da imitare e che può generare valore destinato ad aumentare nel tempo, rappresenta un core asset di massima importanza dell'azienda e permette di ottenere un vantaggio competitivo sostenibile rispetto ai concorrenti.

Le difficoltà insite nella misurazione delle aspettative e delle percezioni, rendono necessaria l'adozione di un modello di riferimento che consenta di tradurre in termini operativi il concetto di reputazione e del relativo rischio. L'approccio più consolidato in letteratura è quello che prevede la definizione dei c.d. "*reputational driver*", ovvero i fattori che

concorrono a determinare la reputazione di una specifica organizzazione, quali ad esempio performance finanziarie in linea con le aspettative o con gli obiettivi aziendali, la capacità di gestire le relazioni con i vari stakeholder, una corporate governance adeguata alla complessità o alla struttura organizzativa dell'impresa, la conformità al Codice Etico dell'azienda, una corretta gestione dei conflitti di interesse, un'adeguata trasparenza verso i clienti, un livello elevato di attenzione verso gli interessi dei consumatori e un adeguato sistema di coordinamento interno. La somma di questi fattori esprime la capacità dell'impresa di creare valore non solo per gli azionisti ma, più in generale, per la comunità degli stakeholder (Twister, 2014).

Nell'era della comunicazione digitale la reputazione sembra essere in pericolo. In realtà, secondo Gianluca Comin, fondatore della società di comunicazione e relazioni pubbliche Comin & Partners e docente di Comunicazione strategica e Marketing alla Luiss, "la diffusione della comunicazione digitale non ha generato un incremento del rischio in materia di reputazione. Il fatto è che i nuovi strumenti e le nuove forme della comunicazione rendono visibili eventi minori che una volta sarebbero passati inosservati. La tecnologia ha aumentato le possibilità di entrare nella vita delle imprese, rendendola più trasparente. Il caso sollevato da un singolo cliente può diventare immediatamente rilevante grazie alla capacità della rete di funzionare come cassa di risonanza, generando un incontrollabile effetto a valanga".

In Italia la sensibilità nei confronti del rischio reputazionale è crescente, anche se non ancora del tutto soddisfacente. Infatti, la maggior parte delle imprese, soprattutto le più grandi, è dotata di piani per gestire la comunicazione nei casi di crisi: strumenti predefiniti e statici per affrontare a posteriori le crisi più probabili. Ma la reputazione non si può trattare a posteriori. Sarebbe opportuna una manutenzione preventiva curata da persone esperte che affianchino il Management e indaghino con loro sulle origini di una potenziale crisi, valutando gli interventi possibili per costruire e difendere progressivamente la reputazione aziendale.

"La parola d'ordine è collaborazione", continua Comin, "tra i comunicatori, o i Responsabili delle Relazioni Esterne, e chi, nelle aziende, si occupa funzionalmente dei rischi e della loro gestione, come ad esempio Risk Manager ed Internal Auditor. Essa consentirebbe certamente di migliorare la qualità dei piani per l'attenuazione dei rischi e la preparazione".

Come per altri tipi di rischio, la gestione del rischio reputazionale può essere sintetizzato in cinque fasi fondamentali:

I. l'impegno del Board e la definizione delle pratiche di gestione;

II. l'identificazione dei rischi rilevanti;
III. la valutazione dei rischi;
IV. l'applicazione di un piano d'azione;
V. le attività di monitoring e reporting.

Il fine principale di tale gestione è la capacità di riconoscere e gestire tutte le situazioni che possono impedire o rallentare l'impresa o una sua unità nel raggiungimento degli obiettivi. L'intero processo, se correttamente eseguito, può fornire al Management informazioni affidabili, la garanzia che i rischi siano correttamente identificati e tenuti sotto controllo e l'ottimizzazione di tutte le attività mirate alla riduzione delle possibilità di insuccesso. La realizzazione di tale processo mette il Board nella condizione di informare al meglio gli stakeholder, aumentando la loro sicurezza e la fiducia nell'impresa e accrescendo, in ultima analisi, la reputazione (Twister, 2014).

Gli organi esecutivi possono inoltre mettere in atto *procedure* e *policies* di supporto per indirizzare al meglio i comportamenti di dipendenti e partner. È importante anche la scelta del linguaggio attraverso il quale comunicare il sistema di gestione del rischio: utilizzare un linguaggio unico e condiviso aiuta nell'esecuzione delle diverse fasi ed aiuta soprattutto a legare il Risk Management agli obiettivi aziendali, chiarendone i benefici e quindi coinvolgendo il Management.

