



**Dipartimento di Impresa e Management**

*Cattedra di*

*Corporate Governance and Internal Auditing*

**L'ATTIVITÀ DI INTERNAL AUDITING NELLA  
PREVENZIONE DELLE FRODI SOCIETARIE**

UN'ANALISI COMPARATA DELLE PRINCIPALI REALTÀ AZIENDALI ITALIANE

**RELATORE:**

Chiar.mo Prof. Simone Scettri

**CANDIDATO:**

Antonio Romano

Matr. 701601

**CORRELATORE:**

Chiar.mo Prof. Giovanni Fiori

A/A 2018/2019

# Sommario

<b>Premessa</b> .....	3
<b>Capitolo Primo. La Funzione Internal Audit nelle Organizzazioni</b> .....	6
1.1. Introduzione .....	6
1.2. Il Sistema di Controllo Interno e i tre livelli del controllo .....	7
1.2.1. Definizione di Sistema di Controllo Interno.....	7
1.2.2. La funzione .....	9
1.2.3. La struttura.....	10
1.2.4. I tre livelli del controllo.....	12
1.3. I modelli internazionali in tema di controllo interno: dal CoSO Report all'Enterprise Risk Management .....	14
1.3.1. Il CoSO Framework .....	14
1.3.2. L'Enterprise Risk Management o il CoSO ERM .....	19
1.3.3. Le principali differenze tra il CoSO Framework e l'ERM.....	24
1.3.4. ERM Integrating with strategy and performance: l'ultimo aggiornamento del modello .. ..	26
1.4. Il contesto autoregolamentare di riferimento in materia di Internal Audit..	27
1.4.1. Il Codice di autodisciplina delle società quotate .....	28
1.4.2. L'International Professional Practices Framework.....	31
1.5. La natura della Funzione Internal Audit.....	42
1.6. Il processo di audit .....	46
1.6.1. Pianificazione.....	48
1.6.2. Esecuzione dei test .....	52
1.6.3. Reporting .....	56
1.6.4. Follow-up.....	58
1.7. Un approfondimento sui principali Standard internazionali.....	59
1.8. Conclusioni .....	63
<b>Capitolo Secondo. L'Internal Audit e le relazioni con gli Organi di controllo</b> ..	65
2.1. Introduzione .....	65
2.2. I rapporti con il Consiglio di Amministrazione .....	66
2.3. I rapporti con il Comitato Controllo e Rischi .....	70
2.4. I rapporti con il Collegio Sindacale .....	74
2.5. I rapporti con l'Organismo di Vigilanza ex D.Lgs. 231/2001 .....	76

2.6.	I rapporti con il Dirigente preposto alla redazione dei documenti contabili societari.....	80
2.7.	I rapporti con la Società di Revisione .....	83
2.8.	Conclusioni .....	86
<b>Capitolo Terzo. Le frodi aziendali: caratteristiche e modalità .....</b>		<b>88</b>
3.1.	Introduzione .....	88
3.2.	Definizione di frode e caratteristiche principali.....	90
3.2.1.	Definizioni .....	90
3.2.2.	Caratteristiche generali dei white collar crime .....	91
3.2.3.	Le ragioni alla base del comportamento fraudolento .....	93
3.3.	Una rassegna delle principali forme di frodi aziendali .....	97
3.4.	Richiami normativi in materia di frodi.....	105
3.4.1.	Il Sarbanes-Oxley Act come risposta americana ai Corporate Scandals .....	105
3.4.2.	La legge sulla tutela del risparmio: la “SOX italiana” .....	108
3.4.3.	Il D.Lgs. 231/2001 .....	110
3.5.	L’attività di Fraud Auditing.....	114
3.6.	Conclusioni .....	118
<b>Capitolo Quarto. Il coinvolgimento dell’Internal Audit nella gestione interna degli illeciti aziendali: applicazioni pratiche .....</b>		<b>120</b>
4.1.	Analisi comparata delle principali società quotate .....	120
4.2.	Il ruolo del revisore interno in un caso italiano di frode .....	137
<b>Considerazioni finali .....</b>		<b>143</b>
<b>Bibliografia .....</b>		<b>145</b>
<b>Sitografia .....</b>		<b>148</b>

## Premessa

Il presente lavoro è volto ad analizzare la relazione intercorrente tra la corretta predisposizione e attuazione della Funzione di Internal Audit e la conseguente riduzione del rischio di frode, in termini di individuazione e prevenzione dell'illecito.

La ricerca parte dalla constatazione degli effetti che uno scandalo societario può provocare nei confronti dell'azienda all'interno della quale è compiuto l'illecito, nonché verso la grande platea di interlocutori sociali che hanno un interesse nei confronti dell'organizzazione. Non solo, l'impatto di una frode agisce altresì sulla reputazione di chi la compie e di ciò che ne ruota attorno, provocando forti cambiamenti in un particolare mercato o in un'area geografica. Ne è un esempio recente e di portata internazionale lo scandalo che ha coinvolto il leader del settore automobilistico Volkswagen (cd. *Dieseltgate*): il “disastro economico”, come cita il Sole 24 Ore<sup>1</sup>, conta un numero di circa 11 milioni di veicoli richiamati e un ammontare di spese che si aggira intorno ai 20 miliardi di euro. Inoltre, a partire dal 18 Settembre 2015 è crollata completamente la reputazione del motore diesel, con conseguenze che hanno riguardato anche gli altri *player* del mercato automobilistico. Infatti, l'evento appena citato ha agito da catalizzatore dell'elettrificazione dei motori, spostando il baricentro del mercato dell'automobile verso l'area asiatica.

Senza soffermarci ulteriormente sullo scandalo appena citato, va detto che le frodi aziendali rappresentano una minaccia per il mondo dell'economia-aziendale, a prescindere dalla portata dell'evento. Infatti, secondo alcune ricerche<sup>2</sup>, un'azienda su due dichiara di aver subito negli ultimi 24 mesi un reato di natura economico-finanziaria, con perdite che in un'azienda italiana su quattro sono state superiori al milione di dollari. Questi dati dimostrano l'importanza del fenomeno in termini di frequenza e impatto, e giustificano l'intensificarsi degli studi di corporate governance

---

<sup>1</sup> CIANFLONE M., *Dieseltgate, 3 anni fa lo tsunami che sconvolse l'auto*, Il Sole 24 Ore, 15 Settembre 2018, [www.ilsole24ore.com](http://www.ilsole24ore.com).

<sup>2</sup> PWC, *Global Economic Crime and Fraud Survey 2018: Pulling Fraud Out of The Shadows*, 2018.

che mirano a creare un sistema dei controlli aziendali più strutturato al fine di ridurre il rischio di accadimento.

Partendo dal presupposto che realtà ben strutturate già dispongono di adeguate procedure e processi aziendali atti a minimizzare il rischio di incorrere in perdite finanziarie e reputazionali derivanti dalla commissione di illeciti, e che nelle medesime società sia costituita una funzione che svolga attività di revisione interna su tali processi, lo scopo del seguente lavoro è quello di analizzare le modalità attraverso cui tale funzione agisce al fine di prevenire ed individuare una frode aziendale.

Il presente elaborato affronta questo tema secondo la seguente articolazione. Nel primo capitolo si cercherà di illustrare il concetto di Sistema di Controllo Interno, facendo particolare riferimento alla sua funzione all'interno dell'organizzazione e agli attori coinvolti e presenti nel suo disegno. Nel farlo, si ricorrerà ai modelli internazionali e al contesto autoregolamentare di riferimento, fonti autorevoli caratterizzate dall'essere definite come *principle-based* e in quanto tali applicabili ad ogni realtà societaria. Successivamente, verrà introdotta la natura della funzione di Internal Audit, quale attività indipendente il cui fine è quello di fornire un *assurance* sull'efficacia dei controlli aziendali già esistenti, e favorire un'implementazione di nuovi controlli per il miglioramento del sistema nel suo complesso. In questo caso, si farà esplicito riferimento agli Standard Internazionali che ne disciplinano la Professione e verranno descritte le attività di revisione e le modalità con cui esse vengono di norma svolte.

Il capitolo secondo, invece, si concentrerà sulle interazioni tra la funzione di Internal Audit e gli altri organi di governance, cercando di individuare gli elementi che accomunano le attività da questi svolte. In questo modo sarà possibile inquadrare l'operato del Sistema di Controllo Interno attraverso un'analisi dinamica dei rapporti che intercorrono tra le funzioni al suo interno, nonché comprendere in che modo è possibile sfruttare l'azione sinergica di questi al fine di ridurre il livello di rischio aziendale complessivo.

Più avanti, nel terzo capitolo sarà affrontato il tema delle frodi aziendali. La trattazione del fenomeno servirà a fornire una definizione di frode e il suo collocamento tra le diverse fattispecie di reato, un'analisi degli elementi essenziali che caratterizzano una

frode e le motivazioni di base che spingono i soggetti a commettere tale reato. In particolare, si parlerà della “simpatia” con cui viene accolta nell’immaginario collettivo, determinata dall’assenza di violenza presente in questa fattispecie di reato e dallo “scontro di intelligenze” che si genera tra chi commette la frode, attraverso raggiri e complessi artifici, e la vittima. Il capitolo proseguirà con l’illustrazione delle forme più comuni di frodi conosciute nel mondo delle aziende e con un breve cenno ai principali interventi del legislatore in materia. Inoltre, verranno descritte le attività poste in essere dall’Internal Audit al fine di prevenire, individuare e gestire i casi di frode aziendale.

Infine, allo scopo di arricchire l’illustrazione del fenomeno attraverso degli esempi pratici, sarà riportata un’analisi empirica che ha ad oggetto la funzione di Internal Audit presente in un panel di società quotate in Borsa. Tale ricerca è volta a comprendere l’effettiva applicazione degli Standard Professionali che regolano l’attività di revisione interna, ricorrendo all’osservazione della presenza o meno di alcuni driver scelti (attribuzioni, periodicità delle comunicazioni, svolgimento di attività di *fraud prevention and detection*, ecc.).

Per concludere, sarà illustrato un caso di frode aziendale nel quale verrà posta enfasi sulla struttura dell’Internal Audit presente in tale società e sulle modalità attraverso cui è stata gestita la dinamica fraudolenta dal revisore interno.

## Capitolo Primo

### **La Funzione Internal Audit nelle Organizzazioni**

#### **1.1. Introduzione**

Il tema del controllo di impresa rappresenta oggi una delle principali tematiche in materia di corporate governance, la quale ha attirato un sempre maggiore interesse, specialmente a seguito dei numerosi casi di *corporate scandals* che si sono susseguiti nei primi anni del nuovo secolo. Il mondo dei controlli aziendali è oggi composto da un'eterogeneità di attori, ognuno dei quali con una funzione specifica, talvolta sovrapponibili, talvolta ben distinta dagli altri, da cui si evidenzia l'esigenza di esercitare un monitoraggio costante sull'operato degli organi esecutivi al fine di indirizzare la gestione verso il perseguimento della creazione di valore.

Tuttavia, se si ritiene opportuno affermare che il fine di ogni impresa è quello di creare valore per sé e per tutti gli stakeholder aziendali, meno chiaro è il concetto del beneficio del controllo. Infatti, nell'instaurazione di nuovi sistemi di controllo, è necessario per la sopravvivenza dell'impresa che tali controlli siano in grado di apportare un valore maggiore rispetto al costo che l'impiego degli stessi comporta. In tal senso, la nascita di un Sistema di Controllo Interno deve trarre origine da una complessa analisi costi – benefici, ove in assenza della quale si palesa il rischio di sostenere dei costi superflui per un controllo inefficace e inefficiente.

Scopo del seguente capitolo è quello di introdurre gli elementi necessari per la comprensione del fenomeno dei controlli di impresa, per poi passare all'analisi più dettagliata e complessa della funzione di Internal Audit. In particolare, si ricorrerà spesso agli Standard Professionali per comprendere a pieno la natura e le modalità di svolgimento di tale attività, con l'obiettivo di rispondere al quesito se una funzione di controllo aziendale, quale è l'Internal Audit, è in grado di impattare sulla dinamica di creazione di impresa.

## **1.2. Il Sistema di Controllo Interno e i tre livelli del controllo**

### **1.2.1. Definizione di Sistema di Controllo Interno**

Nell'ambito della più ampia fattispecie del Sistema dei Controlli di Impresa, nella quale i principali attori sono il Consiglio di Amministrazione (e le sue articolazioni interne) e il Collegio Sindacale, il legislatore ha in più di un'occasione richiamato il concetto di Sistema di Controllo Interno. Infatti, esso viene indicato tra le competenze di vigilanza del Collegio Sindacale o del Consiglio di Sorveglianza, a seconda del modello adottato, e ne vengono altresì imputati una serie di obblighi informativi verso quest'ultimo<sup>3</sup>:

*“Il collegio sindacale vigila... sull'adeguatezza della struttura organizzativa della società per gli aspetti di competenza, del sistema di controllo interno e del sistema amministrativo-contabile nonché sull'affidabilità di quest'ultimo nel rappresentare correttamente i fatti di gestione”.*

Inoltre, il Sistema di Controllo Interno viene menzionato nel Codice Civile, tra gli obblighi del Comitato per il Controllo sulla Gestione, nell'ambito dell'adozione del modello monistico<sup>4</sup>:

*“Il comitato per il controllo sulla gestione... vigila sull'adeguatezza della struttura organizzativa della società, del sistema di controllo interno e del sistema amministrativo e contabile...”.*

Sulla base di quanto appena esposto, ci si è interrogati a lungo sulla obbligatorietà della costituzione di un sistema di controllo interno. Al riguardo, le diverse interpretazioni possono essere classificate nel seguente modo<sup>5</sup>:

- a) È obbligatoria l'adozione (e la manutenzione) di un sistema di controllo interno per tutte le società quotate, sulla base di quanto indicato all'interno del TUF;

---

<sup>3</sup> Art. 149, 1° comma, lett. c), D.Lgs. 24/02/1998 n. 58 (Testo Unico della Finanza, TUF).

<sup>4</sup> Art. 2409-octiesdecies, 5° comma, lett. b), Codice Civile.

<sup>5</sup> CHIAPPETTA F., *Diritto del governo societario*, Wolters Kluwer Italia, CEDAM, 2017, p. 228.

- b) Il sistema di controllo interno deve essere costituito anche all'interno dell'impresa che, seppur non quotata, adotta il modello monistico, in risposta all'art. 2409-octiesdecies, 5° comma, lett. b) del Codice Civile;
- c) Infine, un terzo approccio (e sicuramente anche quello più corretto) vede nella costituzione del sistema di controllo interno la risposta all'esigenza "di proceduralizzare l'attività di impresa svolta in forma di società per azioni", e quindi la necessità di costituire un tale sistema all'interno di tutte le società che adottano tale forma. In questo caso, nella ricostruzione della funzione e della struttura di un sistema di controllo interno, occorre prima di tutto valutare di volta in volta la natura e le dimensioni dell'impresa, e soprattutto far riferimento non tanto alle previsioni normative quanto alle indicazioni dell'autodisciplina.

A quanto appena affermato va aggiunto che il legislatore ordinario non ha fornito, forse volutamente, una definizione unitaria di Sistema di Controllo Interno. In ogni caso, alcune definizioni del sistema sono rintracciabili all'interno del Codice di Autodisciplina delle società quotate<sup>6</sup>:

*“Ogni emittente si dota di un sistema di controllo interno e di gestione dei rischi costituito dall'insieme delle regole, delle procedure e delle strutture organizzative volte a consentire l'identificazione, la misurazione, la gestione e il monitoraggio dei principali rischi.”*

E all'interno del cosiddetto CoSO Report, di cui si discuterà più avanti<sup>7</sup>:

*“Il controllo interno è un processo, svolto dal Consiglio di Amministrazione, dai dirigenti e da tutto il personale aziendale, finalizzato a fornire una ragionevole certezza sul raggiungimento degli obiettivi aziendali che rientrano in particolare nelle seguenti categorie:*

---

<sup>6</sup> Art. 7, P.1, *Codice di autodisciplina*, Comitato per la Corporate Governance, Borsa Italiana, 2018.

<sup>7</sup> L'*Internal Control – Integrated Framework* (cd. *CoSO Framework o report*) costituisce un Framework per l'elaborazione e l'implementazione del Sistema di controllo interno; pubblicato per la prima volta nel 1992 (ultima ed. 2013) da un Organismo internazionale chiamato *Committee of Sponsoring Organization of Tradeway Commission* (CoSO).

- *Efficacia ed efficienza delle attività operative (Operations);*
- *Attendibilità delle informazioni di bilancio (Financial reporting);*
- *Conformità alle leggi e regolamenti in vigore (Compliance).*

Sulla base di quanto riportato, è possibile definire il sistema di controllo interno come un “processo per la completa e corretta identificazione dei rischi aziendali”<sup>8</sup>, attraverso la quale è reso possibile il raggiungimento di finalità eterogenee, quali l’efficienza e la tracciabilità delle operazioni, l’affidabilità dell’informativa economico-finanziaria ed il rispetto delle leggi in vigore, senza tuttavia perdere di vista il conseguimento degli obiettivi strategici aziendali. Ovviamente, per quanto efficace sia il sistema di controllo, non è possibile garantire con certezza il raggiungimento degli obiettivi, ma solo con un ragionevole livello di assurance. Questo processo, infine, è svolto principalmente da risorse umane, che occupano i vari livelli dell’organizzazione.

### **1.2.2. La funzione**

La funzione principale di una tale architettura è quella di diventare un valido strumento per la gestione aziendale nelle mani dell’Organo direzionale. In particolare, il Sistema di Controllo Interno diviene indispensabile dal momento in cui la gestione *day by day* o diretta dell’impresa si scinde dalla “alta direzione strategica”, svolta dal CdA, in virtù della crescita dimensionale e della complessità dell’azienda. Con questo strumento si rende così possibile un miglioramento dell’attività di *monitoring* sulle procedure e sulla gestione dei rischi aziendali, in modo da poter ottenere un maggiore livello di *assurance* circa il raggiungimento degli obiettivi prefissati.

Infatti, è proprio in relazione all’attività di gestione dei rischi che il sistema di controllo interno assume una sua rilevanza: nella strutturazione di un sistema efficiente bisogna tenere in considerazione il *trade-off* esistente tra costi e benefici del controllo, ove l’equilibrio si raggiunge nel punto in cui il costo marginale dei controlli è pari ai benefici ottenuti in termini di riduzione del rischio residuo.

---

<sup>8</sup> CHIAPPETTA F., *Diritto del governo societario*, Wolters Kluwer Italia, CEDAM, 2017, p. 229.

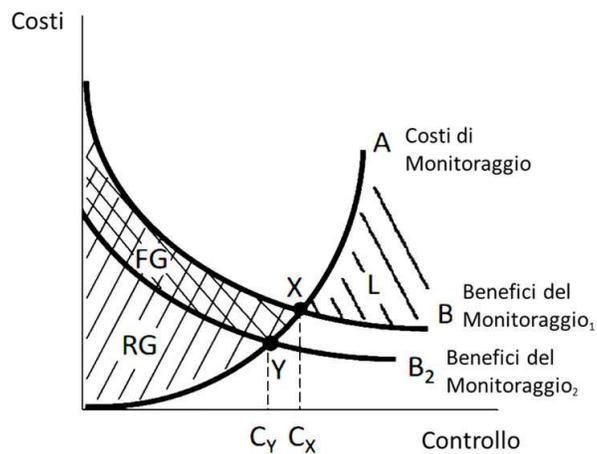


Figura 1 - Analisi costi-benefici del controllo

In sostanza, affinché un Sistema di Controllo Interno possa definirsi efficace, esso deve prevedere il rispetto delle seguenti fasi:

- 1) Mappatura dei rischi aziendali: è di fondamentale importanza identificare i principali rischi a cui va incontro un'impresa sulla base delle sue caratteristiche intrinseche e su quelle del settore di riferimento. Il risultato di quest'analisi è la produzione di una *risk map* e la prioritizzazione dei rischi;
- 2) Valutazione dei rischi prioritari: in questo modo si potrà ottenere una misura del rischio, utile per calcolo della convenienza all'implementazione di nuovi controlli;
- 3) Ricerca degli strumenti per la mitigazione e la gestione dei rischi: tra i principali vanno segnalati il principio di separazione dei ruoli ("*segregation of duties*"), tracciabilità e oggettivazione dei processi.

### 1.2.3. La struttura

In merito alla struttura del sistema di controllo interno, bisogna affermare sin da subito che né il legislatore né l'autodisciplina hanno previsto un modello unico da applicare ad ogni contesto aziendale, rimandando la scelta architetturale alle singole realtà cui si

manifesta la necessità di una sua realizzazione. Nonostante ciò, alcuni elementi rappresentano una costante imm modificabile che prescinde dai diversi contesti applicativi.

Per cominciare, “la responsabilità apicale del sistema di controllo interno compete al consiglio di amministrazione”, il quale svolge un ruolo di indirizzo strategico e di definizione degli obiettivi di rischio che l’impresa dovrà realizzare al fine della massimizzazione dei risultati e, di conseguenza, degli interessi degli interlocutori sociali. Per poter realizzare tali obiettivi di rischio, il CdA si avvale del management nello svolgimento dell’attività di *Risk Management*, cioè “l’insieme di processi attraverso cui l’azienda identifica, analizza, quantifica, comunica, elimina e monitora i rischi associati alle attività aziendali e ai processi operativi” al fine di minimizzare il rischio di incorrere in perdite e massimizzare il risultato aziendale.

In secondo luogo, il Consiglio di Amministrazione assume un ruolo di supervisione e controllo circa l’operato del management e della struttura operativa così predisposta. Nell’espletamento di tale incarico esso si avvale di specifici organi al suo interno, come il Comitato Controllo e Rischi e l’amministratore incaricato del sistema di controllo interno e di gestione dei rischi. In particolare:

*“Il consiglio di amministrazione, previo parere del comitato controllo e rischi... valuta con cadenza almeno annuale, l’adeguatezza del sistema di controllo interno e di gestione dei rischi rispetto alle caratteristiche dell’impresa e al profilo di rischio assunto, nonché la sua efficacia.”<sup>9</sup>*

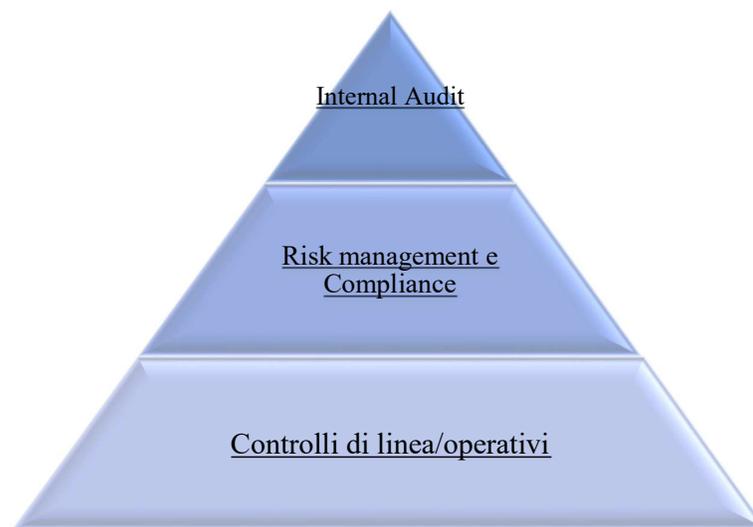
Infine, secondo il Codice di Autodisciplina spetta al Consiglio di Amministrazione, su proposta dell’amministratore incaricato del sistema di controllo interno e gestione dei rischi e sentito il collegio sindacale, il potere di nominare/revocare il responsabile della funzione Internal Audit. Questa funzione, la quale sarà d’ora in avanti principale oggetto di discussione, svolge il compito di verificare l’adeguatezza del sistema di controllo interno e, sulla base di un giudizio finale di assurance, proporre al consiglio

---

<sup>9</sup> Art. 7, C.1, lett. b), *Codice di autodisciplina*, Comitato per la Corporate Governance, Borsa Italiana, 2018.

di amministrazione e al management le azioni correttive da porre in essere al fine di riallineare il rischio residuo ai livelli coerenti con il raggiungimento degli obiettivi strategici.

#### **1.2.4. I tre livelli del controllo**



*Figura 2 - I tre livelli del controllo*

Nonostante l'assenza di espliciti richiami normativi in merito al raggiungimento di una struttura uniforme di sistema di controllo interno, le autoregolamentazioni sembrano essere in grado di definire dei punti cardine attorno ai quali costruire un modello di partenza. Questo modello, che si compone degli organi in parte esposti nelle righe precedenti, si articola su tre livelli, a ciascuno dei quali sono attribuite specifiche funzioni e relative responsabilità nell'attività di identificazione, misurazione, gestione e monitoraggio dei rischi aziendali.

La classificazione dei controlli interni è la seguente:

- 1) Controlli di primo livello: vengono altresì definiti come controlli “di linea” e consistono nei controlli effettuati dai manager dei singoli centri di responsabilità o unità organizzative. Sono controlli volti a verificare il corretto funzionamento dei singoli processi che sono stati predisposti dal management e possono essere di varia natura: procedurale, informatica, comportamentale e amministrativo-contabile.
- 2) Controlli di secondo livello: questi si possono definire come dei controlli trasversali sui rischi e sulla conformità e sono svolti da appositi organi aziendali, che concorrono a definire il sistema di controllo interno. Tra questi va menzionato il risk management, di cui si è accennato in precedenza e che assolve il ruolo di identificazione, misurazione, gestione e monitoraggio del rischio specifico relativo alle diverse aree gestionali.  
  
Altra tipologia di controllo di secondo livello è rappresentata dalla funzione Compliance, con riferimento al rischio di non conformità alla legge, ai regolamenti e alle regole di autocondotta della società. Altre forme di controllo di secondo livello vengono poste in essere dal Dirigente Preposto alla redazione dei documenti contabili societari, rispetto all’attestazione dell’informativa contabile-finanziaria della società, e il controllo di gestione, rispetto al raggiungimento degli obiettivi operativi e alla loro coerenza con le strategie.
- 3) Controlli di terzo livello: questa posizione è ricoperta dalla funzione di Internal Audit, la quale ha lo scopo di fornire un *assurance* riguardo la corretta predisposizione del sistema dei controlli interni, in particolare quelli di primo e di secondo livello. Rispetto alle precedenti linee di controllo, questa si caratterizza per l’assunzione di una posizione di indipendenza, confermata dal fatto che la stessa può essere svolta anche da un soggetto esterno indipendente. Tuttavia, si ritiene opportuno sollevare alcuni dubbi in merito all’indipendenza dell’attività di internal auditing dal momento in cui il responsabile della funzione viene nominato/revocato dal consiglio di amministrazione, ma di questo se ne parlerà meglio nei prossimi paragrafi.

### **1.3. I modelli internazionali in tema di controllo interno: dal *CoSO Report* all'*Enterprise Risk Management***

#### **1.3.1. Il CoSO Framework**

È stato più volte accennato nel paragrafo precedente come l'aumentare dell'esigenza della predisposizione di un efficiente sistema di controllo interno non è stata accompagnata da un adeguato processo di legiferazione in merito alle tecniche e alle modalità di una sua attuazione. Fortunatamente, queste pressioni hanno portato alla creazione, negli Stati Uniti, di una organizzazione volontaria e privata, il cui fine era quello di “migliorare la qualità dell'informativa finanziaria attraverso l'eticità del business, l'effettività del sistema di controllo interno e la solidità della corporate governance”: la Committee of Sponsoring Organizations of the Treadway Commission (CoSO). La Commissione, composta dai membri delle principali istituzioni in materia di controlli aziendali come l'American Institute of Certified Public Accountants (AICPA), l'American Accounting Association (AAA), il Financial Executives Institute (FEI), l'Institute of Internal Auditors (IIA) e l'Institute of Management Accountants (IMA), è stata istituita nel 1985 e ha pubblicato per la prima volta il documento finale nel 1992 con il nome di “Internal Control – Integrated Framework”, successivamente denominato CoSO Report.

Il CoSO Report non costituisce un atto avente forza di legge, e in quanto tale non è previsto alcun obbligo riguardante la sua applicazione, né tantomeno si tratta di uno standard applicativo. Piuttosto, il CoSO Report costituisce un “framework contenente delle *best practices* professionali per la realizzazione di processi e sistemi di business volti a promuovere un efficace ed efficiente controllo interno”<sup>10</sup>.

Secondo il CoSO Framework il controllo interno si definisce come “un processo messo in atto dal consiglio di amministrazione, dal management e da tutto il personale, volto a fornire una ragionevole garanzia sul raggiungimento dei seguenti obiettivi:

- Efficacia ed efficienza delle attività operative;

---

<sup>10</sup> MOELLER R., *Brink's modern internal auditing: a common body of knowledge*, John Wiley & Sons, 2016, pag. 29.

- Attendibilità delle informazioni di bilancio;
- Conformità alle leggi e alle norme vigenti (compliance).”

Attraverso tale definizione, il modello preposto intende chiarire la posizione del sistema di controllo interno come valido strumento a disposizione dell’alta direzione aziendale per il raggiungimento degli obiettivi operativi, di reporting finanziario e di compliance, mediante il coinvolgimento di tutti gli attori presenti all’interno dell’organizzazione (consiglio di amministrazione, management, internal audit e il resto del personale aziendale). In particolare, questo strumento è in grado di ridurre il rischio del mancato raggiungimento degli obiettivi se e solo se tutte le componenti sono presenti e perfettamente funzionanti tra loro, in una logica di integrazione e coordinamento.

Le componenti di cui è costituito un sistema di controllo interno, secondo il CoSO Report, sono:

- 1) Ambiente di controllo;
- 2) Valutazione dei rischi;
- 3) Attività di controllo;
- 4) Informazioni e comunicazione;
- 5) Monitoraggio.