Infine, continue attività di audit sul rischio reputazionale consentono alle imprese di tenere costantemente sotto controllo lo stato della propria reputazione attraverso strumenti che permettono di adottare tempestivamente le contromisure opportune per ridurre tale rischio.

3. ASPIAG SERVICE: UN NUOVO PASSO VERSO L'EFFICIENZA ORGANIZZATIVA

3.1 IL GRUPPO ASPIAG

Ad oggi Aspiag Service si presenta come una realtà sempre più affermata nel settore della Grande Distribuzione Organizzata (GDO), rilevando risultati, in termini di fatturato e di quota di mercato, continuamente in crescita.

L'azienda, concessionaria del marchio Despar per il Nordest italiano, fa parte del Gruppo internazionale SPAR Austria e aderisce al Consorzio Despar Italia che riunisce tutte le concessionarie del marchio sul territorio nazionale. Fondata da Aspiag Management AG (società del gruppo Spar Austria) nel 1991, lavora attraverso i suoi tre centri distributivi (Ce.di.) di *Bolzano* (sede legale), *Udine* e *Mestrino* (centro direttivo, gestionale ed amministrativo), a cui fanno capo tutti i punti vendita, sia diretti (228) che affiliati (362). L'area di competenza comprende le regioni Veneto, Friuli-Venezia Giulia, Trentino-Alto Adige e le province di Bologna, Ferrara, Parma, Reggio Emilia, Modena, Ravenna e Mantova. Nel 2017 il fatturato aggregato di Aspiag Service ha avuto un incremento del 4,5% rispetto al 2016 (Tabella 3), corrispondente a circa il 15% dell'intero Gruppo Spar Austria, seconda solo alla Casa Madre.

Tabella 3: *dati fatturato aggregato* (Dati 2017 comunicati durante la conferenza stampa del giorno 22 febbraio 2018 a Salisburgo)

FATTURATO AGGREGATO ASPIAG (in miliardi di Euro)		
2016	*2017*	*Δ %*
2,07	2,16	+ 4,5

A livello internazionale il marchio è gestito da SPAR International, società cooperativa fondata nel 1932 nei Paesi Bassi come prima unione volontaria di grossisti e commercianti al dettaglio. "Spar" è una parola olandese che significa "abete" e che ha determinato la scelta del simbolo che caratterizza il marchio sin dalla fondazione (Figura 15). Il nome originario del gruppo DESPAR è acronimo di "Door Eendrachtig Samenwerken Profiteren Allen Regelmatig" che significa "Dalla cooperazione armoniosa tutti traggono vantaggio in ugual

modo". Negli anni '50 il marchio viene abbreviato in SPAR e si diffonde dapprima in Europa e poi nel resto del mondo. Il suo arrivo in Italia viene seguito dalla nascita, nel 1960, dell'Unione Volontaria SPAR, che sceglie di adottare il vecchio nome del marchio, divenendo Despar (Report Integrato 2016).

Figura 15: *il marchio SPAR* (fonte: http://spar-international.com/)

Aspiag, come già sopra indicato, opera nel settore della GDO, vendendo all'ingrosso e al dettaglio prodotti alimentari e non, potendo contare, per tale scopo, su un ampio e consolidato sistema, composto da punti vendita e centri commerciali, volto alla produzione, alla gestione e alla promozione di prodotti, nonché alla loro vendita. La rete di vendita è strutturata in tre insegne: Despar, Eurospar e Interspar.

L'insegna *Despar* identifica i supermercati di quartiere dalle dimensioni contenute (100-800 mq), con un assortimento di prodotti specifico per la spesa giornaliera. Le dimensioni ridotte e un ambiente familiare favoriscono la relazione con il cliente.

L'insegna *Eurospar* individua i punti vendita di media grandezza (801-2499 mq) in grado di servire un'area urbana più vasta e con necessità di consumo differenziate. Rappresenta il punto di riferimento ideale per una spesa settimanale.

L'insegna *Interspar* identifica i supermercati di grande metratura, concepiti per offrire il migliore assortimento a tutti i bisogni del cliente della cintura metropolitana.

Per quanto riguarda l'assortimento, accanto ai prodotti nazionali e internazionali, Despar propone un'ampia gamma di *private labels* (prodotti a marchio), che presidia tutte le categorie merceologiche con oltre 1.500 prodotti.

L'obiettivo è diventare leader del settore e per realizzarlo Aspiag si focalizza su una serie di valori, individuati attraverso il coinvolgimento del Management e diffusi a tutti i collaboratori. Tali valori sono espressione di un pensiero integrato e costituiscono la guida dell'agire quotidiano dell'azienda. Essi sono (*Report Integrato 2016*):

- *Attenzione al cliente*, cercando di comprendere bisogni e necessità ed essere così in grado di offrire un servizio di qualità che crei valore.
- *Innovazione*, raccogliendo e condividendo informazioni chiave, considerando la complessità e la variabilità del contesto operativo, al fine di individuare soluzioni evolutive a sostegno del vantaggio competitivo.
- *Sviluppo delle persone*, ottenibile ispirando comportamenti tesi ad un continuo apprendimento con l'obiettivo di facilitare la responsabilità e l'autonomia lavorativa, di motivare al raggiungimento degli obiettivi e di creare un forte senso di appartenenza.
- *Sostenibilità,* creando un rapporto equilibrato e duraturo di tutte le attività considerando i loro effetti economici, sociali ed ambientali.

Uno dei pilastri dell'atteggiamento generale e della strategia di Aspiag Service per la costruzione di solide fondamenta è la valorizzazione dei 7.450 dipendenti, che rappresentano il vero vantaggio competitivo e l'alto livello qualitativo dell'azienda stessa, grazie ad un'efficiente *attività di recruiting* gestita dall'HR. Inoltre, vincendo nel 2017 il premio "*Best Talent Hunter*" dell'Università degli Studi di Padova, ha dimostrato di incoraggiare e coltivare il talento dei giovani.

3.2 IL MODELLO DI GOVERNANCE

Il sistema di Corporate Governance di Aspiag è fondato su alcuni principi cardine, quali una corretta e trasparente scelta di gestione dell'attività d'impresa assicurata anche attraverso l'individuazione di flussi informativi tra gli organi sociali e un'efficiente definizione del sistema di controllo interno e di gestione dei rischi.

Figura 16: *modello di Governance di Aspiag Service* (Report Integrato 2016)

Il modello di governance (Figura 16) prevede una struttura gerarchica che coinvolge diversi attori, al cui vertice è posta *l'Assemblea dei Soci*, presieduta dal presidente del Consiglio di Amministrazione (CdA) o da un'altra persona designata dall'Assemblea stessa a maggioranza semplice, alla quale sono riservate le competenze previste dalle normative civilistiche e dallo statuto. I poteri inerenti all'ordinaria e straordinaria amministrazione della Società spettano al *CdA*, composto da otto membri, di cui cinque esecutivi incluso il Presidente. La scelta di nominare diversi Amministratori Delegati non ha reso la struttura aziendale ulteriormente onerosa, poiché ad essi non spetta alcun compenso per la carica ricoperta. La suddivisione dei compiti, inoltre, assicura una direzione maggiormente coinvolta nelle dinamiche riconducibili alle varie aree aziendali. Al CdA spetta, tra l'altro, il compito di approvare e supervisionare la pianificazione economica e finanziaria della Società.

Ad esso vengono affiancati il *Collegio Sindacale* e la *Società di Revisione*, ai quali è attribuito il ruolo, nelle loro rispettive differenze e competenze, di vigilare sull'operato aziendale e sulla sua struttura e sono entrambi nominati dai Soci. Il Collegio Sindacale, composto da cinque membri, vigila sull'osservanza della legge e dello Statuto Sociale e sui corretti metodi di amministrazione, con particolare attenzione all'assetto organizzativo, amministrativo e contabile, oltre a possedere funzioni di controllo di gestione. Per quanto riguarda il controllo contabile, invece, Aspiag Service ha conferito l'incarico alla Società di Revisione contabile esterna Ernst & Young S.p.A., con mandato di tre esercizi a scadenza dell'assemblea per il Bilancio 2018.

Attraverso il CdA vengono poi istituiti degli organi volti all'amministrazione aziendale, al supporto operativo, e alla vigilanza, quali il *Comitato di Gestione*, i *Procuratori* e l'*Organismo di Vigilanza* (Compliance Office). Il Comitato di Gestione è composto da un numero variabile di membri, di cui fanno parte di diritto il presidente del CdA e tutti gli Amministratori Delegati. Esso ha compiti propositivi, preparatori e di supporto tecnico e gestionale, come ad esempio la predisposizione della proposta di budget e la formulazione del business plan triennale. Un'altra figura che viene in sostegno alle attività del CdA e proprio nominata da quest'ultimo è quella del Procuratore, a cui sono conferiti i poteri di amministrazione ordinaria e straordinaria, nell'ambito delle attività dagli stessi gestite e nel rispetto delle deleghe loro conferite.