Figura 3 - Il CoSO Report: rappresentazione grafica

Osservando la figura è possibile notare come le cinque componenti del CoSO Report siano tutte collegate ai tre obiettivi del sistema di controllo interno (operativi, di reporting, di compliance) e come tale approccio possa essere applicato indistintamente all'azienda nel suo complesso e alla singola *business unit*<sup>11</sup>, nonché ad ogni impresa, a prescindere dalla sua dimensione e struttura interna. Segue una breve descrizione delle singole componenti.

Quanto all'ambiente di controllo, esso si pone al vertice delle componenti che devono essere presenti in un'organizzazione per la predisposizione di un efficiente sistema di controllo interno. L'ambiente di controllo, stando a quanto riferisce il CoSO Report, si definisce come "l'insieme di valori, idee, motivazioni, convinzioni e comportamenti il cui riconoscimento e la cui condivisione da parte dell'organizzazione ne orienta in misura significativa il modo di operare, con particolare riferimento all'attività di controllo". Questo è influenzato da diversi fattori, interni ed esterni, come la storia dell'azienda, i valori morali ed etici delle persone al suo interno, lo stile manageriale e la struttura organizzativa. Affinché si possa considerare efficace<sup>12</sup>, l'ambiente di controllo deve essere tale da rendere l'impresa resiliente nell'affrontare le pressioni esterne, ed elementi come una forte cultura aziendale rendono forte a sua volta l'intero ambiente di controllo.

La seconda componente è rappresentata dall'attività di valutazione dei rischi, o *risk assessment*. Questa si sviluppa in tre fasi:

- a) Definizione degli obiettivi: questa fase, nonostante può apparire a primo impatto estranea rispetto al sistema di controllo interno, ne rappresenta un presupposto. Infatti, il governo aziendale stabilisce in relazione agli obiettivi che intende raggiungere un livello di rischio accettabile;
- b) Identificazione dei rischi: in relazione agli obiettivi che l'impresa intende raggiungere verranno classificati i rischi relativi alle diverse aree di pertinenza. È importante precisare che non tutti i rischi possono avere un impatto

---

<sup>11</sup> ANACLERIO M., MIGLIETTA A., SQUAIELLA S., *Internal Audit: dalla teoria alla pratica*, Wolters Kluwer, IPSOA, 2007, pag. 17.

<sup>12</sup> MOELLER R., *Brink's modern internal auditing: a common body of knowledge*, John Wiley & Sons, 2016, pag. 39.

significativo sull'impresa e ciò giustifica l'importanza di stabilire *ex ante* gli obiettivi in relazione ai quali tali rischi vengono identificati;

- c) Analisi dei rischi: questa si articola a sua volta in valutazione del rischio, misurazione del livello di probabilità e impatto e gestione del rischio. Le strategie di risposta al rischio sono riconducibili alle seguenti quattro categorie<sup>13</sup>: evitare il rischio, riduzione del rischio, condivisione, accettazione.



Figura 4 - Il CoSO Report: risk assessment

Le attività di controllo<sup>14</sup> sono “le procedure e le azioni svolte dalle persone che operano in un’impresa, allo scopo di realizzarne gli obiettivi, ed includono svariate attività come, ad esempio, autorizzazioni, controlli fisici, separazione dei compiti, adeguata documentazione e registrazione delle operazioni, ecc.” Queste si distinguono in base alla tempistica del controllo in controlli preventivi e controlli successivi; mentre in funzione delle modalità con cui viene esercitato il controllo avremo dei controlli manuali e automatizzati.

La quarta componente concerne l’informazione e la comunicazione e prevede che “le informazioni rilevanti, interne ed esterne, siano tempestivamente identificate, catturate, elaborate e diffuse in tutta l’organizzazione”. Questa componente è di fondamentale importanza, specialmente in relazione alla diffusione della cultura etica aziendale: non basta che l’organizzazione adotti un codice etico e delle procedure di

<sup>13</sup> MOELLER R., *Brink’s modern internal auditing: a common body of knowledge*, John Wiley & Sons, 2016, pag. 44.

<sup>14</sup> ANACLERIO M., MIGLIETTA A., SQUAIELLA S., *Internal Audit: dalla teoria alla pratica*, Wolters Kluwer, IPSOA, 2007, pag. 21.

controllo adeguate, c'è bisogno che le stesse vengano comunicate a tutto il personale dipendente ai fini di una loro piena condivisione. La comunicazione è inoltre essenziale per la definizione dei ruoli e delle responsabilità all'interno dell'impresa.

Per concludere, l'ultima componente del CoSO Report è il monitoraggio. Per meglio comprendere il valore di questa componente occorre fare un passo indietro e focalizzarsi sul concetto di rischio di impresa, quale fattore che abbia un impatto negativo sul raggiungimento degli obiettivi aziendali. In merito a questo aspetto, bisogna aggiungere che i rischi a cui un'impresa si espone possono variare nel tempo, sulla base di un mutamento continuo delle condizioni interne ed esterne della stessa. Proprio per tale motivo si rende necessario il processo di valutazione continua nel tempo delle performance del sistema di controllo, "al fine di garantire che esso continui a funzionare coerentemente ai cambiamenti dell'impresa". Attraverso il monitoraggio, in sintesi, si garantisce nel tempo l'adeguatezza del sistema dei controlli interni in relazione alla gestione dei rischi.



*Figura 5 - Il CoSO Report: attività di monitoraggio*

### 1.3.2. L'Enterprise Risk Management o il CoSO ERM

A partire dalla pubblicazione della prima edizione del CoSO Report, le discussioni in tema di corporate governance e di sistema di controllo interno sono, negli anni, profondamente mutate. In particolare, ha preso sempre più piede l'idea di una corporate governance quale strumento per il raggiungimento degli obiettivi aziendali, il quale non può prescindere da un'attenta e accurata gestione dei rischi. Proprio in relazione a quest'ultimo aspetto le autoregolamentazioni di diversi Paesi hanno rivolto una sempre maggiore attenzione, fino a collocare l'attività di risk management tra le principali responsabilità del consiglio di amministrazione<sup>15</sup>, e quindi della massima direzione aziendale. Inoltre, si fa presente che in Paesi quali l'Australia, la Nuova Zelanda e la Germania si è imposta l'introduzione a tutte le imprese di sistemi di risk management<sup>16</sup>, a cui l'Italia ha fatto seguito mediante l'emanazione di un regolamento da parte dell'ISVAP<sup>17</sup>, il quale si rivolge tuttavia alle sole imprese assicurative.

Da questo contesto nasce l'idea che ai fini del raggiungimento dei propri obiettivi, un'impresa dovrà avere sempre più riguardo alla predisposizione di un corretto sistema di governance aziendale, la quale non si limita a concetti come la composizione e il ruolo del consiglio di amministrazione o alla *executive compensation*, ma si estende alle modalità pratiche o operative attraverso cui le decisioni vengono prese e le azioni eseguite, in un'ottica di contenimento dei rischi entro una soglia tollerabile. Ai fini illustrativi, potremmo considerare il risk management come una macro-area della corporate governance, al cui interno rientra il sistema di controllo interno.

---

<sup>15</sup> BORSA ITALIANA S.p.A., *Codice di autodisciplina*, Comitato per la Corporate Governance, 2018.

<sup>16</sup> DITTMEIER C., *Internal Auditing: chiave per la corporate governance*, EGEA, 2011, pag. 141.

<sup>17</sup> ISVAP, Regolamento n. 20/2008.



Figura 6 - Formalizzazione del sistema dei controlli

La crescente importanza della gestione dei rischi aziendali in materia di corporate governance ha portato alla pubblicazione nel 2004, da parte della Committee of Sponsoring Organizations of the Treadway Commission, di un nuovo modello di controllo: l'Enterprise Risk Management Framework, comunemente definito come CoSO ERM. Con la pubblicazione di questo modello si è fornito un approccio innovativo che permetta all'impresa o nello specifico alla funzione di internal auditing di considerare e gestire i rischi a tutti i livelli dell'attività di impresa, dalle singole aree operative al business nel suo complesso.

L'obiettivo di questo framework non è solo quello di fornire al management un valido strumento per l'identificazione dei rischi aziendali e la valutazione di un loro impatto, ma altresì quello di permettere una loro assunzione consapevole e infine una loro mitigazione, in un'ottica di creazione di valore nel medio-lungo periodo. Ciò è reso possibile attraverso<sup>18</sup>:

---

<sup>18</sup> COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO), *Enterprise Risk Management, Integrated Framework*, 2004; ed. it. a cura di AIIA e PwC, *La gestione del rischio aziendale*, Milano, Il Sole 24 Ore, 2006.

- L'allineamento della strategia alla propensione al rischio (*risk appetite*): strategia e rischio sono strettamente legati dal fatto che per conseguire un determinato obiettivo, dovrò necessariamente sostenere un determinato livello di rischio. Di conseguenza, la definizione degli obiettivi passa necessariamente attraverso la primaria definizione del livello di rischio accettabile, e di quello che sono pronto a sostenere. In questo senso, la strategia aziendale trova le sue fondamenta in un'attenta analisi e valutazione dei rischi di impresa.
- La scelta delle azioni di risposta ai rischi previamente identificati e valutati, che verrà effettuata tra: evitarlo, ridurlo, dividerlo o accettarlo.
- L'identificazione dei rischi correlati e multipli: il nuovo modello favorisce un approccio integrato nella valutazione degli impatti degli eventi rischiosi sul risultato aziendale.
- L'identificazione delle opportunità: partendo dalla definizione di base di rischio e accettandone la duplicità di un suo effetto che ne permette la distinzione in *upside risk* e *downside risk*, il nuovo modello vede nel rischio di scostamenti dagli obiettivi delle opportunità di miglioramento del risultato aziendale. L'azienda che è in grado di comprendere le dinamiche di rischio che riguardano il proprio business è altresì in grado di cogliere le opportunità che da tali eventi derivano.
- Il miglioramento dell'impiego di capitale: saper governare i rischi permette infine una più efficiente allocazione del capitale.

Il nuovo Framework, inoltre, fornisce la seguente definizione di Enterprise Risk Management:

*“L'Enterprise Risk Management è un processo, posto in essere dal Consiglio di Amministrazione, dai dirigenti e da altri operatori della struttura aziendale, utilizzato per la formulazione delle strategie in tutta l'organizzazione, progettato per individuare eventi potenziali che possono influire sull'attività aziendale, per gestire il rischio entro i limiti del “rischio accettabile” e per fornire una ragionevole sicurezza sul conseguimento degli obiettivi aziendali”.*

Da questa definizione è possibile comprendere che l'ERM è prima di tutto un processo, cioè un set di azioni per la realizzazione di un risultato. Tuttavia, la scelta dell'utilizzo del termine processo per descrivere la gestione dei rischi di impresa sembra richiamare piuttosto al suo carattere di dinamicità e flessibilità<sup>19</sup>, che lo rende diverso da una banale esecuzione di compiti impartiti in un *rule book*. Inoltre, è un processo posto in essere dalle persone ad ogni livello aziendale, in quanto solo le persone possono realmente comprendere a fondo le singole dinamiche di rischio e gli effetti che queste comportano.

È un processo utilizzato per la formulazione delle strategie in quanto, come precedentemente affermato, soltanto attraverso la definizione di un livello di rischio accettabili l'impresa è realmente in grado di stabilire le azioni perseguibili dal management che rientrano entro tale soglia. A tal riguardo, il nuovo modello aggiunge una nuova tipologia di obiettivo perseguibile attraverso l'ERM rispetto a quelle già trattate dal precedente Report del 1992 (operativi, di reporting e di compliance): quella degli obiettivi strategici.

Infine, il nuovo modello è in grado di fornire solo una ragionevole sicurezza sul raggiungimento degli obiettivi, in quanto si ritiene impossibile prevedere ogni evento futuro al fine di ridurre il rischio ad un livello prossimo allo zero.

La rappresentazione del nuovo modello segue la scia di quella del suo predecessore: elementi interconnessi in una visione olistica tra cui emergono, oltre ai “nuovi” obiettivi strategici, anche ulteriori componenti.

---

<sup>19</sup> MOELLER R., *Brink's modern internal auditing: a common body of knowledge*, John Wiley & Sons, 2016, pag. 154.

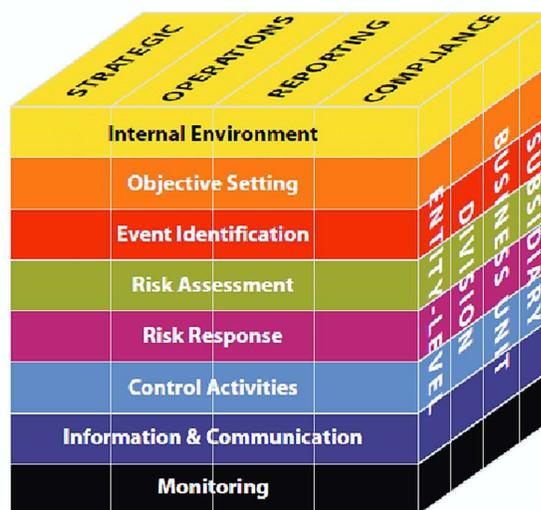


Figura 7 - Il CoSO ERM: rappresentazione grafica

Le componenti sono otto e sono le seguenti:

- 1) Definizione degli obiettivi;
- 2) Identificazione degli eventi;
- 3) Risk assessment;
- 4) Risposta al rischio;
- 5) Ambiente di controllo;
- 6) Attività di controllo;
- 7) Informazione e comunicazione;
- 8) Monitoraggio.

A seguito della definizione degli obiettivi, ciascuna impresa dovrà affrontare un processo di gestione dei rischi, il quale va dalla seconda alla quarta fase. L'ultima fase di questo processo, la risposta al rischio, sarà in grado di definire le azioni che dovranno essere poste in seguito. Infatti, qualora dall'analisi dei rischi dovesse emergere la necessità di evitare o ridurre i rischi rilevati, sarà necessario proseguire con un secondo processo, definito di predisposizione e di attuazione del sistema di controllo interno, il quale coincide con le componenti che vanno dall'ambiente di controllo al monitoraggio.

Nonostante la prima interpretazione appena proposta, bisogna tenere presente che<sup>20</sup> “l’ERM non è un procedimento strettamente sequenziale, ma un processo interattivo e multidirezionale in cui ogni componente può influire su un’altra, indipendentemente dalla sequenza dello stesso”.

Per concludere, partendo dalla constatazione che le componenti dell’ERM si identificano in parte con quelle precedentemente trattate nell’ambito della discussione del CoSO Report, ai fini del seguente lavoro si ritiene opportuno approfondire le principali differenze dei due modelli fin qui esposti.

### **1.3.3. Le principali differenze tra il CoSO Framework e l’ERM**

Per cominciare, bisogna affermare che l’Enterprise Risk Management Framework costituisce un’evoluzione del CoSO Report e in quanto tale non se ne distacca in merito alle finalità, quanto piuttosto in merito alle modalità attuative di un sistema di controllo interno efficace ed efficiente, che si manifesta nel nuovo modello attraverso un approccio maggiormente basato sul rischio. A tal riguardo, Robert Moeller scrive<sup>21</sup>:

*“CoSO ERM sometimes looks like its internal controls brother (cfr. CoSO Report, 1992), but it has a much different feel and approach”.*

Diverse sono infatti le differenze tra i due modelli proposti dalla Committee of Sponsoring Organization of the Treadway Commission, tra cui<sup>22</sup>:

- Gli obiettivi di reporting: mentre nell’ERM Framework per reporting si fa riferimento ad informazioni di diversa natura, sia essa economico-finanziaria o gestionale, e con diverse modalità di diffusione, sia interna che esterna, il suo predecessore guarda all’obiettivo di reporting esclusivamente nell’ottica della affidabilità della reportistica economico-finanziaria;

---

<sup>20</sup> DITTMER C., *Internal Auditing: chiave per la corporate governance*, EGEA, 2011, pag. 149.

<sup>21</sup> MOELLER R., *Brink’s modern internal auditing: a common body of knowledge*, John Wiley & Sons, 2016, pag. 142.

<sup>22</sup> DITTMER C., *Internal Auditing: chiave per la corporate governance*, EGEA, 2011, pag. 167.

- Gli obiettivi strategici: come precedentemente affermato e come rappresentato dal “Cubo – ERM”, il nuovo approccio aggiunge una nuova categoria agli obiettivi, cioè quella di natura strategica;
- L’ambiente di controllo: nel modello del 1992 questo rappresentava il primo elemento fondante di un sistema di controllo interno efficace ed efficiente, in grado di influenzare tutte le altre componenti e gli obiettivi. Attraverso l’instaurazione di un ambiente di controllo basato su principi di eticità e correttezza era possibile esprimere il miglior assetto dei controlli interni aziendali. Con il nuovo approccio, invece, si pone una maggiore enfasi non tanto all’ambiente di controllo, quanto all’ambiente interno nel suo complesso, con particolare riguardo all’attività di gestione dei rischi posta a capo di ogni singola unità decisionale.
- Risk management: l’attività di gestione dei rischi viene affrontata in entrambi i modelli, ma in maniera decisamente più approfondita nel secondo. La prima differenza sostanziale ha ad oggetto la fattispecie “positiva” di rischio, il quale può rappresentare anche un’opportunità di creazione di valore per l’impresa, e non esclusivamente un evento negativo, se gestito correttamente e con l’approccio prescritto. In secondo luogo, l’ERM fornisce delle nozioni ulteriori quali quelle di *rischio inerente* e *rischio residuo*. Il primo costituisce il livello di rischio relativo all’intera impresa in considerazione dell’incrocio di due *driver* fondamentali, probabilità impatto, senza considerare l’effetto dei controlli interni nella riduzione di questo. Il rischio residuo, invece, rappresenta il rischio cui l’impresa va incontro una volta che sono stati predisposti i relativi controlli e poste in essere le azioni di risposta al rischio inerente. Va aggiunto inoltre che si ritiene opportuno un adeguamento del sistema di controllo interno qualora il rischio residuo misurato risulti superiore rispetto agli obiettivi di rischio predeterminati;
- Informazione e comunicazione: nell’ambito di tale componente, il nuovo approccio palesa la necessità di divulgare, tra le varie informazioni, anche quelle relative a dati previsionali;

Infine, come più volte ricordato, i due modelli sono simili sotto molteplici aspetti. In ogni caso, si ritiene necessario ricordare che ogni sistema di controllo è, nella pratica,

diverso da quello esistente in altre realtà aziendali. Tuttavia, devono comunque esistere tutti gli elementi fin qui trattati affinché si possa costituire un sistema di controllo efficace ed efficiente.

#### **1.3.4. ERM Integrating with strategy and performance: l'ultimo aggiornamento del modello**

La Committee of Sponsoring Organizations of the Treadway Commission ha pubblicato nel mese di Giugno 2017 un aggiornamento del modello ERM precedentemente trattato, definendolo “*ERM Integrating with strategy and performance*”, il quale pone particolare enfasi agli aspetti della definizione della strategia e valutazione della performance. Le principali novità introdotte dal modello sono<sup>23</sup>:

- 1) Integrazione del processo di gestione dei rischi aziendali nella fase di definizione della strategia;
- 2) Correlazione tra definizione delle performance aziendali ed Enterprise Risk Management;
- 3) Considerazione del ruolo della globalizzazione dei mercati e delle operazioni nel processo di ERM;
- 4) Considerazione del rischio nella fase di definizione e raggiungimento degli obiettivi aziendali;
- 5) Maggiore coinvolgimento degli stakeholder aziendali nella fase di *information and communication*;
- 6) Implementazione, all'interno del processo decisionale, delle tecnologie informatiche e di elaborazione dei dati;
- 7) Assegnazione al board di primaria responsabilità in merito al processo di definizione e supervisione dei rischi (*risk oversight*).

---

<sup>23</sup> COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO), *Enterprise Risk Management, Integrating with strategy and performance*, 2017.

Infine, il nuovo Framework identifica venti principi tra cui: che il board presieda al processo di supervisione dei rischi e che definisca la struttura operativa e la cultura aziendale desiderata; che sia analizzato il contesto di business, definito il risk appetite e valutate le alternative strategiche prima della definizione degli obiettivi operativi; che sia implementato un sistema di risk management fondato su identificazione, valutazione, prioritizzazione e gestione dei rischi aziendali; che sia posto in essere un continuo monitoraggio del sistema; che le informazioni riguardanti i rischi, la cultura e le performance, siano comunicate e diffuse anche attraverso il supporto delle tecnologie. Ciascuno di questi principi è legato ad una delle cinque seguenti componenti: *Governance and Culture, Strategy and Objective-Setting, Performance, Review and Revision, Information Communication and Reporting.*

#### **1.4. Il contesto autoregolamentare di riferimento in materia di Internal Audit**

Nelle pagine precedenti è stato trattato a fondo il concetto di Sistema di Controllo Interno e la conformazione che questo ha assunto fino ad oggi nelle principali prassi societarie. È stato inoltre chiarito che, in tema di controlli interni, il legislatore ha lasciato ampio margine di discrezione alle singole realtà aziendali e, in particolare, alle organizzazioni private che, attraverso la pubblicazione di framework e standard internazionali, hanno permesso di uniformare quanto più possibile la disciplina garantendo, allo stesso tempo, la applicabilità dei modelli al complesso ed eterogeneo universo aziendale. Tuttavia, ai fini del presente lavoro, gli argomenti trattati assumono carattere introduttivo e propedeutico per la più complessa e specifica trattazione della Funzione di Internal Audit, o revisione interna aziendale.

L'*Internal Audit Function* (IAF) rappresenta un tipo di controllo di terzo livello<sup>24</sup> e anche in merito alla sua definizione, o realizzazione, bisogna far necessariamente riferimento alle fonti autoregolamentari nazionali ed internazionali in materia. In questo paragrafo verranno trattati il Codice di autodisciplina di Borsa Italiana, in

---

<sup>24</sup> Vedi capitolo I, paragrafo 2.4, *I tre livelli del controllo.*

ambito nazionale, e gli International Professional Practices Framework, in ambito internazionale.

#### **1.4.1. Il Codice di autodisciplina delle società quotate**

Il Codice di autodisciplina delle società quotate è il principale punto di riferimento nazionale in tema di corporate governance. Esso è stato redatto da un comitato di Borsa Italiana S.p.A. e pubblicato, nella prima versione, nel 1999 per poi essere aggiornato fino alle più recenti versioni negli scorsi anni. Il Codice, come suggerisce il suo nome, nasce col fine di disciplinare la materia della corporate governance all'interno delle società quotate in borsa, in virtù della loro rilevanza sul pubblico risparmio. Tuttavia, trattandosi di un documento il cui fine è quello di migliorare il governo societario, anche le imprese medio-grandi non quotate hanno iniziato ad uniformarsi alle principali linee guida contenute al suo interno, tra cui:

- a) La presenza di consiglieri indipendenti all'interno del Consiglio di Amministrazione;
- b) La attribuzione degli incarichi rilevanti in capo a persone differenti, in applicazione del principio generale di *segregation of duties*, la quale trova applicazione, ad esempio, nella separazione di Presidente del CdA e Amministratore Delegato;
- c) Ruolo e funzione dei comitati interni;
- d) Politiche di remunerazione manageriale;
- e) Nozione di sistema di controllo interno.

Con riferimento a quest'ultimo elemento, è già stata fornita la sua definizione e trattata l'importanza che il Consiglio di Amministrazione riveste nei suoi confronti e nei confronti dell'attività di risk management. In particolare, si è detto che il CdA riveste un ruolo di impulso nella definizione del Sistema di Controllo Interno, nella valutazione periodica delle sue performance e nella attribuzione di deleghe, in materia, a un amministratore per la sovrintendenza del Sistema di Controllo Interno. In altre parole, "il consiglio di amministrazione è il responsabile primario del sistema di

controllo interno”<sup>25</sup>. L’amministratore incaricato di sovrintendere alla funzionalità del sistema di controllo interno, a sua volta, “propone al consiglio di amministrazione la nomina, la revoca, e la remunerazione di uno o più preposti al controllo interno”<sup>26</sup>.

È proprio in questo passaggio che il Codice introduce, nell’ambito della costituzione di un più efficiente ambiente di corporate governance, l’esigenza dell’esistenza di una figura che eserciti un controllo di terzo livello. Infatti, la figura del Preposto al Controllo Interno coincide di fatto con il responsabile della funzione di internal auditing, in quanto esso<sup>27</sup>:

- “È incaricato di verificare che il sistema di controllo interno sia sempre adeguato, pienamente operativo e funzionante;
- Non è responsabile di alcuna area operativa, ivi inclusa l’area Amministrazione, Finanza e Controllo;
- Ha accesso diretto a tutte le informazioni utili per lo svolgimento del proprio incarico;
- Dispone di mezzi adeguati allo svolgimento della funzione assegnata;
- Riferisce del proprio operato al comitato per il controllo interno ed al collegio sindacale; può inoltre essere previsto che riferisca anche all’amministratore esecutivo incaricato di sovrintendere alla funzionalità del sistema di controllo interno. In particolare, riferisce circa le modalità con cui viene condotta la gestione dei rischi, nonché sul rispetto dei piani definiti per il loro contenimento ed esprime la sua valutazione sull’idoneità del sistema di controllo interno a conseguire un accettabile profilo di rischio complessivo”.

Ove l’ultima riga fa effettivo riferimento ad una funzione aziendale il cui compito è quello di fornire un’assurance sulla efficacia ed efficienza dei controlli di impresa (di primo e di secondo livello), affinché l’intero sistema sia idoneo a perseguire gli obiettivi di rischio definiti dal consiglio di amministrazione. Infine, nel criterio

---

<sup>25</sup> ANACLERIO M., MIGLIETTA A., SQUAIELLA S., *Internal Audit: dalla teoria alla pratica*, Wolters Kluwer, IPSOA, 2007, pag. 71.

<sup>26</sup> Art. 8, C.5, lett. c), *Codice di autodisciplina*, Comitato per la Corporate Governance, Borsa Italiana, 2018.

<sup>27</sup> Art. 8, C.6, *Codice di autodisciplina*, Comitato per la Corporate Governance, Borsa Italiana, 2018.

applicativo immediatamente successivo, il Codice afferma che<sup>28</sup> “l’emittente istituisce una funzione di internal audit” e che “il preposto al controllo interno si identifica con il responsabile di tale funzione”. Inoltre, il Codice prevede la possibilità che tale funzione sia ricoperta da soggetti esterni all’emittente, a condizione che tali soggetti siano dotati di requisiti di professionalità e indipendenza. Tale scelta dovrà essere in ogni caso motivata e comunicata agli azionisti.

Tra i requisiti che l’internal auditor deve possedere va evidenziato sicuramente quello dell’indipendenza. Tuttavia, dalla lettura del Codice di autodisciplina sorgono alcune perplessità circa la coesistenza del concetto di indipendenza della funzione con la naturale “dipendenza” della stessa nei confronti del Consiglio di Amministrazione<sup>29</sup>, il quale nomina/revoca il responsabile della funzione, ne definisce la remunerazione e ne assicura le necessarie risorse per l’espletamento dell’incarico. Nonostante sia innegabile l’esistenza di una relazione tra i due elementi, va fatto presente che il primo rappresenta un organo societario indispensabile per il governo dell’impresa, il quale dà impulso alla creazione del secondo, rappresentato da una funzione, l’Internal Audit, il cui requisito di indipendenza è garantito anche dalla posizione nell’organigramma che essa va a rivestire. Infatti, l’Internal Audit dovrà riferire circa il suo operato e i risultati ottenuti in sede dell’attività di auditing, in ordine, nei confronti del:

- Comitato controllo e rischi;
- Collegio sindacale;
- Amministratore incaricato di sovrintendere alla funzionalità del Sistema di Controllo Interno;
- Consiglio di Amministrazione.

Per tale motivo, da un punto di vista di riporto funzionale, l’indipendenza della funzione è resa possibile, in via primaria, dal rapporto diretto di questa con il comitato controllo e rischi ovvero tra il responsabile della funzione e il Presidente di tale comitato nonché il Presidente del Consiglio di Amministrazione. Inoltre, le linee di riporto dovranno essere ben definite all’interno del Mandato di Internal Audit, di cui

---

<sup>28</sup> Art. 8, C.7, *Codice di autodisciplina*, Comitato per la Corporate Governance, Borsa Italiana, 2018.

<sup>29</sup> CHIAPPETTA F., *Diritto del governo societario*, Wolters Kluwer Italia, CEDAM, 2017, p. 236.

se ne parlerà nel prossimo sottoparagrafo. Quanto appena esposto serve a chiarire come il legame diretto tra il consiglio di amministrazione e la funzione di revisione interna, che si genera a partire dai poteri di nomina/revoca della funzione attribuiti al primo, serve *in primis* a facilitare l'operatività dell'internal auditing senza che ciò mini l'indipendenza della funzione.

Per concludere, quanto appena esposto basta a confermare come fonti di rilievo richiedono la realizzazione di una funzione che, dall'interno dell'impresa, sia in grado di asseverare l'esistenza e il corretto funzionamento dei controlli aziendali. Tuttavia, occorre ricordare che la natura autoregolamentare del provvedimento non lo rende applicabile *ex lege* neppure alle stesse società quotate verso cui esso è rivolto. Tuttavia, è stato comunque previsto il principio di *comply or explain*, secondo cui la mancata conformità alle disposizioni contenute all'interno del Codice è ritenuta lecita solamente se accompagnata da valide ragioni a sostegno di tale scelta. Inoltre, come detto precedentemente, nonostante la sua natura autoregolamentare il Codice di autodisciplina sta diventando sempre più un punto di riferimento anche per le società che non sono quotate nei listini di Borsa.

#### **1.4.2. L'International Professional Practices Framework**

L'International Professional Practices Framework (IPPF) è uno schema concettuale con il quale vengono organizzate un insieme di linee guida per la realizzazione di un efficiente internal auditing. Questo Framework può essere equiparato al CoSO Framework, visto precedentemente, con la differenza che in questo caso l'intento è quello di fornire uno schema concettuale con cui disporre la funzione di revisione interna, piuttosto che il più ampio sistema dei controlli trattato nelle pagine precedenti. L'IPPF contiene un insieme di *guidance* emanate dall'Institute of Internal Auditors (IIA), fondata a New York nel 1941 e divenuta ben presto la principale associazione di categoria in materia di Internal Audit<sup>30</sup>.