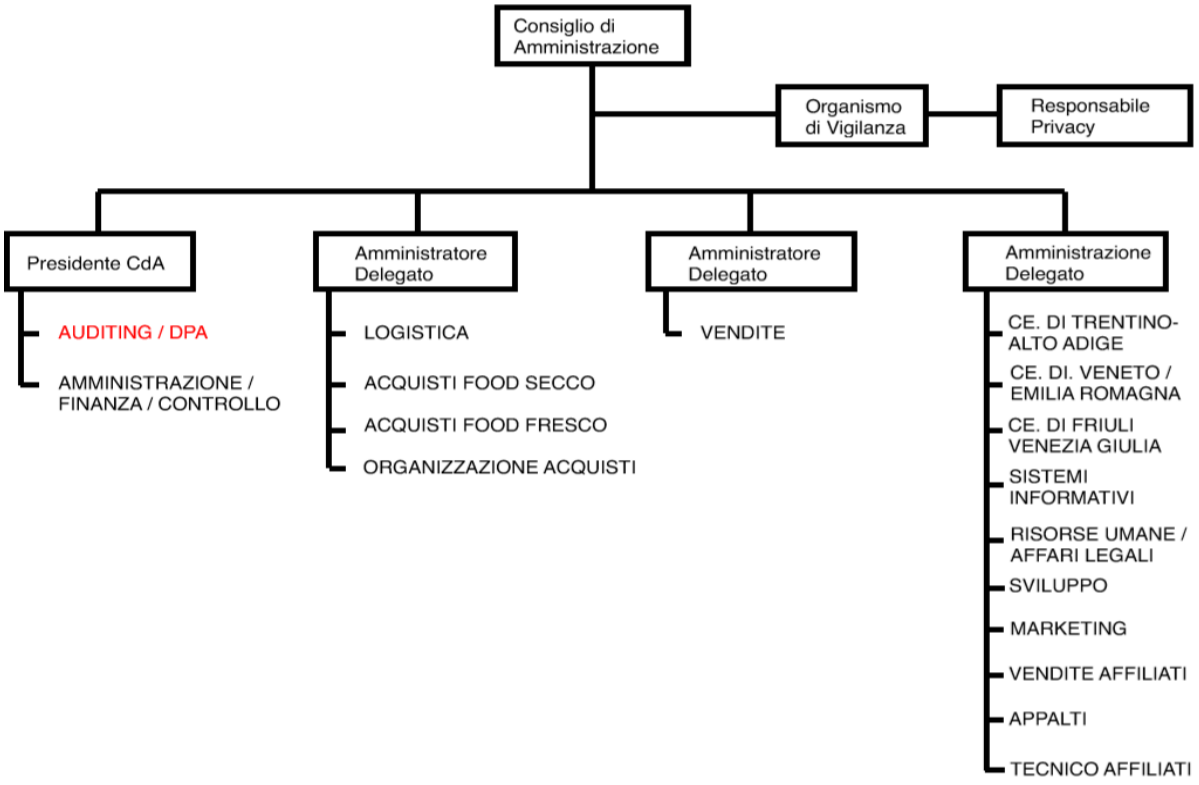
Infine, il ruolo di Organismo di Vigilanza è svolto dal Compliance Office, ai sensi ed ai fini del D.Lgs. 231/01, che disciplina le responsabilità aziendali per gli illeciti amministrativi dipendenti da reati, posti in essere nell'interesse o a vantaggio dell'ente. Tale organo,

attualmente composto da due membri, di cui uno esterno, ha l'obbligo di riferire periodicamente le eventuali criticità nel sistema aziendale in merito all'attuazione del Modello Organizzativo e di predisporre all'inizio di ogni anno il piano delle verifiche e dei controlli da eseguire durante l'anno, rendicontando i risultati al CdA e al Collegio Sindacale (Report Integrato 2016).

3.3 L'ATTIVITÀ DI INTERNAL AUDITING IN ASPIAG

Il dato di fatto di un'azienda che iniziava ad avere delle dimensioni importanti ed un'organizzazione complessa, l'esperienza positiva della funzione IA nella Capogruppo austriaca e in altre realtà da questa controllate, la volontà di non ragionare solamente in un'ottica di redditività ma anche in un'ottica di valutazione dei rischi, la diffusione ai propri collaboratori della cultura del controllo e la necessità di preservare l'azienda da distrazioni di risorse. Questi sono i fattori che hanno spinto il Board di Aspiag Service ad istituire, nel marzo 2015, la Direzione Auditing e DPA (Difesa del Patrimonio Aziendale), dipendente direttamente dal Presidente del CdA (Figura 17), in modo da garantire una corretta indipendenza ed avvalorare il *commitment* delle attività svolte, anche se, ad oggi, non esiste un mandato di Audit formalizzato secondo quanto stabilito dagli IPPF.

Figura 17: *organigramma aziendale di Aspiag Service* (Report Integrato 2016)



I principali interlocutori della funzione sono il Board, destinatario dei Rapporti di Audit, il Collegio Sindacale ed il Compliance Office. Più complicata invece, almeno in fase di kick off, la relazione con le altre funzioni aziendali ed in particolare con Management e Senior Management. Dopo un primo avvio positivo e di curiosità generato dalla non conoscenza della funzione, si è passati ad una fase "negativa" determinata dalle constatazioni di difformità rispetto alle regole e procedure che venivano rilevate dalla funzione e che quindi generavano una sorta di rifiuto.

Ad oggi la funzione, dopo un'accurata attività di *marketing interno*, necessaria al fine di far comprendere l'obiettivo dell'IA, inteso come supporto al business, evidenziando l'importanza del rispetto di regole e procedure e il valore aggiunto generato, viene sempre interpellata e ha acquisito un ruolo di rilievo all'interno dell'organizzazione. Essa, nei tre anni di esistenza, ha intrapreso un percorso evolutivo, accrescendo le competenze interne ed ampliando le aree di business sulle quali interviene, passando dal solo ambito di procurement di merci e servizi a quelli di governance (ad esempio rispetto D.Lgs. 231, segregazione delle informazioni, poteri di firma, ecc.), e gestione ed amministrazione del personale (HR).

Generalmente, in Aspiag la funzione si occupa di:

- A*ttività di "Security"*, con risorse dedicate alla salvaguardia del patrimonio aziendale che si occupano di gestione dei fornitori di servizi di sicurezza (portierato) all'interno delle filiali, formando a dovere gli addetti inviati, e di trasporto valori, impegnati nel trasferimento del denaro dal punto vendita alla Sala Conta (luogo dove viene contato, individuando in caso le banconote false, e custodito nel caveau). Le risorse svolgono inoltre attività di audit proprio sulle Società che offrono tali servizi, ad esempio monitorando costantemente la loro regolarità contributiva (attraverso la consultazione del DURC, Documento Unico di Regolarità Contributiva).
- A*ttività di "Fraud Detection"*, svolta da una risorsa all'interno della funzione, con l'obiettivo di evitare qualsiasi tipo di frode legata al Cash Management dovuta all'elevato volume di denaro gestito, analizzando tutti i dati dei punti vendita, i movimenti di cassa ed i relativi processi. Dall'inizio di tale attività sono state riscontrate le seguenti frodi:
  - Utilizzo fraudolento di carte di credito ed altri mezzi di pagamento elettronici e non;
  - furto di denaro (differenze di cassa);
  - furto di merce (differenza inventariale);
  - procedure di movimentazione del denaro non rispettate.

Per rendere più efficace tale attività, Aspiag sta valutando la possibilità di dotarsi di misure quali i sistemi di "whistleblowing", finalizzati a raccogliere in modo anonimo denunce di frodi, e la formazione specifica su come prevenirle.

- *Attività di "Full Audit Stores"*, al fine di assicurare il corretto funzionamento del sistema di controllo interno sui singoli punti vendita. Essendo solamente due le risorse che si occupano di tale attività, non è possibile coprire tutta la rete di vendita in un solo anno, perciò nel Piano di Audit annuale vengono inseriti un numero limitato di stores oggetto di controlli, selezionati in base al dato di differenza inventariale ed eventuali anomalie rilevate nella gestione del denaro. Il "Full Audit" viene effettuato attraverso una checklist che permette una valutazione uniforme delle condizioni generali del negozio (ad esempio come si presenta al pubblico in termini di pulizia), della sicurezza ambientale (ad esempio la gestione dei rifiuti), della sicurezza alimentare di ogni reparto, della sicurezza delle persone (sia dipendenti che clienti), della sicurezza dei beni e dell'amministrazione e movimentazione del denaro. Ad ogni sezione viene conferito un giudizio (eccellente, buono, insufficiente o molto insufficiente) e vengono elencati gli interventi consigliati in risposta alle criticità rilevate. Sulla base della checklist viene poi redatta una Relazione di Audit destinata ai Capi Area, ovvero i diretti responsabili di una determinata area di punti vendita, ed un Management Summary, contenente solamente le criticità e destinato al presidente del CdA ed all'Amministratore Delegato responsabile dell'area Vendite. Per gli stores con un punteggio medio insufficiente vengono panificati e svolti Audit di follow-up per verificare l'avvenuta implementazione dei piani d'azione.
- *Attività di "Management Audit"*, svolta principalmente dal RIA, il quale verifica l'idoneità ed il rispetto sia delle procedure interne che delle disposizioni di legge, vigila sul rispetto del codice interno di comportamento e controlla che gli obiettivi di ogni funzione siano coerenti con quelli aziendali. Egli si attiene agli Standard per la pratica professionale dell'IA nell'esecuzione dell'intero processo di Auditing, dal Piano di Audit, predisposto alla fine di ogni anno per quello successivo ed approvato dal Board Aziendale, il quale, se necessario, può apportarvi modifiche, al Follow-up finale. I principali strumenti di raccolta di informazioni utilizzati sono *questionari*, specialmente nella fase di kick off, per un Risk Assessment svolto in collaborazione con la Capogruppo, *sistemi di campionamento* su ampie popolazioni di dati e *procedimenti analitici* su campi più ristretti. Una delle fasi più importanti è la comunicazione dei risultati e la proposta dei piani d'azione, che avviene attraverso un Report di Audit illustrato tramite *workshop* al Board e, a seconda del tema, a Senior Management o Management. Esempi di piani