---

<sup>30</sup> Si fa presente che, in materia di internal auditing, anche l'Italia ha la sua associazione per la promozione e lo sviluppo della professione: l'Associazione Italiana Internal Auditors (AIIA). L'AIIA

La prima versione dell'IPPF è stata pubblicata nel 1999, successivamente modificata con un'ampia rivisitazione nella versione del 2009 e in quella ancora più recente del Luglio 2015. In particolare, rispetto alla versione embrionale del '99, come è stato più volte affrontato in precedenza, sono aumentati gli standard richiesti dal mercato globale in tema di corporate governance e cultura del controllo aziendale. Per tale motivo, il Comitato di Revisione o Relook Task Force (RTF) dell'Institute of Internal Auditors è stato incaricato di riadattare i contenuti e la struttura del Framework alle nuove esigenze espresse. In sostanza, le principali modifiche riguardano:

- La mission dell'Internal Auditing;
- I principi fondamentali per la pratica professionale dell'Internal Auditing;
- La transizione da Guidance Interpretative a Guidance Attuative.



Figura 8 - International Professional Practices Framework: rappresentazione grafica

---

funge da affiliata italiana dell'IIA e attraverso la piena condivisione dei principi, delle finalità, della definizione di internal auditing, degli standard professionali IIA e del Codice etico per la professione, ne permette lo sviluppo nel nostro Paese.

Come è stato detto, l'IPPF contiene le *guidance* per la definizione, per l'attuazione e per la conduzione della Professione in modo efficiente. Queste linee guida si dividono in:

- a) *Mandatory Guidance*, o linee guida vincolanti;
- b) *Strongly Recommended Guidance*, o linee guida fortemente raccomandate.

Le linee guida vincolanti richiedono la piena conformità, in quanto ritenute essenziali per la pratica professionale dell'internal auditing. Esse sono:

- 1) Definizione: fornisce gli elementi *core* per la comprensione dell'attività di internal auditing, enunciando gli obiettivi, la natura e l'ambito di riferimento dell'attività;
- 2) Principi Fondamentali: costituiscono gli elementi chiave su cui deve fondarsi la professione;
- 3) Codice Etico: definisce i principi e le aspettative che devono ispirare i comportamenti individuali e delle organizzazioni nella condotta dell'attività di internal audit;
- 4) Standard Internazionali: si tratta di standard *principle-based* per lo svolgimento e la promozione dell'attività di internal auditing.

Le linee guida fortemente raccomandate, invece, non si ritengono necessarie in via assoluta ai fini dello svolgimento dell'attività di internal auditing ma comunque rappresentano degli standard descrittivi finalizzati all'effettiva implementazione del Codice Etico e degli Standard Internazionali. Pertanto, non essendo vincolanti ai fini della nostra trattazione ci limiteremo a fornire la loro principale distinzione in:

- *Guide Interpretative*: per orientare l'approccio, le metodologie e la considerazione dell'attività di internal auditing, senza tuttavia dettagliare processi e procedure;
- *Guide Supplementari*: per dettagliare i processi dell'attività di internal auditing;
- *Position Paper*: per delineare i ruoli e le responsabilità degli auditor in materia di governance, rischi e controlli.

Tornando alle linee guida vincolanti, l'IPPF fornisce immediatamente una definizione dell'attività di internal auditing, tale da rappresentare in maniera sintetica il contenuto e le peculiarità dell'attività, nonché di contestualizzarla nell'ambito del più ampio sistema dei controlli aziendali. La definizione di internal auditing è la seguente:

*“Internal auditing is an independent, objective assurance and consulting activity to add value and improve an organization’s operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance process”.*<sup>31</sup>

Tradotto, la funzione di Internal Audit rappresenta:

“... l'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”.

Nonostante la definizione possa a primo impatto apparire breve e concisa, essa è composta da numerosi elementi essenziali e che si ritiene opportuno approfondire per una completa comprensione della materia oggetto di analisi. Segue un focus sugli elementi più rilevanti:

- a) In primo luogo, l'attività di internal auditing è un'attività indipendente. L'indipendenza va in questo caso intesa come<sup>32</sup> “la concreta possibilità, per l'internal auditor, di esercitare la propria attività scevro da qualsiasi interferenza e nel pieno adempimento delle proprie responsabilità”. L'indipendenza è garantita principalmente attraverso il posizionamento organizzativo del responsabile dell'attività di internal auditing e attraverso la fattispecie per cui gli internal auditor non possono occuparsi di attività di altra

---

<sup>31</sup> INSTITUTE OF INTERNAL AUDITORS (IIA), *International Professional Practices Framework (IPPF): Definition*, 1999.

<sup>32</sup> DITTMER C., *Internal Auditing: chiave per la corporate governance*, EGEA, 2011, pag. 4; Sull'argomento, vedi lo Standard IIA 1100, *Indipendenza e Obiettività*.

natura o intrattenere specifiche relazioni con alcune strutture aziendali. Infine, l'ipotesi di *outsourcing* dell'attività sembra garantire maggiore indipendenza della funzione, tuttavia essa è concreta solo qualora il revisore esterno non sia coinvolto in attività di consulenza verso strutture organizzative soggette a giudizio di *assurance*.

- b) Oltre all'indipendenza, l'attività di internal auditing deve garantire i principi di obiettività, legati essenzialmente alla sfera soggettiva dell'internal auditor. In particolare, affinché l'attività sia svolta in maniera obbiettiva, è richiesto un atteggiamento di totale imparzialità del revisore interno rispetto all'oggetto di controllo, che si traduce altresì nell'evitare il sorgere di conflitti di interesse che possano compromettere l'autonomia e la libertà mentale dell'auditor. In poche parole, il giudizio professionale dell'internal auditor non deve subire pressioni dai giudizi altrui.
- c) L'internal auditing è un'attività di assurance e consulenza. Essa è un'attività di assurance in quanto l'output dell'intero processo di revisione interna è l'emanazione di un giudizio indipendente di assurance, cioè una conferma circa la presenza degli elementi necessari ai fini dell'efficacia e dell'efficienza dei processi di gestione dei rischi e di controllo interno. In un'accezione più ampia, i servizi di assurance comprendono "tutte quelle attività che possono migliorare la qualità delle decisioni, procurando nuove informazioni, oppure rendendo più tempestive quelle già disponibili, oppure ancora assicurandone l'affidabilità o la rilevanza"<sup>33</sup>. Nei servizi di assurance, infine, sono generalmente coinvolte tre parti: il *process owner*, cioè la persona o il gruppo di persone che presiedono l'attività o processo sottoposto a giudizio; l'internal auditor, ossia colui che svolge l'attività di internal auditing; l'*user*, cioè la persona o l'insieme di persone che utilizzeranno tale informazione. I servizi di consulenza in materia di internal audit invece comprendono delle attività di supporto diverse dall'assurance, cioè non finalizzate all'emanazione di un giudizio finale. In questo caso le parti concordano totalmente sull'oggetto dell'attività di consulenza e non sono previsti particolari vincoli per l'auditor, salvo il mantenimento dei requisiti di obiettività e indipendenza. I soggetti

---

<sup>33</sup> GROSSI C. G., *Internal Auditing: l'inizio di una nuova avventura*, Milano, AIIA, 2002.

coinvolti sono esclusivamente il cliente, cioè la persona o il gruppo di persone che richiedono il servizio, e l'internal auditor che lo svolge.

- d) Il fine ultimo dell'attività di internal auditing, come più volte accennato, è il miglioramento dell'efficacia e dell'efficienza dell'organizzazione. L'efficacia va intesa come la capacità dell'organizzazione di realizzare i propri obiettivi. In tema di controlli aziendali, l'efficacia dell'organizzazione richiede l'estensione massima dei controlli e il più elevato grado di presidio del rischio. L'efficienza, invece, è definita come il rapporto tra il grado di raggiungimento degli obiettivi e le risorse impiegate e, se contestualizzata, rappresenta un concetto di ottimizzazione del controllo, che passa necessariamente attraverso un'analisi costi – benefici del controllo.
- e) Gli obiettivi aziendali dovranno essere raggiunti mediante un approccio professionale sistematico, che comprende l'insieme di conoscenze, capacità e competenze attraverso cui l'internal auditor svolge la propria attività professionale. In particolare, un internal auditor deve possedere, oltre alle competenze professionali di base, delle capacità relazionali e di comunicazione. Inoltre, gli standard professionali richiedono un continuo aggiornamento professionale, mediante il quale l'internal auditor è in grado di mantenere elevato lo standard di professionalità richiesto dalla natura dell'incarico.
- f) Inoltre, l'attività di internal auditing deve poter contribuire a determinare un valore aggiunto per l'organizzazione. La creazione di tale maggior valore si misura mediante l'analisi dei rischi dell'impresa e del sistema di controllo interno che è in grado di soddisfare le esigenze degli organi direzionali di realizzazione degli obiettivi prefissati. Fondamentale ai fini della creazione di valore per l'impresa sono le azioni di miglioramento che l'internal auditor suggerisce ai responsabili delle unità organizzative di impresa a seguito dell'esecuzione dell'audit.
- g) L'internal auditing definisce poi gli ambiti di intervento derivanti dallo svolgimento dell'attività e questi sono:
- La corporate governance;
  - I processi di gestione dei rischi;

- I processi di controllo.

Di questi elementi si tratterà in dettaglio durante l'analisi della natura dell'attività di internal auditing, contenuta nel paragrafo successivo.

- h) Per concludere l'analisi delle componenti della definizione di internal auditing, bisogna necessariamente affrontare il tema della natura della revisione interna. Essa, infatti, viene volutamente definita come una attività e non come una funzione. Questo dettaglio deriva principalmente dal fatto che l'internal auditing può essere svolto in *outsourcing* e quindi può non rientrare all'interno del novero delle funzioni o organi aziendali.

Il secondo elemento delle *Guidance* vincolanti è rappresentato dai Principi Fondamentali per la professione di internal auditing. Si tratta di dieci principi cardine il cui obiettivo è quello di realizzare un efficace internal auditing mediante il loro perseguimento. Infatti, una funzione di Internal Audit si considera efficace solamente in presenza di questi dieci principi. Essi sono:

1. Agire con manifesta integrità;
2. Dimostrare competenza e diligenza professionale;
3. Mantenere obiettività e indipendenza di giudizio;
4. Operare in coerenza con le strategie, gli obiettivi e i rischi dell'organizzazione;
5. Avere un appropriato posizionamento organizzativo e risorse adeguate al ruolo;
6. Dimostrare elevati standard qualitativi ed essere orientati al miglioramento continuo;
7. Comunicare con efficacia;
8. Fornire una risk – based assurance;
9. Operare con un approccio propositivo, proattivo e lungimirante;
10. Favorire il miglioramento dell'organizzazione.

Questi principi si intrecciano tra di loro al fine di fornire gli elementi fondamentali della Professione in una visione olistica. Ad esempio, non può esserci indipendenza di giudizio (3) senza avere un appropriato posizionamento organizzativo e risorse adeguate al ruolo (5), ovvero non può ottenersi un miglioramento dell'organizzazione

(10) senza operare con un approccio propositivo, proattivo e lungimirante (9), in quanto il miglioramento dell'organizzazione e la creazione di valore aggiunto passa necessariamente attraverso un'analisi di medio – lungo termine. Naturalmente, l'analisi su cui si basa un processo di internal auditing è fondata sul rischio (8), nell'ottica dell'ottenimento di obiettivi di rischio in linea con il perseguimento degli obiettivi e delle strategie dell'azienda. Infine, altro elemento fondamentale è la comunicazione (7): solamente avviando una concreta e costante comunicazione con i diversi organi aziendali l'internal auditor è in grado di realizzare una corretta mappatura delle principali aree di rischio ovvero di saper comunicare le azioni necessarie che il management dovrebbe porre in essere per ridurre il rischio complessivo ai livelli di accettabilità inizialmente concordati.

Il terzo elemento delle linee guida vincolanti è rappresentato dal Codice Etico della Professione. Il Codice contiene un insieme di principi ritenuti essenziali affinché la condotta dell'internal auditor sia allineata a standard di eticità. Lo scopo è quindi quello di promuovere la cultura etica nell'esercizio della professione di internal auditing ed è fondamentale che tutti gli internal auditor ne siano conformi al fine di mantenere alto il livello di credibilità della professione, fattore ritenuto essenziale affinché i portatori di interesse, a cui è rivolta l'attività di assurance, possano riporre fiducia nel giudizio finale emesso. Il Codice Etico include due componenti essenziali:

- a) I Principi, fondamentali per la professione e la pratica dell'internal auditing;
- b) Le Regole di Condotta, che descrivono le norme comportamentali che gli internal auditor sono tenuti ad osservare. Le Regole fungono da driver per l'applicazione dei principi e forniscono una guida di comportamento professionale per gli internal auditor.

Sono di seguito elencati i Principi e le Regole di Condotta contenute nell'IPPF<sup>34</sup>. I Principi sono i seguenti:

---

<sup>34</sup> INSTITUTE OF INTERNAL AUDITORS (IIA), *International Professional Practices Framework (IPPF): Principles & Rules of Conduct*, 1999.

- 1) Integrità: l'integrità dell'internal auditor permette l'instaurazione di un rapporto fiduciario ed è quindi elemento cruciale per mantenere un elevato livello di affidabilità del giudizio finale.
- 2) Obbiettività: nel raccogliere, valutare e comunicare le informazioni attinenti all'attività o al processo in esame, l'internal auditor deve manifestare il massimo livello di obbiettività professionale. L'obbiettività si ottiene principalmente attraverso l'assenza di influenze altrui nello svolgimento della propria Professione e nell'emanazione del giudizio.
- 3) Riservatezza: con riguardo alle informazioni di cui l'internal auditor entra in possesso nello svolgimento del suo incarico. Vista la sensibilità delle informazioni trattate durante lo svolgimento dell'audit si richiede la riservatezza e la mancata divulgazione impropria di esse, a meno che non lo impongano motivi di ordine legale o deontologico.
- 4) Competenza: nello svolgimento dell'incarico, l'internal auditor deve utilizzare tutte le competenze, le conoscenze e le esperienze di cui è in possesso e che possono contribuire positivamente nell'emanazione di un giudizio più veritiero e corretto possibile.

Per ciascuno dei Principi appena menzionati sono state poi predisposte delle norme comportamentali che gli internal auditor sono tenuti ad osservare. Le Regole di Condotta sono:

1. Integrità: l'internal auditor:
  - 1.1. Deve operare con onestà, diligenza e senso di responsabilità;
  - 1.2. Deve rispettare la legge e divulgare all'esterno solo se richiesto dalla legge e dai principi della professione;
  - 1.3. Non deve essere consapevolmente coinvolto in nessuna attività illegale, né intraprendere azioni che possano indurre discredito per la professione o per l'organizzazione per cui opera;
  - 1.4. Deve rispettare e favorire il conseguimento degli obiettivi dell'organizzazione per cui opera, quando etici e legittimi.
2. Obbiettività: l'internal auditor:

- 2.1. Non deve partecipare ad alcuna attività o avere relazioni che pregiudichino o appaiano pregiudicare l'imparzialità della sua valutazione;
  - 2.2. Non deve accettare nulla che pregiudichi o appaia pregiudicare l'imparzialità della sua valutazione;
  - 2.3. Deve riferire tutti i fatti significativi a lui noti, la cui omissione possa fornire un quadro alterato delle attività analizzate.
3. Riservatezza: l'internal auditor:
- 3.1. Deve acquisire la dovuta cautela nell'uso e nella protezione delle informazioni acquisite nel corso dell'incarico;
  - 3.2. Non deve usare le informazioni ottenute né per vantaggio personale, né secondo modalità che siano contrarie alla legge o di nocimento agli obiettivi etici e legittimi dell'organizzazione.
4. Competenza: l'internal auditor:
- 4.1. Deve effettuare solo prestazioni per le quali abbia la necessaria conoscenza, competenza ed esperienza;
  - 4.2. Deve prestare i propri servizi in pieno accordo con gli Standard Internazionali per la Pratica Professionale dell'Internal Audit;
  - 4.3. Deve continuamente migliorare la propria preparazione professionale nonché l'efficacia e la qualità dei propri servizi.

Tra le linee guida che vincolano l'operato dell'internal auditor va fatta infine menzione agli Standard Internazionali per la Pratica Professionale dell'Internal Audit. Scopo degli Standard è quello di "delineare i principi base che prescrivono come l'attività di internal auditing debba essere svolta, fornendo un quadro di riferimento per lo sviluppo delle attività di audit"<sup>35</sup>. Attraverso questi standard è stato possibile creare un Framework uniforme per lo svolgimento dell'attività di internal auditing, altrimenti lasciata alla discrezione dei singoli ordini professionali nazionali e delle singole legislazioni. Inoltre, gli IPPF prevedono esplicitamente l'obbligatorietà della loro applicazione, qualora non siano in contrasto con le normative nazionali. In ogni caso, la mancata applicazione di un principio che sia giustificata da contrasti con la normativa vigente non nega l'adozione dei restanti principi: in questo caso l'auditor

---

<sup>35</sup> DITTMER C., *Internal Auditing: chiave per la corporate governance*, EGEA, 2011, pag. 19.

dovrà spiegare perché non si è rispettato un particolare Standard ed adottare ugualmente i restanti. È interessante notare come fino al 2009 tali standard, in riferimento alle azioni che l'auditor doveva porre in essere, utilizzavano il verbo "should" (dovrebbe/dovrebbero), evidenziando la natura facoltativa degli Standard internazionali. Attualmente, invece, le recenti modifiche hanno introdotto un sostanziale cambiamento da questo punto di vista mediante l'introduzione del verbo "must" con il quale tali Standard hanno iniziato ad assumere un carattere di obbligatorietà.

Gli Standard comprendono due categorie principali, ed una terza categoria "accessoria". In particolare, essi si dividono in:

- *Standard di connotazione*: precisano le caratteristiche che le organizzazioni e gli individui che effettuano attività di internal auditing devono possedere obbligatoriamente;
- *Standard di prestazione*: definiscono la natura dell'attività di internal auditing e forniscono criteri qualitativi attraverso cui è possibile valutarne la prestazione;
- *Standard applicativi*: servono a personalizzare la applicazione degli standard appartenenti alle prime due categorie. In particolare, si fa riferimento alla distinzione tra gli aspetti di assurance e di consulenza e sono indicati attraverso una lettera che segue il numero dello standard: A per le attività di assurance e C per le attività di consulenza.

Gli Standard di connotazione si articolano in quattro macro-aree e descrivono i "connotati" che deve possedere colui che svolge attività di internal auditing. Le macro-aree sono le seguenti:

1. Finalità, autorità e responsabilità;
2. Indipendenza e obiettività;
3. Competenza e diligenza professionale;
4. Programma di assurance e miglioramento qualità.

Ciascuna di queste macro-aree contiene un diverso numero di standard fino ad arrivare, complessivamente, ad un numero totale di 33 standard di connotazione, più i relativi standard applicativi.

Con riguardo agli Standard di prestazione, invece, va detto che questi si concentrano soprattutto sugli aspetti che riguardano la natura dell'attività svolta dall'internal auditor nonché i criteri attraverso cui è possibile effettuarne una valutazione complessiva. Come visto per gli standard di connotazione, anche questa categoria è suddivisibile in diverse macro-aree, che sono le seguenti:

1. Gestione dell'attività di internal auditing;
2. Natura dell'attività;
3. Pianificazione dell'incarico;
4. Svolgimento dell'incarico;
5. Comunicazione dei risultati;
6. Monitoraggio delle azioni correttive;
7. Risoluzione di contrasti in merito all'accettazione del rischio da parte del senior management.

La categoria in questione arriva a contare un totale di 31 standard di prestazione e oltre quaranta standard applicativi riguardanti i servizi di assurance e consulenza.

Nel paragrafo successivo verrà trattato a fondo il tema della natura della funzione di Internal Audit, analizzando fedelmente quanto contenuto all'interno dello Standard di connotazione numero 2100. Per la trattazione dei rimanenti standard, invece, si fa rinvio al *paragrafo 7* del presente capitolo.

## **1.5. La natura della Funzione Internal Audit**

In questo paragrafo verrà affrontato lo Standard di prestazione n. 2100 e i seguenti 2110, 2120, 2130, contenenti la natura dell'attività di internal auditing. La scelta di affrontare questo Standard separatamente dai rimanenti è motivata dal fatto che

attraverso una sua piena comprensione è possibile contribuire ad avere una idea più precisa dell'attività di internal auditing, oggetto di trattazione di questo testo. Infatti, esso mira a spiegare i compiti e i principali obiettivi che la funzione Internal Audit intende perseguire nello svolgimento del proprio incarico, con particolare riguardo al suo contributo nel miglioramento dei processi di risk management, di controllo e di corporate governance.

In merito alla natura dell'attività di internal auditing, il *revised Standard 2100 – Nature of Work* esprime le seguenti considerazioni<sup>36</sup>:

*“The internal audit activity must evaluate and contribute to the improvement of the organization’s governance, risk management, and control processes using a systematic, disciplined, and risk-based approach. Internal audit credibility and value are enhanced when auditors are proactive, and their evaluations offer new insights and consider future impact”.*

“L'attività di internal audit deve valutare e contribuire al miglioramento dei processi di governance, gestione del rischio e controllo dell'organizzazione, tramite un approccio sistematico, rigoroso e risk – based. La credibilità e il valore dell'internal auditing sono rafforzati quando gli auditor agiscono in maniera proattiva e le loro valutazioni offrono nuove riflessioni e tengono in considerazione gli impatti futuri”.

In primo luogo, l'attività di internal auditing deve contribuire al miglioramento dei processi di governance. Quest'ultima può essere definita come il sistema di principi, procedure e metodi attraverso i quali un'organizzazione garantisce:

- a) La creazione di valore per la società civile e per gli stakeholder;
- b) Il rispetto delle regole, dei principi etici e delle aspettative;
- c) La conformità alle leggi e ai regolamenti;
- d) La completezza e la veridicità dei bilanci.

---

<sup>36</sup> INSTITUTE OF INTERNAL AUDITORS (IIA), *International Professional Practices Framework (IPPF): Standard 2100, Revised Standards*, 2017.

In tale contesto, l'Internal Audit deve “valutare e fornire appropriati suggerimenti volti a migliorare il processo di governance dell'organizzazione”<sup>37</sup>. Il processo di governance assume un ruolo specifico all'interno dello standard 2110 e fa riferimento principalmente a:

- La presa di decisioni di natura strategica e operativa;
- La supervisione dei processi di gestione e controllo dei rischi;
- La promozione di adeguati valori e principi etici nell'organizzazione;
- L'efficace gestione dell'organizzazione e l'*accountability*;
- La corretta comunicazione delle informazioni sui rischi e sui controlli nei confronti di tutti i dipendenti aziendali;
- La coordinazione delle attività e il processo di scambio dei flussi informativi tra i diversi organi aziendali (consiglio di amministrazione, revisore esterno, internal auditor, ecc.).

In sintesi, attraverso l'attività di internal auditing si ottiene un'assurance sulla correttezza della predisposizione e del funzionamento dei diversi meccanismi di corporate governance dell'organizzazione, in modo da avere una fondamentale garanzia sulla veridicità dei bilanci e dell'informativa finanziaria della società.

Un secondo aspetto che bisogna considerare con riferimento alla natura dell'attività dell'Internal Audit è quello relativo alla gestione dei rischi aziendali e quindi ai processi di risk management. In particolare, l'attività di internal auditing deve “valutare l'efficacia e contribuire al miglioramento dei processi di gestione del rischio”<sup>38</sup>. Al fine di verificare l'efficacia dei processi di risk management l'internal auditor deve:

- 1) Valutare che gli obiettivi aziendali siano coerenti con la mission dell'organizzazione;
- 2) Valutare che i rischi significativi siano stati identificati e valutati;

---

<sup>37</sup> INSTITUTE OF INTERNAL AUDITORS (IIA), *International Professional Practices Framework (IPPF): Standard 2110*, Revised Standards, 2017.

<sup>38</sup> INSTITUTE OF INTERNAL AUDITORS (IIA), *International Professional Practices Framework (IPPF): Standard 2120*, Revised Standards, 2017.

- 3) Valutare le azioni di risposta ai rischi affinché questi vengano ricondotti entro i limiti di accettabilità stabiliti dal governo aziendale;
- 4) Valutare che ci sia stata una corretta diffusione delle informazioni concernenti i rischi aziendali in tutta l'organizzazione.

L'internal auditor dovrà raccogliere informazioni inerenti i suindicati aspetti durante lo svolgimento di molteplici incarichi e dovrà valutare l'efficacia del processo di gestione dei rischi in termini di:

- Raggiungimento degli obiettivi strategici dell'organizzazione;
- Affidabilità e integrità delle informazioni contabili, finanziarie e operative;
- Efficacia ed efficienza delle operazioni e dei programmi;
- Salvaguardia del patrimonio;
- Conformità a leggi, regolamenti, politiche, procedure e contratti.

Per formulare un'opinione sull'adeguatezza dei processi di risk management, l'Internal Audit si basa sulla valutazione di cinque obiettivi che l'attività di gestione dei rischi deve conseguire. Essi sono:

1. Identificazione dei rischi e delle priorità;
2. Determinazione dei rischi accettabili;
3. Progettazione e attuazione di strategie per contenere, gestire, condividere ed evitare i rischi;
4. Monitoraggio dei rischi identificati e sull'esito delle azioni di risposta intraprese;
5. Comunicazione, mediante relazioni periodiche al management, al board e agli stakeholder, dei principali rischi riscontrati e dell'esito del processo di gestione dei rischi attuato.

Inoltre, lo standard fa particolare riferimento alla gestione dei casi in cui l'internal auditor presta altresì servizi di consulenza nei confronti dell'impresa auditata. In questi casi, l'internal auditor dovrà valutare i rischi attinenti agli obiettivi dell'incarico e dovrà utilizzare le informazioni concernenti i rischi di cui sia venuto a conoscenza durante lo svolgimento dell'incarico di consulenza. In ogni caso, gli internal auditor

devono evitare di assumere responsabilità manageriali tramite una gestione diretta dei rischi. Infine, nello svolgimento del proprio incarico l'internal auditor deve attribuire un certo peso alla valutazione dei rischi di frode e alle modalità attraverso cui l'organizzazione gestisce tale categoria di rischio.

Nonostante la funzione dell'Internal Audit rappresenti un controllo di terzo livello, e quindi abbia il dovere di "controllare" l'operato delle funzioni di controllo di secondo livello, tra cui il risk management, non di rado può accadere che in assenza di quest'ultimo l'Internal Audit svolga mansioni diverse da quelle di competenza. In particolare, viene richiesto che l'attività di internal auditing assuma un ruolo propositivo nell'avvio di un processo di risk management qualora questo non sia presente in azienda o non sia correttamente predisposto. Tuttavia, il ruolo di internal auditor può essere solamente proattivo e non di assunzione diretta delle responsabilità in materia di gestione dei rischi.

Il terzo ed ultimo aspetto su cui si basa l'attività di internal auditing ha ad oggetto il controllo aziendale. L'attività di internal auditing, infatti, "deve assistere l'organizzazione nel mantenere controlli efficaci attraverso la valutazione della loro efficacia ed efficienza e promuovendo il miglioramento continuo"<sup>39</sup>. Anche in materia di controllo, l'attività che deve essere eseguita dovrà fornire un'assurance obbiettiva circa il raggiungimento degli obiettivi strategici, l'affidabilità delle informazioni, l'efficacia e l'efficienza dei processi, la salvaguardia del patrimonio e la compliance.

## **1.6. Il processo di audit**

L'esercizio dell'attività di internal auditing segue un approccio metodologico tipicamente basato sul project management, il cui output è quello di fornire, come ripetuto più volte in precedenza, un giudizio di assurance sulla qualità della corporate governance, del risk management e dei controlli societari. Nonostante la letteratura in materia e le fonti autoregolamentari sembrano prediligere uno specifico modello nella

---

<sup>39</sup> INSTITUTE OF INTERNAL AUDITORS (IIA), *International Professional Practices Framework (IPPF): Standard 2130, Revised Standards*, 2017.

conduzione di tale attività, occorre ricordare la non vincolatività degli standard internazionali e quindi la discrezionalità che è lasciata agli internal auditor, che potranno mettere in atto la loro professionalità ed esperienza per decidere, di volta in volta, le modalità di svolgimento dell'attività. Tuttavia, ai fini del presente lavoro, si ritiene opportuno fornire un impianto metodologico più vicino possibile a quello comunemente adottato, ricordando l'importanza di un approccio *risk – based*.

Per finalità espositive, è ragionevole scomporre l'intero processo di internal auditing in quattro fasi principali:

1. Pianificazione;
2. Esecuzione;
3. Reporting;
4. Follow-up.



Figura 9 - Il processo di Internal Audit

Durante la fase di pianificazione gli internal auditor raccolgono le informazioni generali e definiscono l'*Audit Universe*, cioè l'insieme degli elementi che possono essere o saranno oggetto di audit. Successivamente, con l'aumentare del livello di dettaglio e di conoscenza dei rischi insiti nelle varie aree, si passerà a considerare esclusivamente gli oggetti maggiormente a rischio, che verranno sottoposti ad un *risk assessment*. Infine, verrà creato un piano di audit. Nella fase successiva, invece, viene disposto un piano di lavoro e verranno eseguiti i primi controlli determinati in sede di

definizione del piano di audit, attraverso i quali si otterranno le principali informazioni per l'emanazione del giudizio. La terza fase è rappresentata dalla stesura di un Report di audit e dalla comunicazione dei risultati ottenuti al management aziendale, attraverso cui il responsabile della funzione di Internal Audit suggerisce le azioni correttive da porre in essere. Infine, si ritiene necessaria una fase conclusiva e continuativa di follow-up, necessaria ad accertare il rispetto e la messa in atto del piano di azione concordato con il management e a monitorare il livello di rischio complessivo dell'impresa auditata. Di seguito verranno trattate in maniera più dettagliata le quattro fasi appena menzionate.

### **1.6.1. Pianificazione**

La fase di pianificazione dell'intervento di internal auditing assume un'importanza fondamentale in quanto essa è funzionale alla profonda conoscenza del business che si va ad analizzare e dei principali rischi insiti nell'attività, quindi di fondamentale importanza per un efficace intervento di audit.

L'intervento di audit ha inizio con la comunicazione ai responsabili delle varie aree aziendali dell'avvio dell'attività, che avviene attraverso una "lettera di notifica". La comunicazione, in questo caso, assume un elevato valore in quanto permette ai dipendenti aziendali di prepararsi ad accogliere l'intervento di audit e quindi di favorire un atteggiamento quanto più possibile collaborativo tra gli auditor e gli auditati. Ovviamente, occorre notare che non sempre si ritiene necessario ed opportuno l'invio di una lettera di notifica. Ad esempio, nel caso di un fraud investigation auditing è preferibile sfruttare "l'effetto sorpresa", venendo meno l'annuncio relativo all'inizio dell'attività che si va ad eseguire.

Con la lettera di notifica, il responsabile dell'internal auditing comunica i seguenti aspetti:

- Gli obiettivi e l'ambito di copertura dell'audit;
- I contenuti generali previsti dall'intervento;

- La data di inizio attività e i tempi stimati per il suo completamento;
- L'indicazione del responsabile dell'internal audit;
- L'indicazione delle procedure che verranno adottate.

La comunicazione dell'intervento prosegue in un *kick-off meeting*, o riunione di apertura, durante la quale si illustrano al personale responsabile delle aree oggetto di audit le metodologie e i processi che verranno adottati durante l'intervento. Questa riunione, fondata su principi di condivisione e di scambio informativo, è essenziale per gli auditor ai fini dell'ottenimento delle prime considerazioni sulle aree maggiormente a rischio e sul livello dei presidi preesistenti all'interno di queste. Inoltre, attraverso la condivisione con il management dell'ente oggetto di audit della mission, degli obiettivi e delle modalità dell'intervento, si creano i presupposti per una maggiore collaborazione anche in sede di definizione ed attuazione degli interventi correttivi che l'internal auditor suggerisce al termine dell'attività.

Al termine della riunione, l'Internal Audit avvia definitivamente la propria attività mediante una ricerca di informazioni generali sull'*entity*, il cui obiettivo è quello di definire le principali *auditables units*, ossia le aree maggiormente a rischio e sulle quali si ritiene necessaria l'esecuzione dei test. Le informazioni maggiormente ricercate in questa fase sono:

- Organigramma;
- Piani strategici e obiettivi di breve e di medio-lungo termine;
- Budget e documentazione economico-finanziaria;
- Carte di lavoro relative a precedenti incarichi;
- Risultati di altre attività di controllo effettuate (revisione esterna, risk management, ecc.);
- Altre informazioni.

Oltre alle richieste documentali, l'attività di auditing generalmente prevede altri strumenti per la raccolta di informazioni come:

- *Walkthrough*: si tratta di un espediente molto utilizzato che consiste nell'osservazione diretta del funzionamento delle varie fasi dei processi;

- Interviste: nei confronti del personale aziendale, a cui vengono sottoposte domande circa lo svolgimento dell'attività. Molto spesso sono sostituite da questionari;
- Analisi dei *flowchart*: mediante i quali si analizzano i processi operativi e di controllo.

A conclusione dell'analisi preliminare appena descritta, viene redatto un planning memorandum, che consiste in una bozza del piano di audit e che contiene elementi fondanti su cui si baserà l'intervento vero e proprio.

Una volta definito l'Audit Universe bisognerà definire quali, tra gli oggetti di audit identificati, dovranno essere sottoposti a una verifica successiva. In tale circostanza, la prassi operativa prevede l'esecuzione di un processo di risk assessment, cioè un processo sistematico per l'identificazione e la valutazione degli eventi che potrebbero influenzare il raggiungimento degli obiettivi aziendali. Rimandando alla lettura dei paragrafi precedenti circa le definizioni di rischio aziendale e di risk management, occorre aggiungere che le modalità di valutazione del rischio possono avvenire in vario modo: ad esempio, attraverso analisi statistiche, valutazioni qualitative, auto-valutazioni, dati storici. Tuttavia, si sostiene sia imprescindibile l'aspetto della *measurement*, dove il rischio inerente si qualifica come un prodotto tra la probabilità di accadimento dell'evento e l'impatto che l'evento stesso possa avere sulle performance finanziarie e reputazionali dell'impresa. Inoltre, il rischio inerente così calcolato non può essere indicativo delle aree sottoposte a maggiore rischio in quanto bisogna tener conto dei controlli già posti in essere dal management aziendale. Per questo motivo, dall'incrocio tra queste variabili si vengono a definire i seguenti scenari:

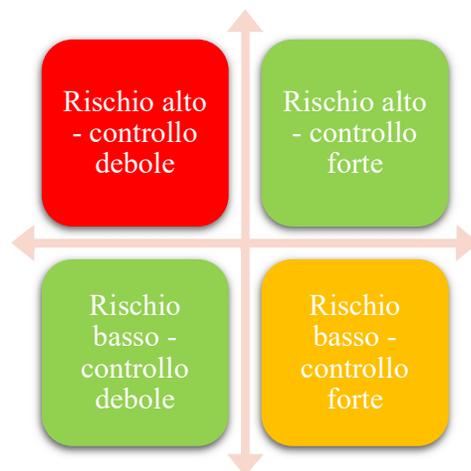


Figura 10 - Matrice rischio-controllo

- a) Rischio inerente basso – controllo aziendale debole: dato il basso di livello di rischio relativo all’area considerata, salvo particolari richieste del management, si ritiene inopportuna l’esecuzione dei test e l’impiego di risorse;
- b) Rischio inerente alto – controllo aziendale debole: in questa particolare casistica l’intervento di audit è essenziale alla misurazione del livello di rischio residuo (rischio inerente al netto dei controlli aziendali) e alla sua comparazione con il *risk appetite* fornito dal CdA in sede di pianificazione strategica. Nel caso in cui le evidenze dimostrino l’esistenza di un rischio troppo elevato, il responsabile di internal audit dovrà suggerire al management delle azioni correttive da porre in essere e l’implementazione di nuovi controlli;
- c) Rischio inerente alto – controllo aziendale forte: in questo caso, l’Internal Audit assume piuttosto una forma di conferma di quanto già disposto dal management interno;
- d) Rischio inerente basso – controllo aziendale forte: l’unica considerazione che può essere effettuata in tal caso è che la sovra-abbondanza di controlli in un’area non soggetta a rischi particolarmente elevati potrebbe significare un inefficiente impiego di risorse all’interno dell’organizzazione, che si traduce in altrettanta inefficienza da un punto di vista del sistema di controllo interno e di corporate governance.

L'attività fin qui esposta si conclude con la predisposizione di un Audit Program, un documento approvato dal responsabile dell'internal auditing che stabilisce le attività di analisi e verifica, le metodologie o le tecniche per lo svolgimento del lavoro, coordina i membri del team di audit fornendo delle specifiche indicazioni operative.

### **1.6.2. Esecuzione dei test**

Una volta effettuato un *mapping* per la definizione dei principali eventi di rischio inerenti al business ed identificati, all'interno del *risk universe*, quelli che hanno un maggiore impatto sull'organizzazione, si procede con l'*execution* dei test. Durante questa fase si procede con un'analisi dettagliata dei processi aziendali e alla mera esecuzione dei test, con le quali è possibile avere un'idea chiara sull'architettura del sistema di controllo interno oltre che ottenere le necessarie informazioni ed evidenze per la formulazione di un giudizio. Entrando nello specifico, vengono poste in essere le seguenti attività di verifica<sup>40</sup>:

- Verifica di coerenza tra quanto rilevato nelle analisi iniziali di processo e quanto avviene effettivamente nella normale operatività aziendale;
- Verifica del rispetto delle procedure;
- Analisi dei dati ed indicatori;
- Ricerca di "eccezioni" all'interno di banche dati;
- Ogni altra attività che sia in grado di generare evidenze per la formulazione del giudizio finale.

Attraverso tali test, l'internal auditor raccoglie le informazioni necessarie alla comunicazione dei rilievi riscontrati nonché per il suggerimento di raccomandazioni. Per la loro rilevanza, le evidenze di audit devono possedere le seguenti caratteristiche:

- 1) Sufficienza: devono essere raccolte un numero adeguato di informazioni per poter arrivare a sostenere delle conclusioni circa la presenza di rilievi o elementi fondanti per la costituzione di un giudizio;

---

<sup>40</sup> DITMEIER C., *Internal Auditing: chiave per la corporate governance*, EGEA, 2011, pag. 331.

- 2) Affidabilità: le informazioni ottenute devono essere affidabili, cioè verificabili e tracciabili. In mancanza di tale elemento il giudizio perde ogni valore;
- 3) Rilevanti e utili al conseguimento degli obiettivi di audit: non tutte le informazioni ottenute debbono essere tenute in considerazione durante un incarico di audit, ma solamente quelle che possono avere un impatto rilevante sul giudizio finale.

Inoltre, è richiesto che le prove raccolte siano adeguate, concrete e convincenti, tali da consentire a qualunque auditor informato di giungere alle medesime conclusioni. Infine, per avere un quadro generale della natura delle evidenze fin qui descritte, è sufficiente accennare che possono essere di diversa natura e genere. In funzione della natura potremmo quindi avere: evidenze fisiche, documentali, testimoniali o analitiche. In funzione del modo in cui si origina l'evidenza si classificano in evidenze interne ed esterne, ma anche evidenze interne-esterne, cioè generate all'interno ma poi rielaborate da un soggetto esterno, o viceversa. In merito alle modalità di raccolta, invece, va accennato che l'ottenimento delle informazioni avviene attraverso: interviste, test di dettaglio, osservazione e ispezione, scansione, campionamento statistico e richieste di conferma<sup>41</sup>.

Una volta accennato allo scopo della fase di esecuzione dei test, al significato della raccolta documentale e alle principali modalità attraverso cui le evidenze vengono ottenute, occorre effettuale una distinzione fondamentale tra le diverse categorie di execution. In particolare, in base alla tipologia di rischio che sottende ciascuna area che si va ad osservare, l'esecuzione dei test si distingue in:

- a) *Operational Audit*;
- b) *Financial Audit*;
- c) *Compliance Audit*;
- d) *Fraud Audit*.

In primo luogo, occorre chiarire che una tale suddivisione degli interventi di auditing è effettuata secondo un approccio non dipartimentale o verticale, bensì trasversale alle

---

<sup>41</sup> GLEIM I.N., CIA Review, Gleim Publications, 2004.

varie funzioni ed aree aziendali, scegliendo come driver il rischio che si va a monitorare.

Con riguardo alla prima tipologia di audit, essa è volta a valutare l'efficacia e l'efficienza dei processi di risk management e di controllo interno posti in essere per la gestione dei principali rischi aziendali. Essa costituisce, inoltre, la principale fonte di informazioni sul buon funzionamento di un sistema di controllo interno e, soprattutto, l'analisi da cui spesso scaturiscono le raccomandazioni che l'auditor impartisce al management circa la riorganizzazione del sistema. In sintesi, attraverso l'operational auditing si intende osservare la presenza di un dato livello di economicità nella gestione dei processi aziendali di controllo, intesa sia come grado di raggiungimento degli obiettivi, sia come efficienza nella gestione delle risorse. In concreto l'attività di operational auditing si basa su un primo studio del processo aziendale, attraverso cui è possibile definire gli obiettivi del processo e i rischi che possono comprometterne il raggiungimento, con particolare riguardo agli attori coinvolti nel processo. Successivamente, una volta ottenuta un'analisi dettagliata del processo, l'internal auditor procede con una misurazione dei fenomeni di rischio individuati. Ad esempio, l'operational auditing nell'ambito del processo di acquisto mira a valutare le seguenti attività: valutazione del fornitore, selezione del fornitore, definizione del fabbisogno, emissione dell'ordine di acquisto, ricevimento del bene o del servizio e fatturazione.

La seconda tipologia di audit è rappresentata dal financial audit. Questa particolare categoria, si chiarisce, nonostante il nome suggerisce dei punti di raccordo con l'audit esterno sui *financial statements*, si discosta da esso mantenendo il carattere di internal audit e quindi di analisi e valutazione dei processi. Espresso in altri termini, l'aspetto financial dell'internal audit può essere definito come un audit volto ad accertare il Sistema di Controllo Interno su processi prettamente amministrativo-contabili o che hanno ad oggetto l'analisi di poste di bilancio identificate sulle quali il management vuole avere un'assurance interna. Tuttavia, resta ferma la necessità di una stretta collaborazione tra revisione esterna ed interna ai fini della verifica di determinate voci di bilancio, ad esempio durante le attività di circolarizzazione e di verifica fisica

dell'esistenza dei beni<sup>42</sup>. Inoltre, va detto che l'esecuzione di un esemplare financial auditing interno è in grado di fornire una primaria assurance sul corretto funzionamento dei processi amministrativo-contabili, utili a ridurre il rischio di errori di bilancio e quindi migliorare la qualità e l'efficienza dell'attività del revisore esterno contabile. Inoltre, non mancano studi che analizzano i rapporti tra le due funzioni e l'impatto che un efficace ed efficiente internal audit può avere sulla revisione esterna del bilancio, sia in termini di maggiore *reliance*, sia in termini di riduzione del carico di lavoro degli *external auditors* e quindi del costo complessivo degli incarichi di revisione<sup>43</sup>. In particolare, la funzione di Internal Audit fornisce le sue attività in materia amministrativo-contabile con riferimento alla comprensione e mappatura del processo amministrativo-contabile, focalizzazione sui principali controlli contabili e valutazione della tracciabilità e documentalità del processo ai fini della supportabilità del dato contabile. Ad esempio, con riguardo al processo di acquisto, il financial audit effettua controlli su: analisi del processo di fatturazione (automatica o manuale), gestione degli accantonamenti, fatture da ricevere, esecuzione dei pagamenti e gestione delle note di credito.

L'attività volta a fornire un'assurance sulla corretta gestione del rischio di inosservanza di norme interne o esterne viene definita come Compliance Audit. In particolare, si fa riferimento al rischio di incorrere in sanzioni, perdite finanziarie o danni reputazionali in conseguenza di violazioni di norme imperative (leggi, regolamenti) o di autoregolamentazioni (statuto aziendale, codici di condotta, codici di autodisciplina, ecc.). L'Internal Audit, in materia, deve assicurare il management circa la capacità dell'organizzazione di prevenire tale rischio di violazione delle normative. L'approccio che viene generalmente utilizzato comprende analisi delle procedure aziendali o della normativa applicabile alla società e al processo oggetto di analisi, nonché verifiche dell'aderenza alle regole interne ed esterne in ogni fase del processo. Ad esempio, nell'ambito del processo di acquisto, l'enfasi è posta sull'applicazione

---

<sup>42</sup> DITTMER C., *Internal Auditing: chiave per la corporate governance*, EGEA, 2011, pag. 258.

<sup>43</sup> ZAIN M.M., ZAMAN M., MOHAMED Z., *The Effect of Internal Audit Function Quality and Internal Audit Contribution to External Audit on Audit Fees*, International Journal of Auditing, 2015, pagg. 134-147.

delle procedure aziendali o della normativa applicabile al settore nelle varie fasi del processo di approvvigionamento.

Per concludere, va accennata brevemente per poi essere ripresa all'interno del terzo capitolo del presente lavoro, l'ultima tipologia di auditing: il Fraud Audit. A tal riguardo, l'attività di fraud auditing si definisce come il processo che si pone l'obiettivo di identificare le cause e le responsabilità afferenti specifici eventi o incidenti o comportamenti di frode o infedeltà societaria. In particolare, questa tipologia di audit assume rilievo nel momento in cui sorgano dei sospetti circa l'avvenuto compimento di atti illeciti volti a raggirare, occultare e abusare delle norme ai fini dell'ottenimento di un beneficio economico. In questi termini, la stessa assume caratteristiche di omogeneità con l'appena menzionato Compliance Audit, anche se da un punto di vista operativo le attività svolte si avvicinano molto più a quelle presenti nell'ambito dell'Operational Audit. Per fornire un'idea più precisa delle attività svolte in tale ambito, nell'esame della corretta esecuzione del processo di acquisto, il fraud auditing analizzerà aspetti come: l'alterazione della gara tra fornitori, l'inserimento di fornitori non esistenti in anagrafica, il pagamento di fatture per prestazioni non esistenti, ecc.

### **1.6.3. Reporting**

La fase di reporting all'interno di un processo di Audit assume carattere di fondamentale importanza in quanto, durante tale fase, avviene la comunicazione dei risultati ottenuti e che, se effettuata in maniera efficace e trasparente, è in grado di creare valore reale per l'Organizzazione. Tale fase si suddivide in due momenti fondamentali:

- *Exit meeting*, in cui vengono presentati formalmente i risultati ottenuti;
- Redazione di un *Audit report*, ossia un documento che riassume i contenuti dell'attività svolta.

Con riguardo al primo momento, il responsabile della funzione di Internal Audit assume la responsabilità di convocare una riunione, molto simile al *kick-off meeting* nella composizione dei partecipanti, in cui si intende comunicare i risultati ottenuti e condividere idee per lo sviluppo di una strategia di azione per la posta in essere delle dovute correzioni. Infatti, durante questo meeting, gli auditor hanno la possibilità di concentrarsi sul contenuto, piuttosto che sulla forma, dell'output del processo di audit, ottenendo una comunicazione efficace anche attraverso la presentazione di slide e il supporto audiovisivo. L'obbiettivo è quello di spiegare i contenuti che saranno presenti nell'Audit Report e di definire, almeno negli aspetti sostanziali, il piano di azione.

L'Audit Report, invece, “costituisce una prova durevole del carattere professionale dell'attività di audit effettuata e consente la valutazione da parte di soggetti terzi”<sup>44</sup>. Con esso, gli auditor sono in grado di fornire informazioni circa i rilievi emersi durante lo svolgimento dell'incarico, spiegando le criticità individuate e ogni altra informazione che permetta di contestualizzare il fenomeno. In particolare, per ogni criticità devono essere definite:

- a) Le raccomandazioni e i suggerimenti dell'auditor per l'eliminazione o riduzione della criticità;
- b) I commenti del management rispetto quanto riscontrato;
- c) Il piano di azione del management in termini di attività, tempistiche e responsabili della messa in atto del piano.

Inoltre, al fine di attribuire al documento un forte potere comunicativo, è buona pratica:

- Utilizzare, per ogni *finding*, un titolo accattivante e che sia in grado di riassumere il fulcro del problema;
- Fornire una descrizione chiara e sintetica del rilievo riscontrato;
- Attribuire un rating a ciascun rilievo, in una scala crescente in base alla gravità di quanto emerso dalle valutazioni degli auditor;
- Indicare brevemente i suggerimenti per la messa in atto di azioni correttive del problema;

---

<sup>44</sup> DITTMER C., *Internal Auditing: chiave per la corporate governance*, EGEA, 2011, pag. 355.

- Indicare i soggetti responsabili dell'area sottoposta a processo;
- Indicare gli obiettivi dell'incarico e il risultato, complessivo, raggiunto.

In sintesi, la fase di Reporting assume rilevanza specialmente per il suo potere comunicativo e l'obiettivo che si intende raggiungere non riguarda una mera comunicazione dei risultati, bensì la creazione dei presupposti per una piena condivisione degli stessi e per lo sviluppo di un piano di azione quanto più possibile condiviso.

#### **1.6.4. Follow-up**

L'ultima fase del processo di Audit è definita come follow-up. Essa consiste nel monitoraggio e nella documentazione del superamento delle carenze identificate e nell'implementazione delle azioni correttive. Infatti, è evidente come l'intervento di internal auditing, affinché possa raggiungere il fine ultimo della creazione di valore per l'organizzazione, non può limitarsi a comunicare i risultati emersi in sede di *execution*, ma deve saper coinvolgere ulteriormente le aree aziendali auditate nell'intraprendere le azioni correttive presenti nei piani di azione. Secondo gli Standard, infatti, il follow-up rappresenta<sup>45</sup> “il processo tramite il quale l'internal auditor determina l'adeguatezza, l'efficacia e la tempestività delle azioni intraprese dal management in risposta ai rilievi e alle raccomandazioni”.

Entrando nello specifico, le attività che vengono poste in essere in tale fase sono le seguenti:

- a) Richieste dello stato di avanzamento al management: attraverso la richiesta di aggiornamenti sullo stato di avanzamento l'internal auditor riesce a mostrarsi presente anche a seguito dell'intervento di audit svolto, sollecitando la posta in essere delle azioni concordate;

---

<sup>45</sup> INSTITUTE OF INTERNAL AUDITORS (IIA), *International Professional Practices Framework (IPPF): Standard IIA 2500: Il processo di Follow-up*, 1999.

- b) Verifica dei piani di azione: attraverso dei nuovi interventi di audit specifici, l'internal auditor apprende notizie circa la reale messa in atto delle azioni predisposte;
- c) Verifica dell'effettivo miglioramento del Sistema di Controllo Interno: mediante interventi di audit successivi, l'auditor è in grado di valutare l'effetto delle azioni messe in atto dal management in termini di riduzione del rischio complessivo e di miglioramento del Sistema di Controllo Interno.

Infine, va evidenziata l'importanza della fase di follow-up nell'ambito di un intervento di audit in quanto essa aggiunge valore al singolo processo, incentivando l'aggiornamento dei sistemi di controllo e la risoluzione delle problematiche evidenziate. Tale incentivo è legato soprattutto al rispetto, da parte del management, delle scadenze pattuite in sede di comunicazione dei risultati. Questo processo è in grado di generare un circolo vizioso di *continuous improvement* con un impatto positivo sul raggiungimento di un sistema di controllo ottimale e quindi con il miglioramento dei risultati aziendali sia nel breve ma soprattutto nel medio-lungo termine.

## **1.7. Un approfondimento sui principali Standard internazionali**

Nel quarto paragrafo del presente lavoro si era fatto cenno all'International Professional Practices Framework e quindi anche agli Standard fondamentali per la Professione di internal auditing, senza entrare tuttavia in dettaglio nella trattazione di questi principi. Inoltre, nel quinto paragrafo e quindi nella trattazione della natura dell'attività di Internal Audit si è fatto specifico riferimento allo standard 2100 e ss., al fine di comprendere al meglio l'argomento oggetto di trattazione. Nel presente paragrafo, infine, saranno trattati alcuni tra gli standard più autorevoli, in modo da fornire ulteriori spunti di riflessione per una conoscenza più completa sull'argomento.

Tra gli standard di connotazione merita sicuramente una menzione lo standard 1000 intitolato "finalità, poteri e responsabilità", il quale ha il merito di introdurre l'argomento dell'Audit Charter, o Mandato di Audit. In particolare, lo stesso recita:

“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 e con gli elementi vincolanti dell’International Professional Practices Framework. Il Responsabile della funzione deve verificare periodicamente il Mandato e sottoporlo all’approvazione del senior management e del board”<sup>46</sup>.

All’interno di questo documento formale, di fatto, vengono stabiliti gli obiettivi strategici della funzione e quindi le aspettative del vertice aziendale. Inoltre, esso è in grado di delineare gli elementi essenziali dell’attività che viene svolta dall’internal audit, con riguardo sia alle attività di assurance che a quelle di consulenza. In particolare, l’Audit Charter autorizza l’accesso ai dati, alle persone e ai beni aziendali e stabilisce la posizione dell’attività di internal audit nell’organizzazione, precisando la natura del rapporto funzionale del responsabile internal auditing al board, quindi garantendo l’indipendenza e l’autonomia della funzione. In relazione a quest’ultimo aspetto, occorre notare che il Mandato rappresenta quindi un punto di riferimento, uno statuto per l’attività di internal auditing, che di fatto la legittima e ne stabilisce l’importanza, gli obiettivi oltre che la collocazione organizzativa.

Per quanto riguarda l’approvazione dell’Audit Charter, infine, lo Standard prevede che essa avvenga ad opera del Consiglio di Amministrazione. Ovviamente, nelle prassi aziendali delle società quotate in borsa, questa funzione viene rimandata al Comitato per il controllo interno, rientrando tra i compiti di vigilanza sul sistema di controllo interno. Nelle banche, invece, è previsto che la regolamentazione dell’attività di internal auditing sia approvata al Consiglio di Amministrazione<sup>47</sup>.

Inoltre, si è più volte fatto riferimento al concetto dell’indipendenza dell’Internal Audit e sull’argomento interviene lo Standard 1100 intitolato “Indipendenza e obiettività”. Questo afferma che “l’attività di internal auditing deve essere indipendente e gli auditor devono essere obiettivi nello svolgimento del proprio incarico”<sup>48</sup>. Tradotto, l’indipendenza e l’obiettività stanno ad indicare la libertà da condizionamenti e

---

<sup>46</sup> INSTITUTE OF INTERNAL AUDITORS (IIA), *International Professional Practices Framework (IPPF): Standard 1000 - Finalità, poteri e responsabilità*, 1999.

<sup>47</sup> BANCA D’ITALIA, *Istruzioni di Vigilanza per le banche: Attività di revisione interna*, 2006.

<sup>48</sup> INSTITUTE OF INTERNAL AUDITORS (IIA), *International Professional Practices Framework (IPPF): Standard 1100 – Indipendenza e obiettività*, 1999.

l'attitudine di imparzialità mentale, che possono essere ottenute solo attraverso una corretta collocazione organizzativa della funzione. Sull'argomento dell'indipendenza gli Standard immediatamente successivi al 1100 aiutano a comprendere meglio come è possibile evitare che questa venga compromessa. Da un punto di vista individuale, ad esempio, è richiesto che gli auditor mantengano un atteggiamento imparziale e senza pregiudizi, evitando qualsiasi conflitto di interesse<sup>49</sup>, dove per conflitto di interesse si intende quella situazione dove un auditor abbia un interesse personale o professionale contrario rispetto a quello dell'Organizzazione. Il conflitto di interesse, secondo gli Standard, non permetterebbe agli auditor di assolvere i propri compiti con imparzialità, compromettendo la qualità dell'attività svolta.

Laddove l'indipendenza e l'obiettività dell'auditor sia compromessa o appaia come tale, “le circostanze dei condizionamenti devono essere rese note ad appropriati interlocutori”<sup>50</sup> e la natura dell'informativa dipenderà dal tipo di condizionamento che l'auditor si trova ad affrontare. Ad esempio, è previsto che gli auditor si astengano nel valutare delle attività per le quali siano stati in precedenza responsabili. Oppure, se durante lo svolgimento di un incarico di consulenza l'internal auditor si renda conto di essere in presenza di un potenziale condizionamento della propria indipendenza o obiettività, deve segnalarlo al cliente prima di accettare l'incarico. Lo standard riporta poi alcuni esempi di fattori che possono condizionare l'indipendenza organizzativa e l'obiettività individuale, tra cui i conflitti di interessi personali e le restrizioni dell'accesso a dati, persone e beni.

Spostando la nostra attenzione agli Standard di prestazione, invece, occorre fare un primo riferimento allo Standard 2000 – Gestione dell'attività di internal audit<sup>51</sup>, secondo cui chi svolge tale attività deve saperla gestire adeguatamente affinché questa sia in grado di fornire valore all'Organizzazione. La gestione dell'attività di internal audit, recita lo Standard, è efficace quando:

---

<sup>49</sup> INSTITUTE OF INTERNAL AUDITORS (IIA), *International Professional Practices Framework (IPPF): Standard 1120 – Obiettività individuale*, 1999.

<sup>50</sup> INSTITUTE OF INTERNAL AUDITORS (IIA), *International Professional Practices Framework (IPPF): Standard 1130 – Condizionamenti dell'indipendenza o dell'obiettività*, 1999.

<sup>51</sup> INSTITUTE OF INTERNAL AUDITORS (IIA), *International Professional Practices Framework (IPPF): Standard 2000 – Gestione dell'attività di internal audit*, 1999.

- Raggiunge le finalità e le responsabilità indicate nel Mandato;
- 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.

Lo Standard 2000 conclude poi affermando che l'attività di Internal Audit è in grado di creare valore solo in una visione integrata di diverse variabili quali le strategie, gli obiettivi e i rischi. In relazione a quest'ultimo aspetto, anche lo Standard 2010<sup>52</sup> insiste sulla considerazione del fattore di rischio nella pianificazione dell'attività di internal auditing. Infatti, come si è più volte affermato all'interno di questo capitolo, essa passa necessariamente attraverso una attenta valutazione dei rischi, legati agli obiettivi che si intendono raggiungere, che deve essere effettuata almeno una volta l'anno e deve tenere in considerazione le aspettative del senior management, del board e degli altri stakeholder. Una volta redatto il piano, questo deve essere approvato dal senior management e dal board<sup>53</sup>.

Oltre al piano di audit, "il responsabile della funzione deve periodicamente informare il senior management e il board in merito a finalità, poteri e responsabilità dell'attività di internal auditing nonché comunicare lo stato di avanzamento del piano e la conformità dell'attività di internal auditing al Codice Etico e agli Standard"<sup>54</sup>. Questo è quanto afferma lo Standard 2060 in riferimento alle comunicazioni che la funzione deve intrattenere con il Consiglio di Amministrazione e il senior management. La frequenza delle comunicazioni può essere decisa liberamente ma in comune accordo tra i soggetti coinvolti e deve includere delle considerazioni circa i rischi significativi, con particolare riguardo al rischio di frode, ai problemi di controllo e governance e ogni altra questione ritenuta di fondamentale importanza.

---

<sup>52</sup> INSTITUTE OF INTERNAL AUDITORS (IIA), *International Professional Practices Framework (IPPF): Standard 2010 - Pianificazione*, 1999.

<sup>53</sup> INSTITUTE OF INTERNAL AUDITORS (IIA), *International Professional Practices Framework (IPPF): Standard 2020 – Comunicazione e approvazione*, 1999.