d'azione implementati sono l'introduzione di doppie firme, doppie autorizzazioni, doppi controlli a "quattro occhi", la suddivisione della funzione che registra da quella che paga le fatture ai fornitori, la definizione di uno standard contrattuale per i fornitori, la creazione di standard nelle modalità e condizioni di pagamento e la revisione del sistema di deleghe e procedure.

- *Attività di "Risk Management"*, svolta sempre dal RIA, il quale, infatti, oltre al terzo (Internal Audit), si occupa anche del secondo livello (Risk Management) del SCI, non esistendo un'apposita funzione all'interno dell'azienda, dando elevata importanza soprattutto alla valutazione del rischio, necessaria per definire le priorità del Piano di Audit. I principali rischi che minacciano l'azienda sono i seguenti:
  - Sottrazione di risorse interne (economiche ed opportunità) attraverso il mancato rispetto delle procedure e delle regole interne (fornitori, clienti e dipendenti);
  - Rischi di sanzioni e sottrazioni di risorse interne per il mancato rispetto dei principi di governance e del D.Lgs. 231/01;
  - Cyberrisk (frodi informatiche, furto di dati);
  - Frodi sulla gestione del denaro dovute all'elevato volume di denaro contante gestito;
  - Furti di merce (differenze inventariali) dovuti all'elevato volume di merci movimentate;
  - Danni economici e di immagine derivanti dal mancato rispetto delle normative.

L'obiettivo è quello di abbracciare tutte le tipologie di Audit con riferimento all'affidabilità ed integrità delle informazioni, all'efficacia ed efficienza delle attività operative ed alla conformità con policies, procedure, leggi, regolamenti e contratti.

Secondo il RIA di Aspiag Daniele Pitassi, lo sviluppo della funzione non si ferma qui: "l'IA deve adeguarsi alla crescita dell'azienda. Sarebbe opportuno rinforzare la funzione in termini di risorse, in modo tale da sviluppare piani di azione e di audit più ampi, e dare la possibilità a queste di ottenere la formazione e le certificazioni (ad esempio CIA) necessarie a conseguire determinate conoscenze e competenze. Tematiche come il rispetto della nuova *normativa sulla Privacy* relativa al trattamento dei dati personali delle persone fisiche (Regolamento Ue 27 aprile 2016 n. 2016/679/UE) in vigore dal 25 maggio 2018 o tematiche IT come il *cybercrime* sono in evidente crescita e dovrebbero essere trattate in maniera più attiva".

"Essendo una funzione giovane", continua Pitassi, "ad oggi l'IA di Aspiag non è mai stata valutata esternamente, ma solo internamente, e non formalmente, dalla funzione di Internal Auditing della Capogruppo. Una valutazione effettuata da un organo o consulente esterno non

solo è necessaria almeno ogni cinque anni, come indicato negli IPPF, ma può essere utile per l'azienda come strumento di verifica della conformità del RIA ai "*Core Principles*" (integrità, obiettività, riservatezza e competenza) definiti dalla normativa".

CONCLUSIONI

L'esperienza svolta nella Direzione Auditing e DPA di Aspiag Service ha determinato uno stimolo per approfondire i contenuti e la natura dell'attività di Internal Audit, il cui compito, come abbiamo visto nel corso della trattazione, è quello di valutare e contribuire a migliorare i processi di gestione del rischio, di controllo interno e di corporate governance dell'organizzazione, attraverso un approccio professionale sistematico che crea valore aggiunto.