<sup>54</sup> INSTITUTE OF INTERNAL AUDITORS (IIA), *International Professional Practices Framework (IPPF): Standard 2060 – Comunicazione al senior management e al board*, 1999.

Infine, per quanto riguarda la fase di reporting dei risultati ottenuti durante lo svolgimento dell'incarico, lo standard 2400 e ss. richiede che vengano comunicati gli obiettivi, l'ambito di copertura e i risultati dell'incarico. Inoltre, la comunicazione deve contenere le raccomandazioni e i piani di azione, corredata dal giudizio dell'internal auditor<sup>55</sup>. Ancora, lo Standard 2420 promuove le caratteristiche che la comunicazione deve possedere affinché sia considerata efficace<sup>56</sup>, le quali sono:

- Accuratezza;
- Obiettività;
- Chiarezza;
- Completezza;
- Tempestività;

Inoltre, si richiede che essa sia concisa e che quindi eviti formulazioni non necessarie e dettagli superflui, oltre che costruttiva nell'indurre i miglioramenti necessari.

Per concludere, è necessario che i risultati siano comunicati agli opportuni destinatari, cioè a quei soggetti in grado di assicurarne un seguito adeguato<sup>57</sup>.

## **1.8. Conclusioni**

Con il presente capitolo sono stati forniti gli elementi chiave ai fini della comprensione del fenomeno dei controlli di impresa e del ruolo dell'internal auditing nel complesso sistema di controllo interno. Tuttavia, alla luce di quanto esposto, occorre chiedersi se la professione dell'internal auditor ha un impatto rilevante nella creazione di valore di impresa o va inquadrata esclusivamente nel suo ruolo passivo di "controllore".

---

<sup>55</sup> INSTITUTE OF INTERNAL AUDITORS (IIA), *International Professional Practices Framework (IPPF): Standard 2410 – Modalità di comunicazione*, 1999.

<sup>56</sup> INSTITUTE OF INTERNAL AUDITORS (IIA), *International Professional Practices Framework (IPPF): Standard 2420 – Qualità della comunicazione*, 1999.

<sup>57</sup> INSTITUTE OF INTERNAL AUDITORS (IIA), *International Professional Practices Framework (IPPF): Standard 2440 – Divulgazione dei risultati*, 1999.

La chiave di risposta va ricercata nell'accezione "consulenziale" dell'attività di internal auditing, piuttosto che nell'idea di un Organo con finalità di vigilanza sull'operato di chi esercita, in prima e seconda battuta, i controlli aziendali. Infatti, come precisato nella definizione degli IPPF, l'Internal Audit rappresenta un'attività che non si limita a fornire assurance sul sistema di controllo, né si qualifica come un processo il cui output è la mera emanazione di un giudizio, bensì contempla un'azione propositiva per il miglioramento della corporate governance, della gestione del rischio e del sistema di controllo interno, il cui fine ultimo è quello di creare valore per l'impresa. Tale finalità può definirsi raggiunta nel momento in cui l'internal auditor estende l'orizzonte temporale dell'intervento anche successivamente alla comunicazione del giudizio al board e al senior management aziendale. La fase di follow-up rappresenta quindi un momento cruciale che, esercitando stimoli continui nei confronti del management affinché ponga in essere le azioni correttive repute necessarie, permette il reale miglioramento del sistema impresa limitando i rischi e in tal senso migliorando le performance dell'impresa e infondendo maggiore fiducia negli stakeholders.

## Capitolo Secondo

### **L'Internal Audit e le relazioni con gli Organi di controllo**

#### **2.1. Introduzione**

Nel capitolo precedente si è fornito un quadro generale utile per la comprensione del fenomeno del Sistema di Controllo Interno oltre che, nello specifico, della funzione di Internal Audit. In particolare, si è analizzata a fondo la natura dell'attività di internal auditing e la sua collocazione organizzativa all'interno del sistema aziendale, senza però considerare le interazioni effettivamente esistenti tra questa e le restanti funzioni di controllo.

In primo luogo, la definizione generale di “controllo dell'impresa” è in grado di assumere diverse sfaccettature<sup>58</sup>, riconducibili principalmente al controllo esercitato dagli azionisti di maggioranza, in termini di guida della dinamica evolutiva della creazione di valore dell'impresa; al controllo di un'entità giuridica nei confronti di un'altra, con cui si imprime il potere di direzione e coordinamento; alla definizione di controllo, comunemente accolta all'interno di questo lavoro, intesa come “verifica di conformità ad un principio, regola o programma”<sup>59</sup>. In virtù del fatto che, nell'analisi degli organi di impresa deputati a svolgere una verifica della conformità rispetto a principi, normative e procedure, ci troviamo di fronte a un sistema sempre più complesso col crescere delle dimensioni aziendali, occorre ricordare la distinzione fondamentale tra i tre livelli del controllo. In secondo luogo, infatti, va ricordato che l'Internal Audit rappresenta un tipo di controllo di terzo livello, la cui funzione è quella di fornire un *assurance* obbiettiva sul corretto funzionamento dei controlli di prima e seconda linea e ciò rende tale funzione indispensabile, per la quantità e l'eterogeneità di informazioni che raccoglie, per il coordinamento tra le varie forme di controllo.

---

<sup>58</sup> BIANCHINI N., DI NOLA C., *I controlli societari: molte regole, nessun sistema*, Milano, EGEA, 2010, p. 116.

<sup>59</sup> GIANNINI M.S., *Diritto Amministrativo*, I, Milano, 1970, p. 308 ss.; ZANDA G., *La funzione direzionale del controllo*, Cagliari, 1967, p. 34 ss. e p. 51 ss.

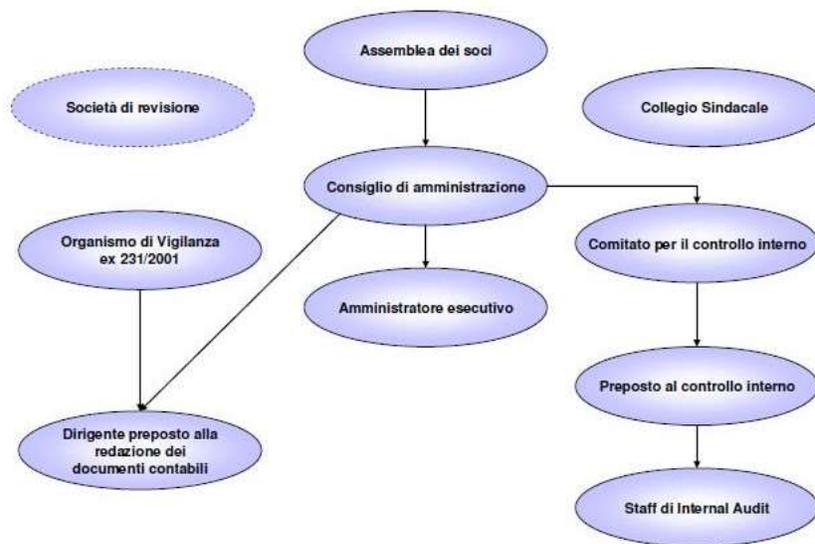


Figura 11 - La governance aziendale nelle società di capitali

Per tale motivo, nel presente capitolo verrà effettuata un'indagine, sia dal punto di vista giuridico e autoregolamentare, sia in ottica operativa, sulle forme di interazione tra la funzione di internal auditing e, in ordine, le seguenti funzioni deputate al controllo dell'impresa:

- Il consiglio di amministrazione;
- Il comitato controllo e rischi;
- Il collegio sindacale;
- L'Organismo di Vigilanza ex D.Lgs. 231/2001;
- Il dirigente preposto alla redazione dei documenti contabili e societari;
- La società di revisione esterna.

## 2.2. I rapporti con il Consiglio di Amministrazione

Con l'avvento delle grandi *public companies* il ruolo dell'organo direttivo sta assumendo sempre più una veste di organo di supervisione strategica dell'ente

piuttosto che di direzione gestionale dello stesso. Per tale motivo, le tipologie di attività che gli si richiedono, oltre alla definizione delle strategie aziendali, si estendono alla supervisione e alla verifica costante del corretto funzionamento del Sistema di Controllo Interno. A tal riguardo, il Codice di Autodisciplina delle società quotate ha ben delineato le funzioni che competono al Consiglio di Amministrazione in tema di corporate governance, precisando che esso<sup>60</sup> “definisce la natura e il livello di rischio compatibile con gli obiettivi strategici dell’emittente, includendo nelle proprie valutazioni tutti i rischi che possono assumere rilievo nell’ottica della sostenibilità nel medio-lungo periodo dell’attività dell’emittente”; nonché “valuta l’adeguatezza dell’assetto organizzativo, amministrativo e contabile dell’emittente [...] con particolare riferimento al sistema di controllo interno e di gestione dei rischi”.



Figura 12 - La relazione tra il Consiglio di Amministrazione e la Funzione di Internal Audit

Da queste assunzioni scaturisce l’esigenza di un confronto periodico tra il Consiglio di Amministrazione e le funzioni aziendali, tra cui rientra l’Internal Audit, che sono in grado di fornire delle valutazioni *risk-based* sulla struttura organizzativa, amministrativa e contabile della società. In particolare, l’Internal Audit è in grado di

---

<sup>60</sup> Art. 1, C.1, lett. b) e c), *Codice di autodisciplina*, Comitato per la Corporate Governance, Borsa Italiana, 2018.

fornire al CdA “assurance sull’efficacia dei processi di governance, gestione dei rischi e controllo interno, prendendo in considerazione i rischi strategici, di reputazione, di mercato, creditizi, operativi e finanziari”<sup>61</sup>, informazioni indispensabili per l’attuazione di strategie in grado di creare valore per l’impresa nel medio e lungo termine. Proprio in relazione alla necessità, da parte dell’Organo direzionale, di attingere a determinate informazioni per svolgere al meglio il proprio incarico, si considera lo stesso come unico responsabile del buon funzionamento del Sistema di Controllo Interno e in quanto tale, come promotore per l’implementazione di una efficace ed efficiente attività di internal auditing.

Entrando in dettaglio, la frequenza e la natura delle discussioni tra la funzione di Internal Audit e il Consiglio di Amministrazione vengono decise proprio da quest’ultimo<sup>62</sup>, a seconda della periodicità delle riunioni da quest’ultimo stabiliti, salvo casi particolari<sup>63</sup>. Il primo momento di contatto coincide con la definizione del ruolo e degli obiettivi che la Funzione deve assolvere. Questi elementi, come è stato trattato all’interno del capitolo precedente, devono essere formalizzati in un documento chiamato Mandato di Internal Audit o *Internal Audit Charter*. Lo standard di connotazione 1000 definisce il contenuto del Mandato e stabilisce che questo venga approvato dal Consiglio di Amministrazione. All’interno del documento dovranno essere ripartite:

- a) Le finalità;
- b) Le autorità;
- c) Le responsabilità.

Ovviamente, la formalizzazione della funzione di Internal Audit in un Mandato non è sufficiente a garantire che questa venga svolta efficacemente. Piuttosto, se l’attività di internal auditing è funzionale al rispetto degli obblighi di supervisione che il Consiglio deve rispettare, il Consiglio di Amministrazione dovrà a sua volta diffondere e

---

<sup>61</sup> ECIA, *L’Internal Auditing in Europa*, Position Paper, 2005, pag. 29.

<sup>62</sup> In materia, si veda l’Art. 1, C. 1, lett. d) del Codice di Autodisciplina delle società quotate, il quale recita “*Il Consiglio di Amministrazione stabilisce la periodicità, comunque non superiore al trimestre, con la quale gli organi delegati devono riferire al consiglio circa l’attività svolta nell’esercizio delle deleghe loro conferite*”.

<sup>63</sup> DITMEIER C., *Internal Auditing: chiave per la corporate governance*, EGEA, 2011, pag. 104.

promuovere una cultura del controllo all'interno della intera Organizzazione al fine di favorire il raggiungimento degli obiettivi di audit.

Quanto appena detto giustifica ulteriormente l'esigenza di un confronto continuativo sulle tematiche di auditing e di gestione dei rischi aziendali tra le due funzioni, necessarie all'espletamento degli obiettivi di entrambe. Questo confronto può avvenire con diversa frequenza, non essendo prevista per legge una periodicità predefinita con cui una funzione debba riferire all'altra sull'operato svolto. Tuttavia, è opinione comune che la periodicità con cui l'internal auditing deve comunicare i risultati ottenuti durante lo svolgimento dell'incarico di audit deve essere tale da assecondare la necessità di un intervento tempestivo da parte del Consiglio di Amministrazione. In questi termini, potremmo suddividere l'informativa tra le due funzioni in:

- Informativa periodica e sistematica, i cui termini e le modalità sono stabiliti in via preventiva;
- Informativa episodica e tempestiva, qualora emergano delle situazioni inaspettate e che richiedono interventi di urgenza da parte del Consiglio di Amministrazione.

Secondo gli Standard e le guide applicative, il Responsabile della funzione di internal auditing dovrebbe, almeno una volta l'anno:

- 1) Sottoporre una sintesi del programma di internal auditing al vertice aziendale, affinché questo ne approvi il contenuto, il piano delle risorse e il budget di spesa;
- 2) Comunicare ogni variazione successiva al programma precedentemente approvato;
- 3) Presentare un rapporto sull'attività svolta.

Per concludere, al fine di permettere il più ampio scambio informativo possibile e di favorire l'indipendenza della Funzione di Internal Audit, è prassi diffusa la partecipazione del Responsabile della Funzione alle riunioni dei vertici aziendali

qualora sia stata definita, all'ordine del giorno, la trattazione di tematiche di corporate governance e di controllo interno.

### **2.3. I rapporti con il Comitato Controllo e Rischi**

Nelle pagine precedenti, si è largamente discusso sull'Organo di impresa cui compete la funzione di sorvegliare, in un'ottica strategica, sul corretto funzionamento del Sistema di Controllo Interno e quindi sull'attività di internal auditing. A tal riguardo, le *best practices* e l'opinione comune vedono nel Consiglio di Amministrazione l'organo ideale al fine di ricoprire tale ruolo. In particolare, in merito ai rapporti tra questo e la funzione di Internal Audit, il Consiglio di Amministrazione deve:

- a) Approvare il Mandato;
- b) Approvare la valutazione dei rischi, espressa dall'internal auditing, e il relativo piano di audit;
- c) Ricevere le comunicazioni sui risultati raggiunti durante lo svolgimento dell'attività di audit;
- d) Approvare le decisioni di nomina e di rimozione dall'incarico del Responsabile della funzione di internal auditing;
- e) Approvare la retribuzione del Responsabile della funzione di Internal Audit;
- f) Sovrintendere al corretto svolgimento dell'attività di auditing e sincerarsi sulla sussistenza del budget necessario allo svolgimento dell'incarico.

Se è vero che quanto previsto dalle autoregolamentazioni in vigore porti a creare una forte dipendenza funzionale tra i due organi, è pur vero che nella prassi questo rapporto viene in genere intermediato da alcune figure di raccordo. Tra queste, assume un ruolo rilevante il Comitato per il Controllo Interno o Comitato Controllo e Rischi.



Figura 13 - I comitati endo-consiliari

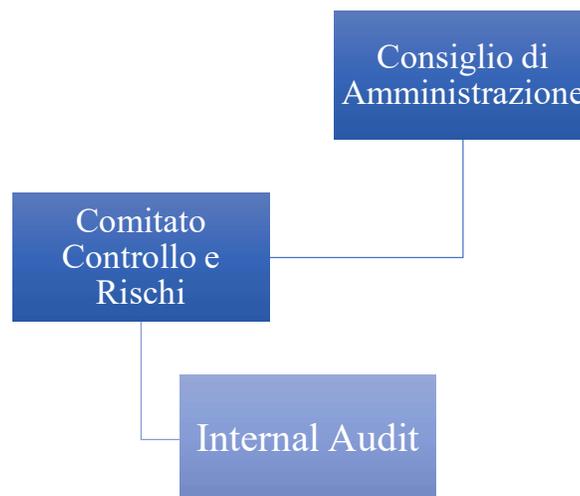
Questo organo diventa fondamentale col crescere delle dimensioni e della complessità della struttura societaria aumentando, di conseguenza, le funzioni e i compiti del consiglio di amministrazione. In realtà strutturate, infatti, al Comitato Controllo e Rischi si richiede che<sup>64</sup>:

- a) Sia composto da amministratori indipendenti ovvero, in alternativa, da amministratori esecutivi a maggioranza indipendenti;
- b) Sia composto da soli amministratori indipendenti se l'Ente è controllato da altra società quotata o sia sottoposto all'altrui direzione e/o coordinamento;
- c) Almeno uno dei componenti deve possedere determinate competenze di natura contabile/finanziaria ed esperienza in materia di risk management;
- d) Fornisca un parere al consiglio di amministrazione in tema di scelte che ricadano nella gestione del sistema di controllo interno;
- e) Esprima un parere su specifici temi circa l'identificazione e la gestione dei rischi aziendali;
- f) Esamini le relazioni periodiche in tema di gestione dei rischi e in particolare quelle fornite dalla funzione di Internal Audit;

<sup>64</sup> Art. 7, C.2, *Codice di autodisciplina*, Comitato per la Corporate Governance, Borsa Italiana, 2018

- g) Monitori l'adeguatezza, l'efficienza e l'efficacia dell'attività di internal auditing;
- h) Può richiedere alla funzione di internal audit lo svolgimento di verifiche su aree operative specifiche, dandone comunicazione al presidente del collegio sindacale;
- i) Riferisca al Consiglio di Amministrazione circa l'adeguatezza del Sistema di Controllo Interno.

In tema di controlli, quindi, il Codice di Autodisciplina da un lato attribuisce primaria responsabilità in capo al Consiglio di Amministrazione, dall'altro prevede per le società quotate che il Consiglio nomini al suo interno un comitato che svolga, in via principale, le funzioni sopra esposte. In questo modo, nel rapporto esistente tra il CdA e la funzione di Internal Audit il comitato per il controllo interno assolve la funzione di "principale collegamento" o "filtro" e sembra essere di fondamentale importanza nei modelli di governance "tradizionale" e "dualistico", in quanto in quello monistico determinate funzioni sono attribuite esplicitamente all'organo di controllo interno.



*Figura 14 - Il Comitato Controllo e Rischi come ponte tra il CdA e l'Internal Audit*

Infatti, da un lato, il comitato controllo e rischi possiede le competenze necessarie a captare tutta l'informativa proveniente dal Responsabile della funzione di internal auditing, e quindi comunicarla, filtrandola, al consiglio di amministrazione. Inoltre, la sua composizione, di regola di soli consiglieri indipendenti, permette all'organo di mostrare maggiore autonomia e indipendenza nelle decisioni. Dall'altro lato, il comitato controllo e rischi è l'organo in grado di guidare dall'alto l'attività di internal auditing, conducendo l'attività di controllo verso il perseguimento degli obiettivi di medio-lungo termine che sono stati pattuiti in sede di pianificazione strategica. In tal senso, nonostante la connotazione di organo di controllo e di supervisione che il comitato riveste, occorre ricordare che si tratti comunque di un comitato interno al consiglio di amministrazione e, in quanto tale, composto da consiglieri di amministrazione, seppur indipendenti. Analizzando questo aspetto si evince come il comitato in questione rivesta a pieno la funzione di supervisione strategica sulla società e sul Sistema di Controllo Interno. Il Consiglio di Amministrazione si serve, in questo modo, delle naturali competenze e conoscenze che compongono il comitato controllo e rischi al fine di esercitare delle funzioni che la legge gli attribuisce, nell'ottica del principio della specializzazione.

Per concludere, appare evidente la stretta collaborazione tra il Responsabile della funzione di internal audit e i consiglieri che compongono il comitato controllo e rischi. In particolare, si ritiene necessario un continuo scambio di flussi informativi che hanno a oggetto:

- Le aspettative, gli obiettivi e le priorità che il vertice aziendale intende conseguire;
- Gli aggiornamenti sull'attività di auditing svolta;
- La valutazione complessiva sul profilo di rischio della società e sull'adeguatezza del Sistema di Controllo Interno.

## 2.4. I rapporti con il Collegio Sindacale

Dopo aver trattato la natura dei rapporti intercorrenti tra la funzione di Internal Audit e il Consiglio di Amministrazione e tra la Funzione e il Comitato Controllo e Rischi, è giunto il momento di analizzare in che modo due funzioni di “controllo”, l’internal auditing e il Collegio Sindacale, operano sinergicamente con l’obiettivo di raggiungere una finalità comune. Occorre chiarire fin da subito che la riforma del diritto societario del 2003 è stata fondamentale al fine di distinguere la natura e le finalità dei diversi Organi di controllo aziendali. In particolare, con la Riforma si è introdotta la possibilità di adottare tra i tre modelli di governance (tradizionale, dualistico e monistico), a cui si collegano tre differenti organi di controllo:

- Collegio Sindacale;
- Consiglio di Sorveglianza;
- Comitato per il Controllo sulla Gestione.

Per semplicità espositiva, poiché le funzioni attribuite all’Organo deputato al controllo dell’Ente sono pressoché identiche, almeno dal punto di vista delle attività di controllo, nel seguente paragrafo verrà trattato il solo Collegio Sindacale.

Una prima distinzione, tra gli organi deputati al controllo, va effettuata in base all’oggetto di analisi e verifica. Va infatti ricordato che l’attività principale svolta dal Collegio Sindacale fa riferimento a un tipo di controllo esclusivamente amministrativo, in quanto il legislatore ha attribuito l’attività di controllo contabile, precedentemente esercitata da questo, alla società di revisione o al revisore legale dei conti esterno, salvo particolari eccezioni. Infine, come è stato più volte ripetuto nelle pagine precedenti, la funzione di Internal Audit esercita un controllo di terzo livello, volto a fornire un’assurance sul corretto funzionamento dell’intero sistema di controllo interno, da cui sembra emergere dunque una piena separazione delle funzioni svolte dagli organi fin qui elencati. In realtà, nel Testo Unico della Finanza<sup>65</sup>, il legislatore ha previsto per i soggetti preposti al controllo interno, tra cui quindi il Responsabile della funzione di internal auditing, il dovere di riferire al Collegio Sindacale tutte le

---

<sup>65</sup> Art. 150, D. Lgs. 24 Febbraio 1998, n.58, *Testo Unico della Finanza*, CONSOB, Gennaio 2019.

informazioni ritenute necessarie per lo svolgimento dell'incarico di tali organi. Inoltre, un primo punto di raccordo tra le attività dei diversi Organi va ricercato ancora nel TUF<sup>66</sup>, il quale sancisce che “il Collegio Sindacale deve vigilare anche sull'adeguatezza del Sistema di Controllo Interno”, ricoprendo in parte quel ruolo che più propriamente spetta alla funzione di internal auditing.

Quanto emerge dall'art. 149 del Testo Unico è fondamentale per comprendere a pieno il fenomeno del controllo societario, in relazione alle numerose forme in cui esso è esercitato e dai diversi soggetti che svolgono tale attività. Infatti, seppur il legislatore attribuisca a una funzione specifici poteri o mansioni sulla base di un criterio di specializzazione, tra gli organi deputati al controllo e tra i componenti di tali organi deve instaurarsi una forma di rapporto basata sullo scambio di flussi informativi, al fine di generare quello che viene definito un “crocevia di informazioni”<sup>67</sup>. Tra i principali temi trattati, tali informazioni avranno ad oggetto l'attività di auditing svolta, che dovrà essere allineata al piano di audit preventivato, e gli eventuali interventi di audit straordinario qualora siano emerse problematiche particolari.

Il legislatore non precisa in alcun modo il contenuto specifico o la periodicità di tali comunicazioni, limitandosi a riferire che la comunicazione può avvenire su richiesta diretta da parte degli organi di controllo (o anche da uno solo dei suoi membri) oppure su iniziativa dello stesso responsabile. Mentre il Consiglio Nazionale dei Dottori Commercialisti ha precisato che il Collegio Sindacale dovrebbe, con cadenza almeno trimestrale, tenere una riunione con il Responsabile della funzione di internal auditing, con la redazione di un verbale in cui siano raccolte tutte le informazioni trattate in sede di consiglio<sup>68</sup>. La cadenza trimestrale indicata nel documento intende essere sufficiente e necessaria al fine di informarsi reciprocamente sull'attività svolta, sulle problematiche emerse e sulle azioni che si ritengono necessarie.

Il contenuto dell'informativa deve assolutamente riguardare<sup>69</sup>:

---

<sup>66</sup> Art. 149, D. Lgs. 24 Febbraio 1998, n.58, *Testo Unico della Finanza*, CONSOB, Gennaio 2019.

<sup>67</sup> DITTMER C., *Internal Auditing: chiave per la corporate governance*, EGEA, 2011, pag. 111.

<sup>68</sup> CNDC, *Principi di comportamento del Collegio Sindacale nelle società di capitali con azioni quotate nei mercati regolamentati*, Norme di comportamento del Collegio Sindacale, Settembre 2015.

- a) L'emersione dei rischi o delle aree di criticità, potenziali o effettivi;
- b) Il rilevamento di violazioni di leggi, atti costitutivi o statuti e norme interne;
- c) La comparsa di fatti censurabili;
- d) La valutazione del generale assetto del Sistema di Controllo Interno;
- e) La determinazione dei requisiti di professionalità e indipendenza necessari allo svolgimento degli incarichi di audit.

Infine, negli incontri tra il Responsabile della funzione di Internal Audit e il Collegio Sindacale devono essere discussi:

- Il piano di audit e lo svolgimento dei lavori;
- Il grado di miglioramento del Sistema di Controllo Interno

## **2.5. I rapporti con l'Organismo di Vigilanza ex D.Lgs. 231/2001**

Con il D.Lgs. 231/2001 è stata introdotta la responsabilità amministrativa dell'Ente che, insieme alla responsabilità penale di chi è il fautore del reato, colpisce la società che non abbia adottato le misure necessarie per la sua prevenzione e ha come obiettivo quello di ridurre il fenomeno dei reati societari<sup>70</sup>. In particolare, nonostante la decisione del legislatore di definire tale responsabilità come "amministrativa", appare evidente come la stessa rientri in realtà nella sfera di competenza penale<sup>71</sup>. Come si diceva, l'ente è responsabile amministrativamente per i reati commessi dai dirigenti, collaboratori o dipendenti aziendali solamente qualora non abbia adottato le misure necessarie per la prevenzione degli stessi. Tra le misure previste dal decreto al fine dell'ottenimento della cosiddetta "condizione esimente" annoveriamo, per semplicità espositiva, principalmente:

---

<sup>70</sup> D.Lgs. 8 Giugno 2001, n. 231, *Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica a norma dell'art. 11 della legge 29 settembre 2000, n.300.*

<sup>71</sup> L'ipotesi di una responsabilità amministrativa esclusivamente formale è peraltro supportata dalla circostanza per cui gli illeciti amministrativi delle società sono materia di competenza del Giudice penale.

- La costituzione di un Modello organizzativo (MOG), con il compito di disciplinare l'attività aziendale al fine di ridurre il compimento dei reati presupposto;
- L'istituzione di un organo, l'Organismo di Vigilanza, con poteri di vigilanza sul rispetto del Modello predisposto.

Sulla base di quanto finora esposto, risultano essere evidenti delle analogie tra il Modello di organizzazione, gestione e controllo e il relativo Organismo di vigilanza con, rispettivamente, il Sistema di Controllo Interno e la funzione di Internal Audit. In particolare, va subito affermato che nonostante siano evidenti determinate assonanze tra tali elementi, avvalorando le ipotesi di un Sistema di Controllo Interno strutturato quale condizione esimente contro la responsabilità amministrativa dell'ente e quale ruolo dell'Organismo di Vigilanza svolto dal responsabile della funzione Internal Audit, la Legge 231 fa espresso riferimento alla prevenzione di specifiche forme di reato, limitando e circoscrivendo il controllo aziendale a tali tematiche.

Ad esempio, con riguardo al MOG ex D.Lgs. 231/2001, esso presenta notevoli elementi in comune con il Sistema di Controllo Interno e di gestione dei rischi, tra cui<sup>72</sup>:

- a) Analisi dei rischi potenziali;
- b) Analisi dei presidi di rischio;
- c) Attribuzione delle responsabilità;
- d) Costituzione di adeguati protocolli e procedure;
- e) Diffusione del modello e attività di formazione del personale;
- f) Controllo da parte di un organo indipendente (Organismo di Vigilanza) al fine di vigilare sull'attuazione del modello e sul suo effettivo funzionamento;
- g) Flussi informativi, tra cui segnalazioni di anomalie, verso l'Organismo di Vigilanza;
- h) Previsione di un sistema sanzionatorio aziendale, in caso di mancata adozione delle norme interne.

---

<sup>72</sup> DITTMER C., *Internal Auditing: chiave per la corporate governance*, EGEA, 2011, pag. 161.

Tutti questi elementi convergono evidentemente con il Modello di Enterprise Risk Management, specialmente in merito:

- a) Alla comunicazione degli obiettivi, la quale si lega al concetto di formazione del personale e di diffusione del modello;
- b) All'ambiente interno, dotato di un codice etico, prassi e procedure e arricchito di norme sanzionatorie;
- c) Al processo di risk management, che partendo da un'identificazione, analisi e valutazione dei principali rischi, si pone come obiettivo quello di determinare il livello di rischio residuo dopo aver tenuto conto dei relativi presidi di rischio presenti in azienda;
- d) Alle azioni di risposta al rischio, le quali richiedono la messa in atto di opportune procedure per evitare, contenere, accettare o gestire i rischi, spesso rivedendo le procedure già esistenti all'interno dell'ente;
- e) All'istituzione di un sistema dei controlli di terzo livello, rappresentato dall'internal auditing da un lato e dall'OdV dall'altro, atto a vigilare sulla correttezza del modello e sulla sua attuazione;
- f) Alla fase di monitoraggio, resa necessaria per lo sviluppo costante del sistema di controllo interno, che in ambito 231 coincide con il processo di aggiornamento continuo del MOG.

Con riguardo all'Organismo di Vigilanza, invece, sulla base di quanto esposto all'interno del decreto e sulla base del contenuto delle Linee Guida per la costruzione dei modelli organizzativi di Confindustria e ABI, si è fin da subito pensato a un accostamento tra esso e il preposto al controllo interno, e quindi all'internal auditing. Infatti, l'Internal Audit possiede i requisiti dell'indipendenza e le competenze necessarie ai fini dell'espletamento di un simile incarico, in quanto in grado di possedere una visione di insieme sui processi aziendali che servono a mitigare il rischio del compimento dei reati. Altro aspetto in comune è rappresentato dalla collocazione dei due organi all'interno dell'organigramma, in entrambi i casi con posizione di riporto nei confronti del Consiglio di Amministrazione o, nello specifico, con il Comitato Controllo e Rischi. Da ciò si può quindi dedurre che il Responsabile della funzione di Internal Audit è il perfetto candidato all'espletamento dell'incarico

di Organismo di Vigilanza, nel caso in cui si decidesse di optare per la costituzione di un Organismo monocratico; altrimenti, questo potrà con grande probabilità rappresentare uno dei componenti di tale organo.

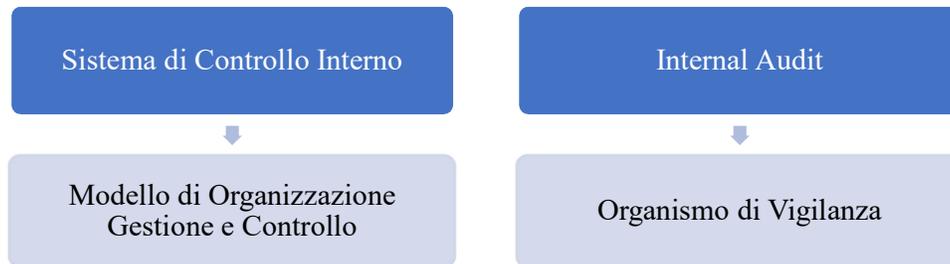


Figura 15 - Il D.Lgs. 231 nel sistema dei controlli

Tuttavia, nonostante la teoria sembra suggerire l'esistenza di una perfetta coincidenza tra l'internal auditing e l'OdV, alcuni studi empirici di corporate governance ci mostrano come si tenda a costituire un apposito organismo collegiale, *ex novo*, con apposite garanzie di indipendenza, qualificazione professionale ed efficienza<sup>73</sup>. In merito alla sua composizione, è previsto che esso sia composto indistintamente da soggetti appartenenti all'ente, come il responsabile della funzione di internal auditing, della funzione compliance, amministratori indipendenti o sindaci, e da soggetti esterni che siano in grado di dotare l'organo di maggiore indipendenza. Nel caso in cui l'organo sia composto principalmente da soggetti esterni, è ovvio come la funzione di internal auditing diventi un supporto strategico ai fini dell'espletamento del suo incarico, sia per le competenze e la professionalità che esso possiede, ma soprattutto per la conoscenza delle procedure esistenti e delle dinamiche aziendali. In ogni caso, dalle più recenti ricerche viene confermata la presenza, nella maggior parte dei casi,

<sup>73</sup> DITTMER C., *Internal Auditing: chiave per la corporate governance*, EGEA, 2011, pag. 113.

della funzione di internal auditing all'interno dell'Organismo di Vigilanza, affiancata da un sempre crescente numero di componenti esterni.

Nel caso in cui, invece, la funzione non fosse presente all'interno dell'OdV, essa si configurerebbe ugualmente come il suo "braccio operativo", ottenendo delega per lo svolgimento di attività di:

- Risk assessment per l'identificazione delle attività potenzialmente sensibili alla commissione dei reati di cui al D.Lgs. 231/2001.
- Analisi e verifiche di audit per la valutazione dell'adeguatezza dei presidi aziendali esistenti e il loro effettivo funzionamento.

In altri termini, ci si aspetta che l'Organismo di Vigilanza approvi un piano di verifiche che l'internal auditing deve eseguire al fine di fornire assurance su determinate aree aziendali soggette al rischio di compimento dei reati presupposto. Inoltre, l'internal auditing fornirebbe un continuo aggiornamento della *risk map* con ad oggetto i rischi di reato all'Organismo di Vigilanza, il quale, a sua volta, la utilizzerebbe come base informativa per la realizzazione di proposte di modifica al Modello Organizzativo.

## **2.6. I rapporti con il Dirigente preposto alla redazione dei documenti contabili societari**

I *corporate scandals* che hanno interessato numerose realtà aziendali verso gli inizi degli anni duemila hanno portato a una reazione, tra gli altri, anche da parte dei *regulator* internazionali e nazionali attraverso l'emanazione di alcune normative in materia di controllo contabile. Tra queste, la principale è stata senza ombra di dubbio il Sarbanes-Oxley Act (comunemente definita "SOX") a cui ha fatto seguito, in Italia, la Legge sulla Tutela del Risparmio<sup>74</sup>, che ne condivide la materia e ne presenta alcuni tratti in comune. In particolare, la Legge n.262 del 2005, intitolata "Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari", è famosa per aver

---

<sup>74</sup> Legge 28 Dicembre 2005, n. 262, *Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari*.

introdotto una nuova figura apicale in azienda, il Dirigente preposto alla redazione dei documenti contabili societari.

La principale funzione svolta da tale organo è quella della redazione dei documenti contabili della società, quindi del bilancio di esercizio, e in quanto tale esso è responsabile della correttezza dell'informativa societaria e nei confronti degli stakeholders. Altra materia trattata dal dirigente preposto riguarda la predisposizione dell'apparato organizzativo e procedurale relativo all'impianto amministrativo e contabile, dove entra fortemente in contatto con la funzione di internal auditing e si rendono necessari quindi continui scambi di informazioni tra queste.

In più di un'occasione sono stati sollevati dei dubbi circa la possibilità che un tale organo possa essere il naturale supervisore e diretto superiore di organi di controllo, di verifica e funzioni di audit all'interno di un'organizzazione aziendale. A risolvere ogni singolo dubbio è tuttavia intervenuta in materia l'Associazione Italiana Internal Auditors (AIIA) che, in diversi *position paper* ha espresso l'impossibilità di obblighi di riporto delle funzioni di controllo di terzo livello nei confronti del Dirigente preposto in quanto si verrebbero a generare dei conflitti di competenze e delle sovrapposizioni nelle funzioni<sup>75</sup>. Quindi, come affermato anche all'interno di un documento dell'Associazione Nazionale dei Direttori Amministrativi e Finanziari (ANDAF), la situazione per la quale una funzione di Audit si qualifichi da un punto di vista organizzativo come il sottoposto del Dirigente preposto costituisce una vera "diseconomia nella gestione aziendale"<sup>76</sup> ed il "presupposto per il generarsi di carenze di controllo in aree in cui si verifichi conflittualità tra sistemi concomitanti".

A prescindere dalla collocazione organizzativa, appare tuttavia evidente come sia necessaria ed opportuna una stretta collaborazione tra la figura del preposto alla redazione dei documenti contabili societari e i vari organi di controllo. In particolare,

---

<sup>75</sup> ASSOCIAZIONE ITALIANA INTERNAL AUDITORS (AIIA), *Legge sulla Tutela del Risparmio*, Position Paper, marzo 2006; Associazione Italiana Internal Auditors (AIIA), *Approccio integrato al sistema di controllo interno: gli organi e le funzioni preposte al controllo interno aziendale e le loro relazioni*, Corporate Governance Paper.

<sup>76</sup> ASSOCIAZIONE NAZIONALE DEI DIRETTORI AMMINISTRATIVI E FINANZIARI (ANDAF), *Il dirigente preposto alla redazione dei documenti contabili societari*, Position Paper ANDAF, maggio 2007.

è opinione diffusa quella per cui il Dirigente preposto si configuri come una funzione “cerniera” tra gli organi direzionali e le funzioni dedicate al controllo contabile<sup>77</sup>. Infatti, le principali attività che esso svolge sono:

- a) Predisposizione delle procedure amministrative e contabili finalizzate alla formazione del bilancio;
- b) Trasmissione al comitato di controllo interno e all’intero Consiglio di Amministrazione di tutte le informazioni utili e necessarie al fine di consentire di esprimere un parere sull’adeguatezza dell’assetto organizzativo e amministrativo contabile della società.

Nello svolgimento di tali mansioni, il dirigente preposto dovrà fare affidamento alle conoscenze e alle competenze possedute dalla funzione di internal auditing che, nel valutare l’intero Sistema di Controllo Interno, possiede senza dubbio principali informazioni in merito ai singoli processi amministrativo – contabili aziendali. Si viene in tal modo a generare una sinergia tra due importanti figure, l’una espressiva della dirigenza aziendale e quindi di chi ha il potere-dovere di predisporre le procedure contabili, l’altra espressiva dell’attività di controllo che su di questa viene esercitata e che quindi è in grado di fornire importanti pareri sulla corretta predisposizione di queste. Quindi, il dirigente preposto non ha un ruolo tipicamente “di controllo” all’interno dell’Organizzazione, piuttosto esso svolge un ruolo “gestionale”, partecipando alla predisposizione delle strutture amministrative e dei processi contabili, senza però poter partecipare al processo di valutazione e stima dei dati contabili<sup>78</sup>. Nel fare ciò, il dirigente proposto può richiedere che siano svolte attività di audit in specifiche aree in cui si evidenzino delle situazioni di rischio e di criticità. L’internal auditing potrà quindi fornire un’assurance “preventiva” sul corretto o meno funzionamento di determinati processi contabili, che servirà al Preposto a capire se poter fare affidamento su tali processi. Inoltre, l’Internal Audit svolgendo attività consulenziale può “verificare e valutare i rischi aziendali, contribuire in modo significativo all’implementazione di un sistema per la loro gestione, assistere nella

---

<sup>77</sup> DITTMAYER C., *Internal Auditing: chiave per la corporate governance*, EGEA, 2011, pag. 120.

<sup>78</sup> ASSONIME, *Il dirigente preposto alla redazione dei documenti contabili nel sistema dei controlli societari*, Circolare 44, novembre 2009.

formazione interna richiesta per diffondere le necessarie competenze metodologiche per l'autodiagnosi dello stato del Sistema di Controllo Interno riguardo a specifici rischi di natura contabile<sup>79</sup>.

Per concludere, non solo l'Internal Audit è in grado di fornire importanti informazioni al Dirigente preposto per l'assolvimento del proprio incarico, ma anche tutto il Sistema di Controllo Interno costituisce uno strumento a ciò dedito. In particolare, va menzionato il grande contributo offerto a tal fine dal revisore esterno legale dei conti e dal Collegio Sindacale.

## **2.7. I rapporti con la Società di Revisione**

Come è stato più volte ribadito, il mutato contesto della corporate governance oggi è soprattutto frutto di quanto accaduto attorno agli anni duemila e agli scandali societari che hanno caratterizzato questo periodo storico. Dopo i *corporate scandals* è certamente aumentata l'attenzione verso la professione della revisione legale esterna e l'aumentare delle fattispecie che i legislatori hanno previsto e per le quali essa debba essere affidata a una società di audit. Il revisore legale dei conti, sia esso una società di revisione o una persona fisica, ha il compito di “esprimere, attraverso un parere (*opinion*) sul bilancio sottoposto a revisione, se i fatti di gestione sono correttamente rilevati nelle scritture contabili, se il bilancio corrisponde alle risultanze di tali scritture e se esso risulta conforme alle norme che ne disciplinano la redazione”<sup>80</sup>. Da tale definizione è possibile comprendere, sulla base di quanto finora affermato, come l'attività di revisione esterna sia cosa diversa dall'attività di internal auditing, principale oggetto di questo lavoro. Infatti, da un lato l'internal auditing deve fornire un'assurance obiettiva sulla corretta predisposizione e sul effettivo funzionamento dell'intero sistema dei controlli aziendali, sulla base di quanto richiesto dalla direzione aziendale, nei confronti dei quali esiste un rapporto organizzativo. Dall'altro, l'audit

---

<sup>79</sup> DITTMAYER C., *Internal Auditing: chiave per la corporate governance*, EGEA, 2011, pag. 121.

<sup>80</sup> DITTMAYER C., *Internal Auditing: chiave per la corporate governance*, EGEA, 2011, pag. 128.

finanziario e contabile si concentra esclusivamente sulla corretta redazione del bilancio, andando a verificare:

- La correttezza e la concordanza dei dati aziendali originari;
- L'affidabilità dei dati contabili;
- Il riscontro dei dati di bilancio attraverso determinate tecniche di revisione ed analisi.

Se le definizioni generali sembrano non lasciare alcun dubbio sulla differente funzione svolta dai due soggetti, nella prassi operativa non poche sono le analogie e i punti di raccordo tra le due attività, tra cui le tecniche di lavoro utilizzate (gestione delle carte di lavoro, tecniche di campionamento, *checklist*, test di verifica, analisi di processo, ecc.). Altro elemento di forte assonanza tra le due materie concerne il *financial audit* svolto dall'Internal Audit, più precisamente l'attività di revisione interna volta ad attestare la corretta predisposizione e l'effettivo funzionamento del processo amministrativo-contabile e di bilancio. Anche in questo caso, ovviamente, la revisione esterna svolge un controllo contabile sui dati espressi in bilancio dalla società, mentre l'internal auditing esprime un parere sul funzionamento dei processi che conducono alla redazione del bilancio. Le due attività sono chiaramente complementari, seppur distinte, e per tale motivo non mancano studi che dimostrano come l'azione sinergica tra le due attività è in grado di comportare minori costi e risultati più efficienti per l'una (la revisione legale esterna) qualora l'altra (l'Internal Audit) sia svolta in maniera efficiente ed efficace<sup>81</sup>. Altri studi più recenti dimostrano invece come non sia tanto la *reliance* sul corretto operato della funzione di revisione interna a ridurre le *fee* della società di audit, quanto più la diretta assistenza prestata dagli internal auditor nei confronti dei revisori<sup>82</sup>.

Inoltre, è noto che in sede di pianificazione il revisore esterno compie delle valutazioni preliminari sull'attività svolta dalla funzione di internal auditing al fine di comprendere come ed in che modo il lavoro svolto dall'Internal Audit possa essere

---

<sup>81</sup> ZAIN M.M., ZAMAN M., MOHAMED Z., *The Effect of Internal Audit Function Quality and Internal Audit Contribution to External Audit on Audit Fees*, International Journal of Auditing, 2015, pagg. 134-147.

<sup>82</sup> PRAWITT D.F., SHARP N.Y., WOOD D.A., *Internal audit quality and earnings management*, The Accounting Review, Vol. 84, pp. 1255 – 1280.

funzionale al lavoro di audit esterno considerando l'organizzazione, gli obiettivi, la competenza tecnica della funzione e la diligenza professionale con la quale sono svolti i lavori di audit.

Sul tema, occorre però aggiungere che non sempre la cooperazione tra le due funzioni è in grado di generare valore aggiunto, celandosi dei rischi relativi a problematiche di coordinamento che potrebbero manifestarsi. In materia si è pronunciato l'Institute of Internal Auditors con la Guida Interpretativa allo Standard numero 2050 ("Coordinamento") il quale sottolinea, per l'appunto, la necessità di specificare le singole attività che i due soggetti svolgono nell'ambito della revisione di un'azienda affinché venga minimizzato il rischio di "duplicazioni". In generale, il rischio di un mancato coordinamento tra le due attività potrebbe comportare le seguenti conseguenze:

- a) Duplicazioni di attività;
- b) Omesso controllo di alcune aree da parte di entrambi i soggetti;
- c) Mancanza dei requisiti di indipendenza e professionalità necessari allo svolgimento dell'incarico.

In merito a quest'ultimo aspetto, ne è un esempio la fattispecie per la quale un revisore legale dei conti si sostituisca all'internal auditor nello svolgimento del proprio incarico, minando di conseguenza la sussistenza delle condizioni di indipendenza e professionalità richiesti. Altro rischio è l'eccessivo affidamento che un revisore esterno possa fare sul lavoro svolto dall'internal auditor. A tal riguardo, occorre ricordare che il revisore legale dei conti rimane l'unico responsabile sull'*opinion* espressa, sull'attività di revisione svolta e quindi sulle circostanze e sulle evidenze che lo hanno condotto all'emanazione di un certo giudizio. Questa responsabilità, quindi, non può essere attenuata dal lavoro svolto dall'Internal Audit.

In sintesi, è importante che si verifichi una stretta collaborazione tra il soggetto che svolge attività di revisione esterna e gli internal auditors, però è altrettanto importante che le attività condivise e i punti di raccordo siano definiti minuziosamente e siano in grado di apportare valore all'audit, sfruttando le sinergie che, per naturale predisposizione, tali attività offrono. Ad esempio, l'attività di auditing interno svolta

su determinate aree aziendali legate a procedure di redazione del bilancio, se efficace, può comportare una corretta riduzione dell'ampiezza delle verifiche svolte dal revisore esterno o una rivisitazione delle aree di analisi. Infine, è opportuno che venga avviato tra i due soggetti un continuo scambio di flussi informativi su tutte le tematiche che possono influenzare l'operato di entrambi i soggetti. In tal senso, appare opportuno fissare incontri periodici e aumentarne la frequenza in prossimità delle fasi di *reporting* e di emissione di *opinion*<sup>83</sup>. In tali occasioni è indispensabile che vengano condivise informazioni riguardo:

- 1) L'ampiezza dell'attività (è fondamentale che vengano chiariti i singoli programmi di audit al fine di evitare le duplicazioni e di coprire ogni area aziendale);
- 2) Le tempistiche;
- 3) Il livello di dettaglio delle verifiche da svolgere;
- 4) La metodologia utilizzata (campionamento statistico, strumenti di analisi, ecc.);
- 5) La gestione delle carte di lavoro e il rispettivo accesso e utilizzo;
- 6) Le modalità di controllo ed emissione dei rapporti sull'attività svolta;
- 7) Lo scambio di rapporti di audit e *management letter*.

## **2.8. Conclusioni**

Alla luce di quanto evidenziato nelle pagine precedenti, si è fornita un'idea più chiara e complessa della funzione di Internal Audit. Infatti, mentre nel primo capitolo ci si è soffermati sulla natura della funzione, sui requisiti che deve possedere un internal auditor, sulle peculiarità che caratterizzano lo svolgimento di tale attività e sul ruolo di tale funzione nell'organigramma aziendale, nei più recenti paragrafi si è entrati in dettaglio nella trattazione concreta e reale dello svolgimento dell'attività di auditing. E al fine di raggiungere un simile risultato, si è reso indispensabile chiarire che tale attività non assume una posizione di estraneità rispetto alle altre funzioni di

---

<sup>83</sup> DITTMER C., *Internal Auditing: chiave per la corporate governance*, EGEA, 2011, pag. 132.

amministrazione e controllo, bensì si rende indispensabile alla loro corretta esecuzione e le completa.

Partendo da questa assunzione è lecito considerare la funzione di Internal Audit come una attività di supporto, benché indipendente, rispetto alla presa di decisioni strategiche in tema di Sistema di Controllo Interno, da un lato, e rispetto allo svolgimento delle attività del Collegio Sindacale, del Dirigente preposto e della società di revisione esterna, dall'altro. Tutto ciò è reso possibile soltanto attraverso la creazione di canali di trasmissione di informazioni tra le diverse funzioni e quindi attraverso la predisposizione, laddove non sia il legislatore a farlo, di procedure aziendali che prevedano incontri periodici tra le varie funzioni al fine di condividere i risultati ottenuti. Appare altresì necessario individuare con chiarezza le aree di competenza oggetto dei vari controlli al fine di limitare le situazioni di *over-auditing* e raggiungere una maggiore copertura sulle aree aziendali auditate.

## Capitolo Terzo

### **Le frodi aziendali: caratteristiche e modalità**

#### **3.1. Introduzione**

Nei capitoli precedenti è stato profondamente affrontato il tema dell'attività di revisione interna ed è stata affermata l'importanza della Funzione di Internal Audit nello sviluppo e nel miglioramento dell'intero sistema dei controlli aziendali. Partendo dal presupposto che il Sistema di Controllo Interno costituisce l'insieme delle strutture, dei ruoli e delle procedure il cui ruolo è quello di sostenere la crescita dell'impresa mediante un'efficace gestione dei rischi aziendali, va da sé che l'attenzione dell'Internal Audit sia rivolta verso tali dinamiche di rischio. Tra queste, assume rilievo il rischio di frode, il quale costituisce anch'esso oggetto di attenzione della Funzione di revisione interna per via dell'impatto che un evento fraudolento può provocare all'interno dell'Organizzazione. Il tema delle frodi, infatti, ha visto crescere notevolmente la sua importanza all'interno degli studi sulla corporate governance, specialmente a seguito dei principali scandali societari che si sono susseguiti agli inizi degli anni duemila. Infatti, le esperienze di Enron, Tyco, WorldCom, Parmalat, fino alla più recente Volkswagen, hanno via via condotto i legislatori nazionali e la letteratura manageriale verso un maggiore impegno ad analizzare e studiare tali comportamenti fraudolenti e, di conseguenza, migliorare le strutture aziendali atte a prevenire il compimento di questi reati.

Per avere un'idea più chiara circa il peso che le frodi aziendali hanno assunto e continuano ad assumere a livello mondiale, si riporta la seguente statistica relativa a una ricerca effettuata dall'*Association of Certified Fraud Examiners (ACFE)*: dal 2008 al 2009 in 106 Paesi emerge che le aziende abbiano subito danni per frode per un valore pari a circa il 5% del loro fatturato, con una perdita complessiva stimata attorno

ai 2,9 trilioni di dollari<sup>84</sup>. Se si considera che tale dato fa riferimento alle sole frodi che sono state portate alla luce durante quegli anni si può comprendere come questi numeri siano in realtà sottostimati. Ovviamente, il fenomeno delle frodi non nasce negli anni duemila ma sembra risalire ad epoche ben lontane, a partire dalla nascita delle prime forme di commercio nell'antichità. Tuttavia, oggi assistiamo a forme di frodi caratterizzate da una struttura di gran lunga più complessa rispetto a quelle del passato, e i cui impatti negativi sono altrettanto peggiori. È proprio per il suo aspetto ingegnoso e per la scarsa percezione del danno che essa produce che la frode ha assunto negli anni passati una luce diversa rispetto agli altri reati. Essa è stata troppo a lungo osservata con fascino e ammirazione dall'immaginario collettivo, ed è stata percepita come uno scontro tra intelligenze, dove l'attore della frode è sicuro di poter aggirare la vittima mediante la sua intelligenza e mediante un sofisticato schema di inganno, senza produrre un concreto atto di violenza nei confronti di costui, ma assicurando un profitto per sé o per altri<sup>85</sup>. Quanto appena esposto è stato inoltre confermato dal Presidente della *Commission on Law Enforcement and the Administration of Justice* che, nel 1968, dichiarava che l'opinione pubblica non solo era indifferente verso tali crimini, ma talvolta provava ammirazione verso chi li compieva<sup>86</sup>.

Sulla base di quanto appena affermato, si sostiene che le frodi a carattere economico e commerciale siano sempre esistite e che la percezione della diffusione del fenomeno negli anni recenti dipende piuttosto dalla maggiore attenzione che l'opinione pubblica ha rivolto verso tale reato. Appurato l'effetto pernicioso che il fenomeno produce nei confronti della società in generale e il contributo che la funzione di revisione interna può avere nella prevenzione e nella riduzione dei casi di frode, il presente capitolo fornirà un'esamina approfondita del tema, fornendo le definizioni principali e le strutture teoriche ad esso sottostanti, affrontando le discipline normative poste in essere per contrastarlo, fino ad arrivare a un'analisi più approfondita dell'attività di fraud auditing.

---

<sup>84</sup> POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali: forensic accounting, fraud auditing e litigation*, EGEA, 2012, pag. 2.

<sup>85</sup> ALLEGRINI M., D'ONZA G., MANCINI D., GARZELLA S., *Le frodi aziendali: frodi amministrative, alterazione di bilancio e computer crime*, Franco Angeli, 2007, pag. 9.

<sup>86</sup> President's Commission on Law Enforcement and Administration of Justice, *Challenge of Crime in a Free Society*, Washington, DC, U.S. Government Printing Office, 1968.

## 3.2. Definizione di frode e caratteristiche principali

### 3.2.1. Definizioni

Per poter giungere a una definizione generale di frode bisogna necessariamente compiere alcune distinzioni fondamentali in materia di criminologia. In primo luogo, potremmo interpretare la frode come un atto di appropriazione illecito con il quale si ottiene un vantaggio per sé o per altri. È dunque l'elemento dell'appropriazione che caratterizza tale fenomeno e che, quindi, allontana il reato di frode dalla fattispecie della "criminalità violenta". Infatti, ricollegandoci a quanto detto nel paragrafo introduttivo, la frode è stata vista in passato con "simpatia" proprio in virtù del fatto che viene meno il carattere violento, presente ad esempio nell'omicidio. All'interno della categoria dei reati appropriativi rientra la fattispecie del furto che comprende a sua volta il sottoinsieme delle frodi. Una definizione di frode può essere la seguente:

*Serie di comportamenti ingannevoli mediante i quali carpire la buona fede altrui allo scopo di appropriarsi illecitamente di ricchezza<sup>87</sup>.*

O ancora:

*Atto o comportamento diretto a ledere con l'inganno un altrui diritto<sup>88</sup>.*

Da un punto di vista giuridico il nostro ordinamento non fornisce una definizione chiara ed univoca di frode, limitandosi a chiarire la fattispecie del "contratto in frode alla legge", ossia di un contratto utilizzato per eludere fraudolentemente una norma imperativa. Sempre sul versante giuridico il codice penale, pur non fornendo un'esplicita definizione di frode, contempla la fattispecie della truffa, definendola come l'azione attraverso la quale uno o più soggetti, con artifici e raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno.

Riassumendo, la frode si configura come segue: l'attore (soggetto attivo), attraverso artifici e raggiri, induce in errore la vittima (soggetto passivo) e procura a sé stesso o

---

<sup>87</sup> POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali: forensic accounting, fraud auditing e litigation*, EGEA, 2012, pag. 4.

<sup>88</sup> [www.treccani.it](http://www.treccani.it)

ad altri un vantaggio ingiusto congiuntamente ad un altrettanto ingiusto danno per la vittima o per altri. Partendo da questa definizione, pienamente condivisa dai teorici, è possibile individuare gli elementi essenziali di ogni schema di frode (l'attore, la vittima, l'inganno, il beneficio ingiusto e il danno ingiusto), sintetizzabili nella figura che segue<sup>89</sup>:

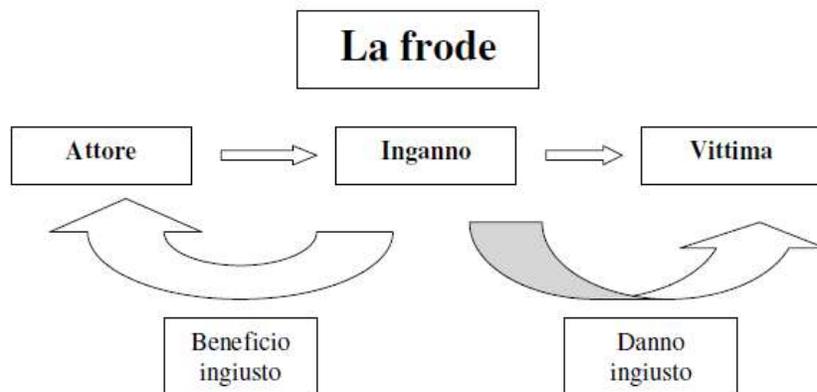


Figura 16 - Gli elementi fondamentali della frode

Le definizioni appena fornite sono tuttavia insufficienti ai fini di una circoscrizione del fenomeno in quanto, ai fini della nostra trattazione, si farà riferimento esclusivamente alle frodi di natura economica, cioè a tutti quei comportamenti illeciti con un contenuto economico e legati allo svolgimento di un'attività imprenditoriale o professionale. Si fa, cioè, riferimento a quelle pratiche criminali che la letteratura anglosassone ha definito generalmente con il termine *white collar crime*.

### 3.2.2. Caratteristiche generali dei *white collar crime*

L'espressione *white collar crime* fu coniata per la prima volta verso la fine degli anni Trenta da uno dei più noti criminologi statunitensi, Edwin Sutherland. L'idea di Sutherland era che soggetti "rispettabili" come i colletti bianchi, in virtù del ruolo che

<sup>89</sup> ALLEGRINI M., D'ONZA G., MANCINI D., GARZELLA S., *Le frodi aziendali: frodi amministrative, alterazione di bilancio e computer crime*, Franco Angeli, 2007, pag. 15.

rivestivano nella società e della fiducia che destavano verso gli altri, erano in grado facilmente di compiere atti illeciti di natura economica. In particolare, questo fenomeno fu descritto come una “realtà diffusa, quasi di massa, tra gli operatori e caratterizzato da elementi di raffinata professionalità e diffusa recidività”<sup>90</sup>.

Seppure furono oggetto di numerose critiche, le teorie di Sutherland ebbero il merito di fungere da catalizzatore per la nascita di un nuovo filone di studi incentrato sulle frodi aziendali. In particolare, ad oggi, la frode economica viene intesa come un comportamento deviante del normale atteggiamento posto in essere da tali operatori economici, il quale:

- Trae beneficio dallo schermo costituito dall’attività economica che viene svolta o dall’intera organizzazione, che rende il fatto illecito scarsamente percettibile agli occhi di terzi;
- Sfrutta il bagaglio di competenze tecniche posseduto da tali soggetti al fine di rendere l’inganno posto in essere un complesso e sofisticato insieme di azioni;
- Approfitta degli effetti (negativi) a lungo termine che la frode comporta per le vittime;
- In genere, la vittima non si identifica con un singolo soggetto ma verso una categoria sociale ovvero verso la comunità in generale e, in quanto tale, rende l’impatto di difficile misurazione a livello individuale.