La continua evoluzione dell'ambiente di riferimento ha portato inevitabilmente la necessità di un rafforzamento interno della struttura aziendale e quindi l'esigenza di dotarsi di una figura che si occupi dei controlli, a tutti i livelli. L'Italia, sotto tale aspetto, si è rivelata leggermente in ritardo rispetto ai paesi più industrializzati, dove la funzione è presente da decenni. La causa? La difficoltà a comprendere i vantaggi che può dare una funzione all'interno dell'azienda che valuta le scelte strategiche e l'organizzazione secondo l'ottica del rischio, dando quindi l'informativa al Board anche in termini economici dei rischi che certe decisioni comportano.

La regolamentazione della disciplina (attraverso gli IPPF) è stata certamente essenziale per la definizione del ruolo del RIA, e della funzione in generale, all'interno dell'azienda. Ciò che ancora manca però non sono solo risorse sufficienti e ben formate per lo svolgimento dell'incarico, ma un vero e proprio "salto culturale": l'IA deve rafforzare la propria immagine e la percezione del proprio ruolo e del valore che è in grado di generare. Sebbene siano già stati fatti passi in avanti dal punto di vista organizzativo e di governance, garantendo linee di riporto verso i più alti vertici societari, la sfida di elevare lo "*status*" della funzione passa anche e soprattutto dalla capacità degli stessi RIA di farsi percepire come partner strategici.

Nel futuro prossimo, se le aziende non saranno in grado di sviluppare sistemi informativi pienamente integrati o soluzioni tecnologiche innovative, non riusciranno a cogliere vantaggi rilevanti ed effettivamente misurabili. Non fanno eccezione le modalità con cui le attività di internal audit sono condotte. L'analisi dei processi deve continuare, naturalmente, ma dovrà avere una dimensione tecnologica, perché i rischi connessi alla violazione di un processo possono essere più ampi che in passato. Infatti, una delle caratteristiche essenziali che l'Internal auditor del futuro dovrà possedere sarà appunto la capacità di anticipazione.

La scommessa della Direzione Auditing e DPA si traduce nel percorrere linee evolutive all'avanguardia, conformemente alle dinamiche della struttura organizzativa dell'azienda, alle politiche del Board e alla diffusione della "cultura del controllo", che garantiscono una gestione dei rischi di business, nonché dei processi di valutazione, in grado di fornire una visione integrata della governance aziendale. In virtù della sua recente costituzione (marzo 2015) la funzione si pone l'obiettivo di offrire una consulenza "giovane" che possa dare impulso a nuovi progetti per sfruttare appieno i cambiamenti del contesto ambientale di riferimento e per confermare il favorevole trend di crescita di Aspiag.

[1]

[1] Numero di parole dell'elaborato: 16257

RIFERIMENTI BIBLIOGRAFICI

AMATO, A., 2017. Governance e Risk Management: il Ruolo dell'IA. *Diploma in Controllo e Internal Auditing. Governance Aziendale, Gestione del Rischio e SCI*, Milano. Editore: AIIA – Associazione Italiana Internal Auditors.

AMATO, A., 2017. Il Sistema di Controllo Interno e di Gestione dei Rischi. *Diploma in Controllo e Internal Auditing. Governance Aziendale, Gestione del Rischio e SCI*, Milano. Editore: AIIA – Associazione Italiana Internal Auditors.

AMATO, A., 2017. International Professional Practices Framework (IPPF). *Diploma in Controllo e Internal Auditing. Governance Aziendale, Gestione del Rischio e SCI*, Milano. Editore: AIIA – Associazione Italiana Internal Auditors.

ANON., s.d.. *Definizione di Internal Auditing* [online]. IPPF, AIIA – Associazione Italiana Internal Auditors. Disponibile su: <http://www.aiiaweb.it/definizione-di-internal-auditing>.

ANON., s.d.. *International Professional Practices Framework (IPPF)* [online]. AIIA – Associazione Italiana Internal Auditors. Disponibile su: <http://www.aiiaweb.it/international-professional-practices-framework-new-ippf>.

ANRA – Associazione Nazionale dei Risk Manager e Responsabili Assicurazioni Aziendali, e STRATEGICA GROUP, 2011. Gli standard di Risk Management e l'ISO 31000. *Position Paper*, Milano.