Gli elementi che caratterizzano il reato sono quindi i seguenti:

- a) L’inganno: viene posta in essere una mistificazione della realtà attraverso la falsificazione, l’occultamento o la manipolazione degli atti e dei fatti;
- b) L’intenzionalità: il crimine economico va inteso come tale solo se si poggia su un complesso e premeditato disegno;
- c) La violazione del rapporto fiduciario: le relazioni economiche si fondano tendenzialmente su un rapporto di fiducia tra più soggetti. La chiave per la

---

<sup>90</sup> POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali: forensic accounting, fraud auditing e litigation*, EGEA, 2012, pag. 6.

commissione di tale reato economico è l'abbassamento delle difese dei soggetti lesi, che avviene violando il suddetto rapporto;

- d) Il danno: come si era detto in precedenza, lo schema della frode rientra nella fattispecie dei crimini appropriativi. Il vantaggio dell'attore è uguale e contrario al danno recato alle vittime;
- e) L'occultamento: è essenziale al fine di rendere l'azione fraudolenta "invisibile" agli occhi della vittima o del soggetto che esercita l'azione di vigilanza;
- f) La rispettabilità apparente: l'attore del reato gode di un rispetto derivante dalla posizione rivestita nella piramide sociale;
- g) La vittima: generalmente, la vittima è invisibile agli occhi di chi compie il reato, e l'assenza di coinvolgimento tra questi due soggetti giustifica, nella mente del frodatore, il compimento del reato. Infatti, questo viene visto dall'attore come un semplice atto elusivo delle normative vigenti.

### **3.2.3. Le ragioni alla base del comportamento fraudolento**

Quanto finora affermato è essenziale per la comprensione generale del fenomeno ma non è sufficiente al fine di arginarlo. Per tale motivo, si è fin da subito ritenuto opportuno scavare molto più a fondo e risalire alla radice del comportamento fraudolento, andando a scovare le cause che inducono alcuni soggetti al compimento di tali atti. Infatti, fin dal XIX secolo si sono susseguite una serie di teorie circa le motivazioni alla base dei criminali economici, gran parte delle quali è riconducibile al filone della "scelta razionale". Secondo tali teorie, i criminali sono esseri razionali e il loro scopo è quello di massimizzare il soddisfacimento dei propri bisogni e il proprio benessere. La valutazione dei vantaggi che i criminali razionali compiono si basa su tre elementi:

- a) La pressione per il raggiungimento degli obiettivi;
- b) La certezza e la severità delle sanzioni;
- c) La cultura volta all'accettazione e agevolazione di condotte criminali.

In sintesi, secondo tali teorie il compimento di un illecito parte da una razionale valutazione dei costi e dei benefici derivanti dall'illecito, e quindi "la condotta illegale trae origine dalla percepita convenienza a delinquere"<sup>91</sup>. Quanto affermato è stato oggetto di numerose critiche e altri studiosi hanno provato a fornire delle spiegazioni diverse rispetto alla più nota *economicità a delinquere*; il quadro complessivo che ad oggi emerge, circa le motivazioni di base alle frodi societarie è il seguente:

- La struttura della società capitalistica e i valori su cui essa si fonda;
- La cultura interna dell'impresa e le sue dinamiche;
- L'acquisizione di vantaggi ottenibili con il compimento del reato, superiori rispetto alle probabilità di essere scoperti e alla conseguente perdita;
- L'interesse diffuso all'emulazione, che complica l'accertamento;
- La fiducia riposta dalla società nei confronti degli attori del reato;

Il contributo più importante offerto in materia è riconducibile al criminologo Donald R. Cressey, che formulò le sue teorie più importanti verso la fine degli anni '50 sotto gli insegnamenti del sopraccitato Sutherland<sup>92</sup>. Lo studio condotto da Cressey si fonda su delle interviste poste a un campione di 200 persone, tutte accusate del reato di appropriazione illecita, da cui sono emerse le principali ragioni che conducono gli individui al compimento di illeciti. Nello specifico, la conclusione di Cressey fu che un individuo è spinto dal compiere un crimine economico solo se sono presenti contemporaneamente tre fattori:

- 1) Necessità di soddisfare bisogni (finanziari) percepiti e pressanti;
- 2) Consapevolezza di avere l'opportunità (percepita) di compiere e di occultare l'illecito;
- 3) Considerazione del proprio comportamento come atto non criminoso, definibile anche come razionalizzazione atta a rendere il comportamento come soggettivamente accettabile.

---

<sup>91</sup> POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali: forensic accounting, fraud auditing e litigation*, EGEA, 2012, pag. 13.

<sup>92</sup> CRESSEY D.R., *Other people's money: a study in the social psychology of embezzlement*, Tree Prees, Glencoe, Illinois, 1953.

Tale considerazione finale dell'autore è stata resa ancora più nota dalla rappresentazione grafica che ne è seguita: il triangolo della frode.



*Figura 17 - La piramide della frode*

Uno sviluppo di tale modello è stato fornito da Steven Albrecht quarant'anni dopo, il quale, attraverso dei fondi stanziati dall'Institute of Internal Auditors Research Foundation, riuscì ad analizzare 212 casi di frode, giungendo a delle evidenze molto simili a quelle di Cressey. In questo caso, i fattori alla base del fenomeno criminale sono i seguenti<sup>93</sup>:

- a) Situazione di pressione;
- b) L'opportunità a compiere la frode;
- c) Il livello di integrità dell'individuo.

La novità introdotta rispetto al modello precedente sta nel non ritenere necessaria una piena compresenza degli elementi indicati, quanto piuttosto misurare

---

<sup>93</sup> ALBRECHT W.S., HOWE K.R., ROMNEY M.B., *Detering fraud: the internal auditor's perspective*, Altomonte, 1984.

contemporaneamente il livello di ciascuno di essi, come rappresentato nella figura che segue:

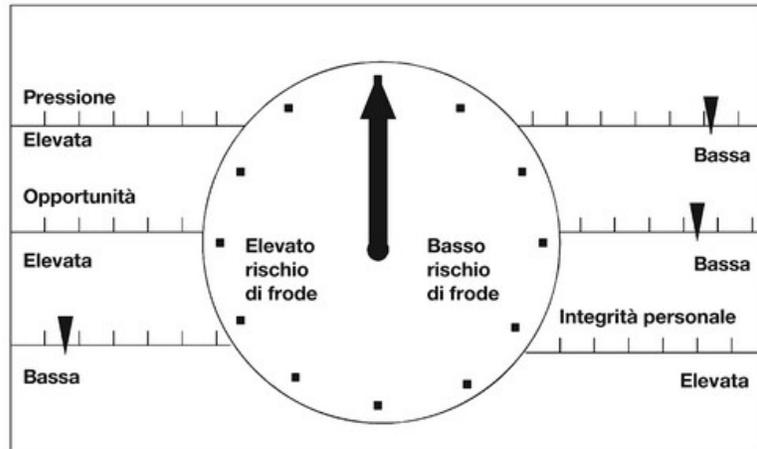
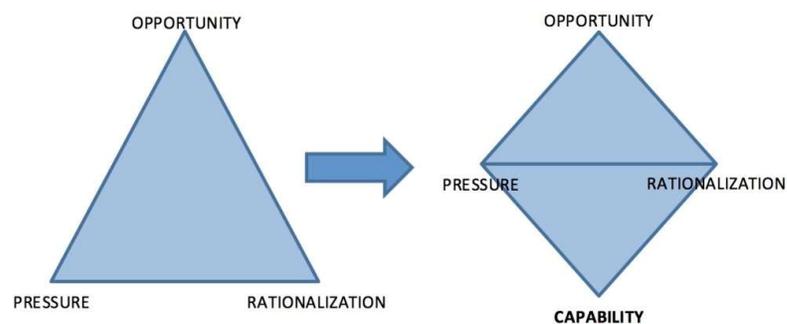


Figura 18 - La scala della frode

Per concludere, per completezza espositiva si riporta un ultimo “aggiornamento” della teoria della piramide della frode. Tale recente sviluppo è dovuto agli studi di David Wolfe e Dana Hermanson, i quali nel 2004 presentarono un’estensione del modello di Cressey, definita come teoria del diamante della frode. Questa teoria contempla un quarto elemento rispetto ai primi tre visti precedentemente, la capacità. In particolare, secondo Wolfe e Hermanson, fermo restando la funzionale coesistenza dei precedenti tre elementi ai fini del compimento della frode, l’atto criminale non può avvenire senza che l’attore possenga le dovute conoscenze e competenze professionali nel porlo in essere, specialmente per quelle frodi caratterizzate da un elevato tasso di complessità<sup>94</sup>.

<sup>94</sup> WOLFE D.T., HERMANSON D.R., *The Fraud Diamond: Considering the Four Elements of Fraud*, CPA Journal, 2004, pagg. 38-42.



*Figura 19 - Dalla Fraud Triangle Theory alla Fraud Diamond Theory*

In altri termini, se la “pressione percepita” e la “razionalizzazione” forniscono a un individuo la motivazione ad agire, la “capacità” è l’elemento che permette a tale soggetto di riconoscere “l’opportunità” che il compimento di un determinato illecito rappresenta, legata al vantaggio che ne consegue, e di porre in essere il reato.

### **3.3. Una rassegna delle principali forme di frodi aziendali**

Nelle pagine precedenti è stato introdotto il concetto di frode e ne sono stati posti in evidenza i tratti caratteristici, fornendo una chiara immagine dello schema concettuale della frode, i cui elementi essenziali sono l’attore, l’inganno, la vittima, il danno e il beneficio ingiusti. Inoltre, occorre ricordare che la frode rappresenta un fenomeno di natura economica, in quanto il danno (verso terzi) o il beneficio (verso sé) che essa produce è rappresentato dalla perdita finanziaria o reputazionale della vittima. Da questo schema, tuttavia, è possibile definire una serie numerosa di fattispecie fraudolente, le quali verranno riassunte e analizzate nel presente paragrafo, col fine di fornire un’idea concreta delle varie modalità con cui esso si realizza.

In primo luogo, occorre distinguere le frodi interne dalle frodi esterne. Le prime si manifestano all’interno del contesto organizzativo della società, dove i principali attori sono gli amministratori o i dipendenti della stessa. Le frodi esterne invece si

qualificano per la presenza esterna degli attori, i quali possono essere clienti o fornitori della società. Le frodi interne, tuttavia, rappresentano la casistica di frode più affascinante e sulla quale ci soffermeremo durante il prosieguo del presente lavoro. All'interno di questa categoria, infatti, è possibile distinguere tra *corporate fraud* e *white collar crime* a seconda se il soggetto che compie la frode è un amministratore (o l'intero consiglio) oppure un dipendente/agente della società. Altra distinzione va effettuata tra i reati di natura contabile (*on-the-book*) e quelli di natura extracontabile (*off-the-book*)<sup>95</sup>. Per frode extracontabile si fa in genere riferimento ad atti di corruzione, come un manager che favorisce un particolare fornitore verso cui ha uno o più interessi di natura personale, o magari intascando una tangente. La registrazione contabile di questa operazione può risultare corretta, mentre scorretto è il comportamento a monte dell'operazione. Diverso è il caso di frode *on-the-book*, la quale consiste nella scorretta rilevazione contabile di una data operazione ovvero, seppure la contabilizzazione risulta essere giusta, in un mancato rispetto delle normative interne circa il processo amministrativo-contabile della società.

Quanto appena detto illustra come le frodi sono in grado di assumere aspetti e connotazioni molto diversi tra loro, avendo in comune gli elementi chiave finora analizzati. Una ricerca condotta nel 2018 da PwC<sup>96</sup>, nota società di revisione e consulenza, ha elencato le principali forme attraverso cui tale reato si manifesta: appropriazione indebita, falso in bilancio, corruzione, infrazioni fiscali, aggio, insider trading e frode informatica. In particolare, dalla relazione si evince come meno del 50% delle società appartenenti al campione analizzato ha posto in essere delle attività di *specific risk assessment* con ad oggetto l'individuazione, l'analisi e la valutazione del rischio di frode all'interno della propria organizzazione.

---

<sup>95</sup> ALLEGRINI M., D'ONZA G., MANCINI D., GARZELLA S., *Le frodi aziendali: frodi amministrative, alterazione di bilancio e computer crime*, Franco Angeli, 2007, pag. 25.

<sup>96</sup> PWC, *Global Economic Crime and Fraud Survey 2018: Pulling Fraud Out of The Shadows*, 2018.

## Appropriazione indebita

Secondo il sondaggio effettuato da PwC, l'appropriazione indebita rappresenta la forma di reato societario maggiormente diffusa al mondo. Infatti, in quattro *industry* su cinque (*Consumer, Financial Services, Industrial Products, Professional Services, Technology*), essa risulta avere la percentuale maggiore in termini di accadimento, come raffigurato nella seguente immagine<sup>97</sup>.

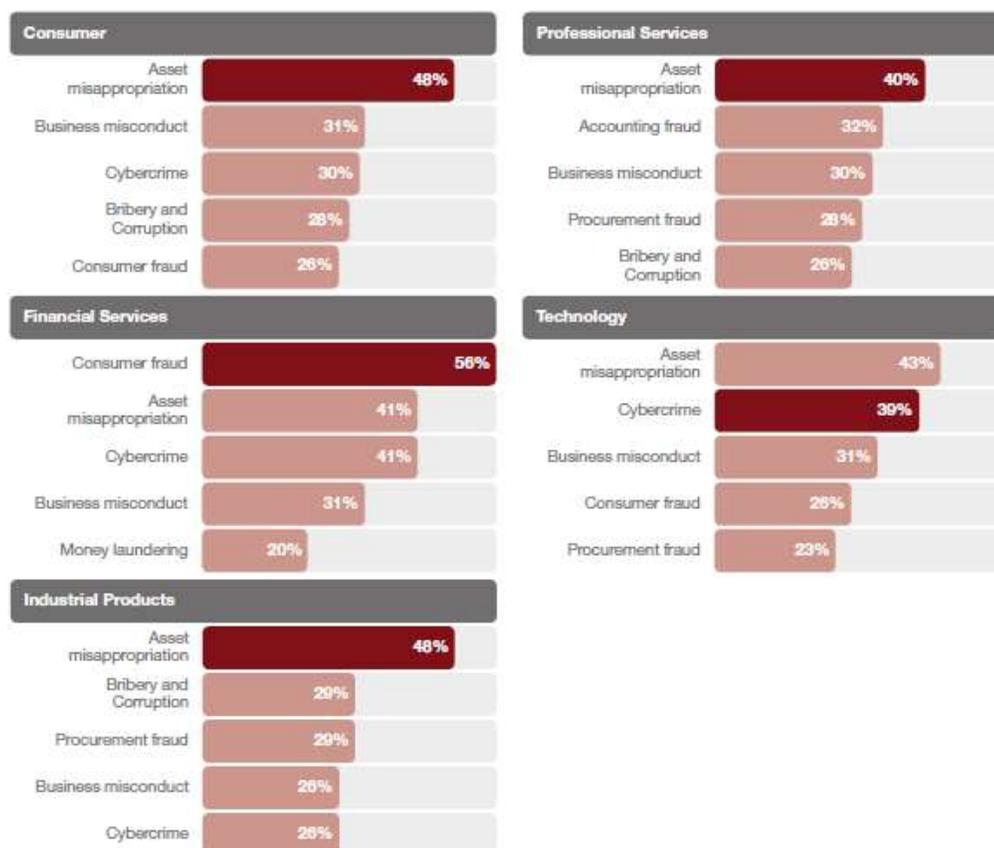


Figura 20 - Le principali forme di frodi aziendali

<sup>97</sup> PwC, *Global Economic Crime and Fraud Survey 2018: Pulling Fraud Out of The Shadows*, 2018, pag. 8.

Il reato di appropriazione indebita si realizza essenzialmente attraverso la sottrazione e la appropriazione illecita dei beni aziendali. Tali beni possono essere costituiti da denaro, beni aziendali materiali o proprietà intellettuali, scarti di produzione. Costituisce appropriazione indebita non soltanto il furto di tali beni, ma anche l'utilizzo improprio per fini personali o comunque estranei rispetto al regolare svolgimento dell'attività di impresa.

### *Frode contabile*

La frode contabile ha visto crescere il suo impatto mediatico specialmente a seguito dei fatti avvenuti negli anni duemila. Infatti, i casi Enron e Parmalat, su tutti, hanno mostrato le potenzialità negative di tali reati sull'immagine della società, con ciò che ne consegue, aumentando quindi l'attenzione della comunità in generale e incentivando l'intervento dei legislatori nazionali con norme atte a prevenire tali comportamenti. Volendo fornire una definizione della fattispecie specifica, possiamo definire frode contabile l'aggiramento della regolamentazione contabile e l'alterazione dei dati di bilancio con cui è possibile ottenere, in genere, un incremento dell'attivo contestualmente a un occultamento delle passività. Le motivazioni che spingono gli operatori al compimento di alterazioni dei dati contabile possono essere molteplici, ad esempio: la pressione esercitata dagli investitori, i conflitti di interesse tra proprietà e management, le scarse sanzioni (soprattutto in passato) istituite per punire gli attori di tali reati, la crescente complessità aziendale e il venir meno di una buona struttura di controllo e di governance. Tra le motivazioni a compiere una frode contabile rientra anche l'articolato sistema di incentivi legato all'attribuzione di quote societarie al top management aziendale. Con questa affermazione non si cerca di puntare il dito contro uno strumento di incentivazione come le *stock option*, quanto piuttosto far presente che la squilibrata composizione del pacchetto remunerativo del senior management può creare forti conflitti di interesse tra la "veritiera e corretta" rappresentazione delle poste in bilancio e la ricerca (forsennata) dell'aumento del valore di borsa delle azioni.

Le conseguenze delle frodi di natura contabile sono inoltre tra le più disastrose, sia in termini finanziari che reputazionali. Prendendo in considerazione il caso Enron, ad

esempio, la scoperta della frode societaria ha portato a un crollo del valore dei titoli di borsa della società, i quali sono passati da un valore che si aggirava attorno agli 80 dollari per azione ad un valore di 26 centesimi per azione, il tutto nel giro di qualche mese. Ancora, il danno maggiore che un simile evento può provocare va ricercato nella sfera reputazionale: il crollo delle azioni della Enron non solo ha obbligato la stessa a dichiarare fallimento nel Dicembre del 2001, ma ha riservato una sorte simile nei confronti della Arthur Andersen, la società di revisione a cui era stato conferito, a partire dall'esercizio 1987, l'incarico di audit.

### *Corruzione*

Il fenomeno della corruzione si manifesta quando un soggetto ottiene un beneficio indebito, per sé o (nella maggior parte dei casi) per altri (un ente o un gruppo di persone), a discapito di terzi, ricevendo in maniera disonesta un bene di valore. In questa forma di reato è ancora più marcato il venir meno della percezione dei danni che tale frode produce in capo a terzi, e di conseguenza il senso di responsabilità per l'illecito compiuto, e ciò ne favorisce la diffusione. Il reato di corruzione può essere distinto tra:

- a) Corruzione tramite tangenti, la quale consiste nell'offerta o donazione di un qualsiasi bene di valore che sia in grado di influenzare il giudizio del soggetto che, in genere, riceve la tangente;
- b) Corruzione tramite omaggi e regali, che si differenzia dalla corruzione per tangenti in quanto l'omaggio concesso, consistente in un bene di diversa natura, avviene a seguito del compimento dell'atto richiesto;
- c) Estorsione, la quale si distingue nettamente dalle prime due forme in quanto in essa l'opera di convincimento passa attraverso un atto violento o intimidatorio;

### *Infrazioni fiscali*

All'interno di questa fattispecie occorre far riferimento sia al reato di evasione fiscale, sia al reato di frode fiscale. L'evasione consiste in una violazione di una norma fiscale ai fini della sottrazione al pagamento di un tributo, e quindi alle conseguenze che derivano dall'applicazione di tale norma. Attraverso la frode fiscale, invece, non si verifica una palese violazione di norme, ma si ottiene un vantaggio fiscale indebito mediante l'utilizzo di artifici volti al solo fine di conseguire tale vantaggio, aggirando la *ratio* delle norme. Queste operazioni, per la loro complessità, sono molto più difficili da individuare e complicano la fase di accertamento dell'amministrazione finanziaria.

Le infrazioni fiscali rientrano senza ombra di dubbio nel novero delle frodi in quanto c'è la presenza di tutti gli elementi che caratterizzano il reato in questione. Infatti, seppur anche in questo caso il "danno" provocato non gravi su un unico soggetto, ma verso l'intera comunità, e quindi riduce la percezione dell'effetto e il senso di responsabilità dell'attore, c'è la netta presenza di un beneficio ingiusto ottenuto da uno o più soggetti mediante l'attuazione di un "inganno", costituito dal raggiramento della normativa fiscale.

### *Aggiotaggio*

Con il termine aggio si fa riferimento all'atto illecito attraverso il quale uno o più soggetti sono in grado di creare artificialmente una movimentazione del valore di titoli o merci, ottenendo per sé o per altri un vantaggio ingiusto. Una delle più note modalità attraverso cui tale illecito si realizza consiste nella diffusione di notizie false con le quali si ottiene, a seguito della variazione di valore di titoli o merci, un vantaggio indebito. Le modalità attraverso le quali si realizza tale divulgazione di notizie non assume importanza ai fini del compimento del reato, in quanto essa potrà avvenire sia attraverso il passaggio di informazioni in via confidenziale, sia attraverso comunicati ufficiali. Ciò che rileva ai fini del compimento della frode è la "cattiva fede" con la quale la notizia falsa viene riportata e il vantaggio indebito che ne consegue.

Oltre alla diffusione di notizie tra gli operatori di mercato, costituiscono aggio anche altre operazioni il cui fine rimane pressoché lo stesso, cambiando il mezzo attraverso il quale esso si realizza. Ad esempio, lo scambio simulato di titolo (in quantità elevate) tra operatori di mercato, dove più operatori si accordano affinché tale scambio sia reso pubblico “su carta” ma senza che si realizzi concretamente, è in grado di dare l’immagine di un mercato “attivo”, manipolando o influenzando il comportamento di altri operatori.

### *Insider trading*

Introdotta nell’ordinamento italiano con la legge n. 157/1991, l’insider trading è il reato che indica l’abuso di informazioni privilegiate<sup>98</sup>. In particolare, la disciplina ad esso dedicata ha l’obiettivo di reprimere “il compimento di operazioni su strumenti finanziari mediante informazioni privilegiate possedute in ragione della partecipazione al capitale di una società e dell’esercizio di una funzione pubblica o di una professione”. In particolare, affinché il reato si configuri è necessario che l’agente utilizzi direttamente l’informazione ottenuta in virtù di un rapporto sopramenzionato con una particolare istituzione, o la comunichi a terzi al di fuori del normale svolgimento della propria attività o professione. Ad esempio, la segnalazione a un soggetto terzo dell’acquisto di determinate azioni sulla base di informazioni in proprio possesso derivanti da un rapporto professionale che lega l’attore all’emittente, costituisce forma di reato e rientra perfettamente nella fattispecie dell’insider trading.

Inoltre, il Testo Unico della Finanza mira a precisare il concetto di informazione privilegiata, che viene descritto come segue<sup>99</sup>: “informazione di carattere preciso, non ancora resa pubblica, concernente, direttamente o indirettamente, uno o più emittenti strumenti finanziari o uno o più strumenti finanziari, che se resa pubblica potrebbe influire in modo sensibile sui prezzi dei predetti strumenti”.

---

<sup>98</sup> [www.treccani.it](http://www.treccani.it)

<sup>99</sup> Art. 181, D.Lgs. n.58/1998, *Testo Unico della Finanza*, CONSOB.

Nonostante anche nell'insider trading assuma rilevanza la gestione delle informazioni, il reato di insider trading si differenzia dall'aggiotaggio in quanto, mentre nell'insider trading le informazioni sono realmente possedute dal soggetto, che ne è in possesso mediante l'esistenza di canali preferenziali, come un rapporto professionale intrattenuto con l'emittente (es. di revisione, di consulenza, ecc.); nel caso di aggiotaggio l'informativa che viene diffusa non trova alcun fondamento nei rapporti che l'attore del reato intrattiene con altre istituzioni, né ha rilevanza la sua veridicità, quanto piuttosto l'obiettivo di influenzare le decisioni di altri operatori di mercato<sup>100</sup>.

### *Cybercrime*

Nella figura 5, precedentemente mostrata, è possibile notare come il reato informatico costituisca una delle principali forme di illecito, soprattutto nel settore tecnologico. In particolare, va detto che con l'avvento delle nuove tecnologie all'interno delle organizzazioni questa forma di crimine ha trovato ampia diffusione e aumenta a mano a mano l'attenzione verso forme di prevenzione e sistemi aziendali di controllo per la riduzione del rischio di frodi informatiche. Per frode informatica si intende quel comportamento per cui "chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico e telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno"<sup>101</sup>.

I crimini di natura informatica, secondo gli esperti, costituiranno in futuro le principali forme di reato verso cui una società dovrà difendersi, sia per il sempre crescente numero dei casi, sia per la sensibilità che i dati, gestiti tramite apparecchiature informatiche ed elettroniche, costituiscono per la società.

---

<sup>100</sup> [www.solofinanza.it](http://www.solofinanza.it)

<sup>101</sup> [www.treccani.it](http://www.treccani.it)

### **3.4. Richiami normativi in materia di frodi**

Attraverso la preliminare analisi fin qui compiuta è emerso come le frodi siano sempre esistite e si siano manifestate in tipologie e grado differenti. Inoltre, si è precisato come la frode segua uno schema ricorrente che nelle mente umana crea i presupposti affinché ci siano gli incentivi a commettere un simile reato e si è visto che all'interno delle organizzazioni tale fenomeno sia presente con maggiore frequenza. Tuttavia, come si è più volte ripetuto all'interno di questo testo, nonostante gli studiosi non abbiano tardato nell'affrontare il fenomeno già nei decenni passati, lo stesso non è accaduto in ambito normativo. Infatti, sembra che gli ordinamenti legislativi nazionali abbiano avuto bisogno di determinati stimoli, come lo scandalo Enron negli Stati Uniti o il caso Parmalat in Italia e in Europa, al fine di cominciare a considerare seriamente il fenomeno e quindi a fornire gli strumenti normativi necessari atti a prevenirlo.

Quello che segue è un breve richiamo alle forme attraverso cui il legislatore, nazionale e non, ha normato la disciplina delle frodi societarie al fine di prevenirne il compimento.

#### **3.4.1. Il Sarbanes-Oxley Act come risposta americana ai *Corporate Scandals***

Nel capitolo precedente, si è accennato al reato di frode contabile come uno dei più frequenti all'interno delle organizzazioni aziendali. Senz'altro esso rappresenta la forma di reato che più di ogni altra ha dato avvio a quel processo di legiferazione in materia da cui, tra le varie, è nata la normativa antifrode definita Sarbanes-Oxley Act o, più brevemente, "SOX"<sup>102</sup>. L'obiettivo di questo mutamento normativo era principalmente quello di porre in risalto il tema della corporate governance, migliorando il sistema dei controlli societari, attribuendo maggiori responsabilità ai diversi attori sociali e tutelando, quanto più possibile, non soltanto gli interessi degli azionisti ma di tutti gli stakeholder aziendali, tra cui le banche, i fornitori e i partner commerciali, i clienti, le autorità di vigilanza e i dipendenti aziendali.

---

<sup>102</sup> SARBANES OXLEY ACT, Public Law 107-204, 30 Luglio 2002, USA.

In accordo con quanto appena detto, possiamo definitivamente affermare che lo scandalo Enron del 2001 e WorldCom del 2002 hanno senz'altro evidenziato i limiti del sistema di governance americano, oltre che del sistema capitalistico in generale spingendo il legislatore statunitense ad approvare, nel 2002, il Sarbanes-Oxley Act. Il merito più evidente di tale normativa fu quello di attribuire piena responsabilità ai funzionari aziendali, in particolare ai vertici societari, circa le false dichiarazioni finanziarie riportate dalla società. Gli altri elementi fondanti sono<sup>103</sup>:

- *Indipendenza della società di revisione contabile e la vigilanza sul suo operato.* In primo luogo, il comportamento della Arthur Andersen, società di revisione incaricata di revisionare i bilanci della Enron, rappresentò una lezione appresa davanti alla quale il legislatore non poté restare impassibile. A tal riguardo, la SOX impone la creazione di un organismo pubblico di vigilanza (Public Company Accounting Oversight Board) con funzioni di controllo e di regolamentazione circa lo svolgimento delle attività di revisione contabile. In questo modo ottenne una maggiore regolamentazione dell'attività di audit tra i quali interventi va segnalato l'obbligo di rotazione delle figure chiave incaricate della revisione e il divieto di svolgere incarichi di consulenza presso società di cui si revisionano i bilanci. Entrambi questi interventi hanno come fine ultimo quello di ridurre al minimo potenziali conflitti di interesse e di aumentare l'indipendenza dei revisori.
- *Maggiore attendibilità delle informazioni finanziarie e dei processi di controllo interno contabile.* A tal riguardo, la SOX ha attribuito primaria responsabilità circa i processi informativi che hanno ad oggetto dati contabili e finanziari e il Sistema di Controllo Interno all'Amministratore Delegato e al Direttore Finanziario della società. CEO e CFO dovranno, da un lato, sovrintendere alla corretta gestione dei flussi informativi, in particolare quelli verso l'esterno, e, dall'altro, garantire l'implementazione di un Sistema dei Controlli che sia in grado di valutare la corretta predisposizione e funzionamento dei processi aziendali, tra cui quelli di natura amministrativo-contabile. Nello specifico, al fine di garantire la correttezza dei dati finanziari

---

<sup>103</sup> DITTMIEIER C., *Internal Auditing: chiave per la corporate governance*, EGEA, 2011, pag. 39.

aziendali e quindi prevenire le frodi di natura contabile, la disciplina ha previsto nella Section 302 che tali soggetti attestino, costituendosi come responsabili, la veridicità del bilancio annuale e delle relazioni finanziarie. Ancora, si richiede che essi valutino con cadenza periodica l'efficacia e l'efficienza del Sistema di Controllo Interno e del processo di redazione del bilancio, comunicando i risultati nel bilancio stesso e nelle relazioni emesse (Section 404). Infine, viene attribuito alla Società di revisione il dovere di esprimere un parere circa l'efficacia del Sistema di Controllo Interno nel processo di valutazione del processo contabile della società.