AONDIO, K., BARBIERI, P., CASSINARI, B., CHIESA, F., GUTIERREZ, S., MARSECANE, S., e MICOCCI, A., 2014. Internal Auditing: dove siamo. *Comunicazione e Marketing della funzione di Internal Audit*, 6-8, Milano. Editore: AIIA – Associazione Italiana Internal Auditors.

ARCHABEAULT, M., e ROSE, M., 2010. *The ABCs of Communicating Results*, Dayton. Editore: The IIA – Institute of Internal Auditors.

CASANA, G., 2005. *Accettabilità del rischio e raggiungimento degli obiettivi*, Milano. Editore: AIIA – Associazione Italiana Internal Auditors.

CATANI, D., 2017. L'evoluzione necessaria. Standard Professonali. *PMI alla prova dei controlli*, 21-24, Milano. Editore: AIIA – Associazione Italiana Internal Auditors.

CIANFARANI, E., 2017. Guardare più avanti. *Survey: le priorità dei CAE europei*, 36-39, Milano. Editore: AIIA – Associazione Italiana Internal Auditors.

COMMITEE OF SPONSORING ORGANISATIONS OF THE TRADEWAY COMMISSION (COSO), 2004. Executive Summary. *Enterprise Risk Management — Integrated Framework*, Jersey City.

CREGUT, M., 2017. Principi di Corporate Governance. *La Corporate Governance in Italia e nel Mondo*, Milano. Editore: AIIA – Associazione Italiana Internal Auditors.

D'ONZA, G., 2016. E ora? Bisogna accelerare. *A che punto è la professione*, 5-9, Milano. Editore: AIIA – Associazione Italiana Internal Auditors.

FARGION, R. (Direttore Generale AIIA), 2014. Oltre la lettera del Mandato. *Governance, come evolve il ruolo della professione*, 1, Milano. Editore: AIIA – Associazione Italiana Internal Auditors.

FARGION, R. (Direttore Generale AIIA), 2014. Più sinergie per difendersi dal nuovo reputation risk. *Reputazione: come cambia il rischio*, 1, Milano. Editore: AIIA – Associazione Italiana Internal Auditors.

IIA – The Institute of Internal Auditors, 2013. IIA Position Paper: *The Three Lines of Defense in effective Risk Management and Control*, Altamonte Springs, Florida.

IIA - The Institute of Internal Auditors, 2016. Standard Professionali per la pratica professionale dell'Internal Auditing (Standard). *Standard and Guidance*, Altamonte Springs, Florida.

MANCINI, S., 2017. *La definizione del Piano di Audit ed il processo di Audit*, Milano. Editore: AIIA – Associazione Italiana Internal Auditors.

MARCANDALLI, E., 2005. *Il mandato dell'Internal Auditing*, Milano. Editore: AIIA – Associazione Italiana Internal Auditors.

PAGANINI, D., 2007. *L'indipendenza dell'internal audit*, Milano. Editore: AIIA – Associazione Italiana Internal Auditors.

POLITECNICO DI MILANO E CONFINDUSTRIA DIGITALE, 2017. Fattore ICT. *In*: TWISTER COMMUNICATIONS GROUP, a cura di, 2017. Esami di riparazione. *Digital Transformation, che cosa accadrà se adesso si accelera*, 5-7, Milano. Editore: AIIA – Associazione Italiana Internal Auditors.

RUSSO, R., e FRATICELLI, U. (Poste Italiane), 2007. *Si può misurare il valore dell'audit?*, Milano. Editore: AIIA – Associazione Italiana Internal Auditors.

TARALLI, E., 2015. L'importanza della seduzione. *Lo stato della professione: parlano i CAE*, 24-27, Milano. Editore: AIIA – Associazione Italiana Internal Auditors.

TRIVELLATO, R. (CFO di Aspiag Service), a cura di, 2017. *Report Integrato 2016*, Mestrino (PD). Disponibile su: <https://www.despar.it/it/report-integrato/>.

TWISTER COMMUNICATIONS GROUP, a cura di, 2017. Per camminare a testa alta. *Reputazione: come cambia il rischio*, 6-8, Milano. Editore: AIIA – Associazione Italiana Internal Auditors.

TWISTER COMMUNICATIONS GROUP, a cura di, 2017. Prevenzione intelligente. *Reputazione: come cambia il rischio*, 13-14, Milano. Editore: AIIA – Associazione Italiana Internal Auditors.

RIFERIMENTI NORMATIVI

Decreto legislativo 24 febbraio 1998 n. 58.

Decreto legislativo 08 giugno 2001, n. 231.

Regolamento Ue 27 aprile 2016, n. 2016/679/UE.