- *Attribuzione di maggiori poteri di regolamentazione e vigilanza alla Security Exchange Commission (SEC).* La SEC rappresenta l'organo federale statunitense preposto alla vigilanza dei mercati di borsa e può quindi essere equiparato alla "nostra" CONSOB. L'introduzione della SOX ha attribuito alla Security Exchange Commission ulteriori poteri e responsabilità, tra cui l'obbligo di supervisione dell'organismo di vigilanza pubblico delle società di revisione (Public Company Accounting Oversight Board). Inoltre, le è stato richiesto di regolamentare l'attività di redazione del bilancio di esercizio e dei report finanziari, affinché tali informazioni rispecchino la reale situazione economico-finanziaria della società e contengano anche quelle operazioni definite come "fuori-bilancio", che incidono sugli equilibri finanziari della società ma che in passato non facevano parte dell'informativa societaria. Infine, alla SEC è stato attribuito il compito di disciplinare il settore borsistico e delle società di rating, al fine di ridurre gli interessi di questi ultimi nel fornire valutazioni divergenti dal reale valore accertato delle società oggetto di analisi.

Il mancato rispetto di questi elementi comporta delle sanzioni penali e amministrative molto severe. Ad esempio, in merito alla manipolazione e alla falsificazione dei dati economico-finanziari e di bilancio, il CEO e il CFO che abbiano, attraverso la documentazione prodotta e rilasciata, fornito informazioni false rischiano la reclusione fino a venti anni e una multa fino a cinque milioni di dollari. In questo modo la SOX mira a disincentivare il compimento di operazioni fraudolente, aumentando notevolmente il peso delle sanzioni nel caso in cui la frode venisse scoperta e quindi

l'impegno del top management affinché l'informativa societaria sia corretta e rispecchi fedelmente la situazione economico-finanziaria aziendale.

Per concludere, è possibile affermare che la SOX segue in un certo senso la disciplina contenuta all'interno del "nostro" D.Lgs. 231/2001. Infatti, la normativa statunitense del 2002 mira alla creazione di un sistema di controllo quale indicatore dell'effettivo impegno dei vertici societari nell'evitare situazioni di frodi contabili. Come nella 231, i dirigenti della società devono esercitare un potere di vigilanza sul corretto svolgimento dei controlli aziendali e la cui implementazione costituirebbe una prova dell'effettivo impegno dei vertici affinché l'informativa di bilancio sia veritiera e corretta.

#### **3.4.2. La legge sulla tutela del risparmio: la "SOX italiana"**

È stato detto che il Sarbanes-Oxley Act rappresenta una risposta del legislatore americano rispetto ai principali scandali che hanno avuto ad oggetto alcune tra le più grandi società statunitensi. Allo stesso modo, anche in Italia non sono mancati casi di frode societaria che hanno destato l'attenzione dei principali studiosi di corporate governance nonché dei legislatori nazionali. Questi ultimi, infatti, a seguito delle vicende che hanno riguardato aziende come Cirio e Parmalat, quest'ultima reputata come il maggior scandalo economico italiano, hanno sentito l'esigenza di formulare una disciplina normativa in tema di informativa contabile e controlli aziendali, col fine di prevenire reati di frode contabile e punire i responsabili di tali fattispecie fraudolenta.

La Legge 28 Dicembre 2005 n. 262<sup>104</sup>, dal titolo "Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari" e brevemente detta Legge sul Risparmio ha profondamente innovato l'ordinamento normativo in materia di

---

<sup>104</sup> Legge n. 262/2005, Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari, 28 Dicembre 2005.

corporate governance e controlli societari, oltre a rappresentare, di fatto, la risposta italiana alla SOX<sup>105</sup>. Tra i temi fondamentali, la Legge sul Risparmio ha previsto:

- La responsabilità personale di alcuni attori aziendali in merito alla veridicità dei documenti contabili e delle relazioni finanziarie;
- L'introduzione della figura del Dirigente preposto alla redazione dei documenti contabili societari, il cui compito principale è quello di istituire e sovrintendere l'intero processo amministrativo-contabile e di redazione del bilancio di esercizio;
- La modifica della disciplina della revisione esterna, con particolare riguardo a temi come il conflitto di interessi e l'indipendenza dei revisori.

Da una prima lettura dei punti appena elencati, è possibile notare la somiglianza tra la disciplina italiana e la sua fonte di ispirazione statunitense, tuttavia, emergono fin da subito alcune differenze. In primo luogo, è possibile notare come nonostante in entrambi i casi si cerchi di attribuire responsabilità personali in materia di predisposizione e vigilanza dell'intero processo amministrativo-contabile, nella SOX tale responsabilità va ricercata nelle persone dell'amministratore delegato e del direttore finanziario, mentre nella Legge sul Risparmio del 2005 viene istituita una nuova figura, il Dirigente preposto, cui spetta tale funzione. Altra differenza tra le due normative è data dalla maggiore chiarezza con la quale ci si riferisce al Sistema di Controllo Interno. Infatti, la SOX fa esplicito rinvio al Framework internazionale costituito, per l'appunto, dal CoSO Report, mentre la disciplina italiana manca di esaustività nell'indicare il Sistema di Controllo Interno. Nonostante ciò, in entrambi i casi si afferma il ruolo dell'organo esecutivo nel sovrintendere all'intero sistema e, di conseguenza, nel verificare periodicamente la sua efficacia e il suo corretto funzionamento.

Con riguardo alle responsabilità verso cui può incorrere il Dirigente preposto, va detto che a tale figura si estendono anche quelle che tipicamente spettano agli amministratori. Infatti, l'art. 154 – bis del Testo Unico della Finanza recita “le

---

<sup>105</sup> DITTMIEIER C., *Internal Auditing: chiave per la corporate governance*, EGEA, 2011, pag. 67.

disposizioni che regolano la responsabilità degli amministratori si applicano anche ai dirigenti preposti alla redazione dei documenti contabili societari...”

A titolo esaustivo, va aggiunto che tale responsabilità non sostituisce quella degli amministratori, ma vi si aggiunge, inasprendo obbiettivamente la normativa, chiarendo i ruoli e disincentivando gli illeciti in materia di informativa finanziaria e di bilancio.

### **3.4.3. Il D.Lgs. 231/2001**

Nonostante le normative fin qui introdotte abbiano rappresentato una vera e propria risposta alle vicende, più volte citate, che si sono susseguite attorno agli anni duemila, l’ordinamento italiano si era già dotato, in quegli anni, di una norma atta a prevenire e disincentivare il compimento degli illeciti economici. Il riconoscimento della necessità di affrontare il problema delle frodi aziendali è arrivato infatti in anticipo rispetto al caso Parmalat e l’obiettivo che si intendeva raggiungere era quello di scoraggiare gli illeciti aziendali non soltanto colpendo le persone fisiche responsabili, ma estendendo tale responsabilità alle imprese che non si fossero dotate di appositi sistemi di controllo al fine di prevenirli.

In particolare, il D.Lgs. 231/2001 ha ad oggetto la responsabilità amministrativa delle società e degli enti, la quale mira a disincentivare il compimento di reati, quindi riconducibili alla sfera penale, al fine di favorire in modo ingiusto le organizzazioni aziendali. A tal riguardo è necessario chiarire che nonostante la disciplina parli di responsabilità “amministrativa”, essa si costituisce solo formalmente come tale, in quanto può emergere solo se determinati soggetti, come si vedrà più avanti, commettono reati (sfera penale) al fine di procurare un vantaggio ingiusto alla società. Questa peculiarità è determinata dal fatto che le aziende non possono, secondo il nostro ordinamento, essere soggette a responsabilità penale poiché questa colpisce solamente le persone fisiche<sup>106</sup>. Inoltre, seppure in passato un soggetto aziendale avesse compiuto un illecito al fine di favorire una società, la responsabilità penale di

---

<sup>106</sup> Art. 27 C.1, Cost.

questo non si sarebbe estesa alla società beneficiaria dell'indebito vantaggio secondo il principio per cui *societas delinquere non potest*.

La portata innovativa del decreto va ricercata proprio in questo aspetto: con l'introduzione del concetto di responsabilità amministrativa dell'ente, l'intera organizzazione è maggiormente coinvolta nell'individuazione e prevenzione delle frodi societarie, al fine di evitare le conseguenze (sanzioni pecuniarie, sanzioni interdittive, ecc.) che derivano dall'applicazione della norma. Tale coinvolgimento è riscontrabile nella emersione di un Modello Organizzativo efficace e che permetta una piena diffusione dei valori etici e del controllo all'interno dell'organizzazione aziendale.

Entrando in dettaglio con quanto afferma il decreto, la responsabilità amministrativa colpisce gli enti forniti di personalità giuridica e le società/associazioni anche prive di personalità giuridica. Mentre rimangono esclusi i seguenti soggetti: Stato, enti pubblici territoriali, enti pubblici non economici, enti che svolgono funzioni di rilievo costituzionale e imprese individuali. Bisogna tuttavia fare attenzione a distinguere la natura del bene o servizio offerto dall'organizzazione con la natura giuridica dell'ente stesso. Infatti, l'illecito compiuto da un dirigente di una società controllata da un ente pubblico, estende comunque la responsabilità (amministrativa) in capo alla società stessa, che nonostante la natura pubblica del servizio offerto si configura giuridicamente come un'azienda. Inoltre, la società o l'ente si considera responsabile se e solo se abbia un interesse o un vantaggio nel compimento dell'illecito.

Non tutte le forme di reato contemplate nel nostro ordinamento comportano l'emersione della responsabilità amministrativa dell'ente. Infatti, l'ente è responsabile amministrativamente solo per i reati compiuti da soggetti persone fisiche, nell'interesse o a vantaggio della società, tassativamente previsti dalla disciplina, che sono:

- Delitti contro la pubblica amministrazione (corruzione, truffa allo stato, ecc.) o contro la fede pubblica (falsità in monete, in carte di pubblico credito, ecc.);
- Reati societari (false comunicazioni, falso in bilancio, illecita influenza sull'assemblea, ecc.);

- Delitti in materia di terrorismo e di eversione dell'ordine democratico;
- Delitti contro la personalità individuale;
- Abusi di mercato;
- Pratiche di mutilazione degli organi genitali femminili;
- Reati transazionali (associazione a delinquere, contrabbando di tabacchi lavorati esteri, traffico di stupefacenti, ecc.);
- Omicidio colposo e lesioni gravi o gravissime, commessi con violazione delle norme;
- Reati di ricettazione, riciclaggio o impiego di denaro o beni di provenienza illecità;
- Delitti informatici;
- Reati ambientali;
- Ecc.<sup>107</sup>

Come accennato nelle righe precedenti, al fine di non incorrere in responsabilità amministrativa l'ente dovrà dimostrare che:

- 1) È stato adottato ed efficacemente attuato un Modello di Organizzazione, Gestione e Controllo (MOG) idoneo a prevenire le fattispecie di reato previste dall'ordinamento;
- 2) È stato costituito un Organismo di Vigilanza, dotato di autonomi poteri di iniziativa e controllo, a cui spetta il ruolo di vigilare sul corretto funzionamento del MOG;
- 3) I soggetti hanno compiuto il reato hanno eludendo fraudolentemente il Modello;
- 4) Non vi sia stata omessa e insufficiente vigilanza da parte dell'Organismo di Vigilanza.

La società, e in particolare il top management aziendale, dovrà quindi adoperarsi al fine di realizzare un efficace ed efficiente sistema di controllo interno al fine di individuare e prevenire il compimento dei reati tassativamente previsti dalla normativa. Tuttavia, la normativa non indica le modalità con cui viene realizzato il

---

<sup>107</sup> [www.portale231.com](http://www.portale231.com)

Modello Organizzativo ma lascia che siano le associazioni di categoria, come Confindustria, a redigere delle Linee Guida per la sua realizzazione<sup>108</sup>. Quindi, la costituzione di un simile sistema di prevenzione passa necessariamente attraverso specifiche fasi, che possono essere così delineate:

- 1) Rilevare e mappare i processi e le strutture aziendali maggiormente a rischio;
- 2) Rilevare e valutare le procedure a rischio all'interno di ciascuna area individuata;
- 3) Individuare i rischi potenziali (fattispecie di reato e modalità di commissione);
- 4) Aggiornare (o predisporre *ex novo*) il sistema di prevenzione, con l'obiettivo di ridurre ad un livello accettabile i rischi identificati, il codice etico e i modelli di organizzazione e gestione;
- 5) Integrare tale sistema nel più generale Sistema di Controllo Interno, attivando idonei meccanismi di sorveglianza sul Sistema.

Inoltre, un efficiente sistema di prevenzione deve prevedere:

- *Il codice etico di condotta antifrode e anticorruzione*, cioè un documento al cui interno sono contenuti tutti i comportamenti che le persone all'interno dell'azienda o che con essa entrano in contatto dovrebbero avere al fine di prevenire qualsiasi forma di illecito. Questi codici possono inoltre essere inclusi nel più ampio Codice Etico della società ed hanno l'obiettivo di diffondere la cultura etica all'interno dell'Organizzazione aziendale, aumentare la conoscenza delle persone sulle politiche in campo etico intraprese dalla società e sostenere la reputazione dell'impresa.
- *Un Modello di Organizzazione e Gestione* che permetta di individuare le attività caratterizzate da un maggiore livello di rischio-reato; che preveda una serie di specifici protocolli per la programmazione e l'attuazione delle decisioni dell'ente in merito alla prevenzione delle frodi; che preveda specifiche procedure per la gestione delle risorse finanziarie, in modo da evitare il compimento di illeciti; che disponga appositi canali di trasmissione

---

<sup>108</sup> DITTMEIER C., *Internal Auditing: chiave per la corporate governance*, EGEA, Milano, 2008, pag. 60.

delle informazioni verso l'organo deputato all'osservanza del Modello stesso; che preveda sanzioni interne nei confronti dei soggetti che violano il Modello.

- *Il manuale delle procedure di attuazione del Modello*, che contiene le procedure e i processi che andranno messi in atto per l'attuazione di quanto disposto nel Modello, come la predisposizione di specifici strumenti per il monitoraggio del contesto esterno, e quindi del livello di rischio complessivo, o la previsione di un apposito sistema di reporting alla Direzione.

Alla luce di quanto finora esposto, è possibile affermare che l'impatto della legge 231 è stato notevole in termini di incentivo alle imprese nella messa in atto di attività di gestione dei rischi di reato e di prevenzione e individuazione delle frodi societarie. Infatti, con essa molte grandi organizzazioni hanno dovuto affrontare il tema della gestione di tali rischi, implementando apposite strutture di governance e migliorando il Sistema di Controllo Interno nel suo complesso. In conclusione, l'implementazione dei controlli fin qui discussi ha permesso alle aziende di evitare il rischio di incorrere in sanzioni, derivanti dall'applicazione della normativa sulla responsabilità amministrativa, disincentivare le pratiche corruttive all'interno dell'organizzazione, migliorare la reputazione aziendale e di conseguenza l'*appeal* dell'impresa in termini competitivi, conservare il valore del patrimonio aziendale.

### **3.5. L'attività di Fraud Auditing**

Nelle pagine precedenti è stata illustrata la dinamica mediante la quale si realizza uno schema di frode e si è più volte accennato agli effetti che un simile reato può avere nei confronti delle organizzazioni. In particolare, è stato visto come la frode possa essere causa, da un lato, dell'appropriazione da parte di uno o più soggetti di un indebito vantaggio, ma soprattutto possa causare, dall'altro lato, la perdita di valore nei confronti di un gruppo di soggetti e il venir meno della credibilità e della reputazione dell'azienda. In passato il concetto di frode aziendale è stato spesso equiparato alla categoria più specifica, come trattato precedentemente, del reato di frode contabile. Per tale ragione, si pensava che la figura più idonea alla sua prevenzione ed

individuazione fosse il revisore legale esterno o la società di revisione. Tuttavia, in virtù del fatto che le frodi societarie non si limitano alla sola categoria dei reati di natura contabile, ove la contabilità rappresenta l'oggetto di attenzione delle società di revisione, ne discende che la valutazione di queste figure professionali non sia esauriente ai fini dell'accertamento di un basso livello del rischio di frode. Inoltre, come afferma il Principio di Revisione ISA 200<sup>109</sup>, l'attività di revisione contabile è volta a "acquisire ogni elemento necessario per consentire al revisore di esprimere un giudizio se il bilancio sia redatto, in tutti gli aspetti significativi, in conformità al quadro normativo di riferimento", venendo meno quindi l'attività di ricerca specifica di comportamenti fraudolenti con cui i *preparer* alterano i valori iscritti in bilancio. In sintesi, il revisore contabile non sembra essere la figura più adatta allo svolgimento dell'attività di prevenzione ed individuazione delle frodi aziendali in quanto egli guarda al solo bilancio e lo fa nell'ottica di fornire un'assurance sulla ragionevole attendibilità dello stesso.

La funzione di Internal Audit, invece, rivolgendosi nella sua analisi al più ampio Sistema dei Controlli aziendali, sembra essere la figura più idonea allo svolgimento di attività di *fraud prevention and detection*. Infatti, siccome il fenomeno delle frodi aziendali rappresenta un importante canale di sottrazione del valore prodotto dall'impresa, una delle principali attività che i revisori interni dovrebbero eseguire è rappresentata appunto dal Fraud Auditing. Come si è detto, ogni frode aziendale è rappresentata dall'aggiramento del sistema dei controlli interni o dallo sfruttamento di debolezze di tale sistema attraverso cui si attenta al patrimonio della società, e l'Internal Audit costituisce la funzione cui spetta fornire un'assurance sulla corretta predisposizione ed attuazione dei controlli. Ovviamente, partendo dal presupposto che per un internal auditor non sia possibile eliminare completamente il rischio di frode, scovando ogni possibile comportamento illecito, è comunque auspicabile che attraverso un'attenta analisi sull'adeguatezza del Sistema di Controllo Interno, si possa

---

<sup>109</sup> INTERNATIONAL AUDITING AND ASSURANCE STANDARDS BOARD (IAASB), *Principio di Revisione Internazionale (ISA Italia) 200*, 2010.

fornire una maggiore garanzia affinché la frode non avvenga<sup>110</sup>. A tal riguardo, il fraud auditing si può suddividere in tre tipologie di attività:

- 1) Auditing per il rafforzamento del sistema di controllo preventivo;
- 2) Auditing di tipo ispettivo per l'individuazione di atti sospetti;
- 3) Investigazione di gravi sospetti di atti illeciti al fine di determinare le responsabilità e i danni subiti.

In merito alla prima forma di fraud auditing, è chiaro come essa si svolga in via assolutamente preventiva al fine di ottenere un complessivo livello di assurance sul rischio di frode intrinseco nei processi aziendali. Infatti, l'attività si svolge nelle modalità dell'*operational audit* ed ha l'obiettivo di individuare le aree grigie aziendali dove è maggiore la probabilità che si realizzi un caso di frode. L'individuazione dei rischi di frode e la loro successiva valutazione sono propedeutici al miglioramento del sistema dei controlli attraverso la predisposizione di azioni correttive dei sistemi esistenti e l'implementazione di nuove procedure.

Oltre all'attività di analisi e valutazione del rischio di frode, l'Internal Audit può svolgere, al fine di identificare e prevenire il compimento di illeciti, un monitoraggio sui cosiddetti *red flag*. I red flag, o segnali di allarme, rappresentano segnali di possibili azioni fraudolente che possono emergere ad ogni livello del controllo e da cui è possibile partire per valutare se occorre approfondire o meno l'anomalia rilevata. I red flag sono numerosi e si distinguono per caratteristiche o genere. Ad esempio, se a una gara per l'aggiudicazione di un appalto vi partecipino un numero eccessivamente ridotto di società, questo potrebbe rappresentare un segnale di allarme. Oppure, qualora una procedura generalmente utilizzata subisca notevoli variazioni a seguito di un numero consistente di deroghe, essa potrebbe indicare un possibile punto di debolezza del sistema o un'attività di manipolazione da parte del *process owner*.

Infine, l'attività di fraud auditing entra nel vivo qualora vi siano gravi sospetti circa il compimento di atti illeciti. In tal caso, è richiesta all'auditor una conoscenza delle

---

<sup>110</sup> DITTMER C., *Internal Auditing: chiave per la corporate governance*, EGEA, Milano, 2008, pag. 260.

diverse forme di frode, dei modi attraverso i quali esse vengono commesse e dei red flag che ne segnalino l'esistenza<sup>111</sup>. In materia di competenza degli internal auditor, gli standard internazionali prevedono che essi posseggano le competenze necessarie ai fini della valutazione del rischio di frode e delle modalità con cui un'organizzazione è in grado di gestirli<sup>112</sup>. Tuttavia, chiariscono gli standard, non è richiesto che tali competenze siano parificate a quelle possedute da chi svolga, come responsabilità primaria, il ruolo di *fraud investigator*. In ogni caso, qualora venga identificato un possibile caso di frode, viene richiesto alla funzione di Internal Audit di effettuare un'indagine ai fini di accertare le responsabilità, quantificare i danni e supportare il management aziendale nel processo di miglioramento del Sistema di Controllo Interno. Inoltre, l'indagine portata avanti dall'internal auditing dovrà essere svolta in modo tale da non inficiare quella parallelamente condotta dall'autorità giudiziaria nel caso in cui l'evento di possibile frode sia stato oggetto di denuncia.

Riassumendo, l'attività di indagine a seguito di una segnalazione circa un possibile evento fraudolento può e deve essere svolta dalla funzione di Internal Audit, i cui componenti devono possedere conoscenze e competenze di base ai fini dell'individuazione e gestione delle frodi. Tuttavia, la prassi contempla sempre più il possesso di competenze tecniche ancor più specifiche e quindi la costituzione, all'interno della Funzione, di un nucleo dedito all'attività di fraud investigation. Gli internal auditor potranno quindi fornire un apporto maggiore in termini di individuazione e prevenzione delle frodi aziendali qualora siano in possesso di una specifica certificazione, la "Certified Fraud Examiner" (CFE). Il criterio della specializzazione si rende più visibile soprattutto all'interno delle grandi organizzazioni, dove viene a costituirsi una funzione dedicata all'investigazione sulle frodi aziendali, mentre è meno presente nelle piccole imprese in cui l'Internal Audit assolve a tale ruolo. Nonostante l'istituzione di una specifica funzione sembra essere preferibile nello svolgimento di tale ruolo, si ritiene comunque necessario un grande coinvolgimento dell'Internal Audit, in ragione del contributo che tale funzione può

---

<sup>111</sup> DITTMER C., *Internal Auditing: chiave per la corporate governance*, EGEA, Milano, 2008, pag. 261.

<sup>112</sup> INSTITUTE OF INTERNAL AUDITORS (IIA), *International Professional Practices Framework (IPPF): Standard 1210.A2: Competenza*, 1999.

fornire in termini di conoscenza delle debolezze e delle carenze del Sistema dei controlli. Non a caso, secondo gli standard internazionali, gli internal auditor dovranno suggerire al management l'impiego di un consulente esterno in materia di frodi qualora ravvisino l'assenza di una simile figura all'interno dell'azienda e l'assenza di competenze specifiche all'interno della stessa funzione di audit, ma al contempo non possono mancare le conoscenze generali del fenomeno e delle modalità con cui esso va fronteggiato.

### **3.6. Conclusioni**

Alla luce di quanto esposto all'interno del presente capitolo, è possibile dunque affermare l'importanza che il fenomeno delle frodi ha assunto, in particolar modo negli ultimi vent'anni, nel contesto dell'economia aziendale e degli studi sulla corporate governance. È stato inoltre detto a più riprese che il vero catalizzatore nello sviluppo di normative contro gli illeciti aziendali è rappresentato dagli eventi dei primi anni duemila, i cosiddetti *corporate scandals*, da cui sono derivate pesanti critiche all'intero sistema capitalistico occidentale.

In tale contesto, anche in Italia non sono mancate delle normative che hanno inciso fortemente, modificandolo, sul sistema dei controlli aziendali. Come è stato visto nelle pagine precedenti, la normativa che ha avuto un maggiore impatto nel nostro Paese, in tema di prevenzione di illeciti, è sicuramente la 231/2001, la quale ha stimolato la creazione di un Modello organizzativo, oltre che di un nuovo organismo di controllo, con un ruolo molto importante nella lotta alle frodi. Attraverso il decreto in questione, infatti, l'azienda non resta indifferente rispetto all'illecito compiuto da un soggetto a cui è legato un interesse o vantaggio per l'azienda stessa, ma essa è punibile severamente qualora non avesse adottato un idoneo modello, composto da procedure e processi aziendali, atto a prevenire determinate fattispecie di reato. Il decreto ha così stimolato le imprese a porre maggiore attenzione al tema delle frodi aziendali e a considerare l'individuazione e la prevenzione degli illeciti come una tematica fondamentale ai fini della *going concern*.

Inoltre, la 231 richiede che venga costituito un Organismo di Vigilanza, la cui funzione è appunto quella di vigilare sulla corretta predisposizione, attuazione e funzionamento del MOG e che, in termini comparativi, potremmo ben paragonare al ruolo ricoperto dall'Internal Audit in materia di Sistema di Controllo Interno. Infatti, come è stato detto all'interno del capitolo secondo, OdV e Internal Audit spesso si equivalgono, assolvendo alla medesima funzione, e il Rappresentante della funzione Audit è in genere un componente dell'Organismo. In tale ottica, il legislatore vede nell'Organismo di Vigilanza un elemento chiave nella lotta agli illeciti compiuti all'interno delle imprese. Per proprietà transitiva, si potrebbe affermare, la funzione Internal Audit svolge un ruolo altrettanto simile, estendendo il proprio oggetto di interesse a tutti i rischi a cui un'azienda incorre nella sua dinamica evolutiva, andando oltre alla verifica delle sole procedure che hanno ad oggetto i reati contemplati dal Decreto 231. In tal senso, la funzione Audit gioca un ruolo rilevante in termini di *fraud prevention and detection* e deve pertanto possedere, al suo interno, le competenze e le conoscenze necessarie in materia, come confermato dagli standard internazionali.

Infatti, l'Internal Audit può fornire un grande contributo in termini di individuazione delle “aree grigie” nelle quali è più probabile il compimento di illeciti, di potenziamento dell'intero sistema dei controlli e quindi di prevenzione del fenomeno, ponendo particolare enfasi all'attività di risk assessment in materia di frodi. In una fase successiva di gestione di un possibile evento fraudolento, invece, potrebbe ritenersi opportuno demandare ad unità tecniche specializzate in *fraud detection* la scelta delle azioni di risposta da porre in essere.

## Capitolo Quarto

### **Il coinvolgimento dell'Internal Audit nella gestione interna degli illeciti aziendali: applicazioni pratiche**

#### **4.1. Analisi comparata delle principali società quotate**

In accordo con quanto esaminato nei capitoli precedenti, è possibile dunque sostenere che l'internal auditing costituisce una funzione chiave per il corretto funzionamento del Sistema di Controllo Interno, oltre che per la rilevanza strategica che esso assume in sede di definizione del livello di rischio residuo. Si è altresì insistito sull'importanza della generazione di un circolo vizioso positivo che la Funzione è in grado di avviare attraverso il processo di *follow-up*, e non limitando il suo ruolo alla sola emanazione di un giudizio di assurance, bensì arricchendolo fornendo al senior management la propria consulenza in materia di Governance, Controllo Interno e Risk Management. Ancora, si è detto che l'esercizio dell'attività di auditing è possibile solo se viene mantenuta salda l'indipendenza del revisore interno, sia che la Funzione venga svolta internamente sia che venga svolta in *outsourcing*, e che il suo giudizio sia frutto di una valutazione obbiettiva e non condizionata da fattori esterni.

Tuttavia, occorre ricordare che quanto fin qui emerso è frutto di testi teorici elaborati da istituzioni internazionali (*International Professional Practices Framework* di Institute of Internal Auditors) o dall'autoregolamentazione nazionale (*Codice di Autodisciplina* di Borsa Italiana S.p.A.), senza che ciò sia normato da fonti aventi forza di legge. Se si considera anche l'adattabilità di questi schemi teorici ad ogni realtà aziendale, dalle PMI alle grandi *public companies*, è evidente come ogni società possa adottare il proprio modello di Internal Audit, lasciando al libero arbitrio l'istituzione di tale Funzione. Per tale motivo, appare riduttivo analizzare l'Internal Audit basandosi su dei modelli *to be* senza considerare la struttura *as is*, cioè senza tener conto dell'applicazione pratica degli standard internazionali e nazionali in materia di auditing e quindi dei risvolti concreti che tali principi hanno nelle realtà societarie.

In ragione di quanto appena esposto, si è ritenuto opportuno fornire un quadro più completo della Funzione attraverso l'analisi delle strutture di internal auditing in alcune realtà societarie di primaria importanza sul territorio nazionale. Nel farlo, è stato selezionato un campione casuale di venti società (dieci delle quali riconducibili al ramo *industrial*, e dieci al settore *financial*) tra quelle che compongono il FTSE MIB<sup>113</sup>, di seguito elencate:

- Atlantia;
- Banco BPM;
- BPER Banca;
- Campari;
- Enel;
- Eni;
- FinecoBank;
- Generali;
- Intesa SanPaolo;
- Italgas;
- Leonardo;
- Mediobanca;
- Pirelli;
- Poste Italiane;
- Prysmian;
- Saipem;
- Telecom Italia;
- UBI Banca;
- UniCredit;
- Unipol.

Di queste società è stata analizzata la struttura fondamentale della Funzione di Internal Audit facendo riferimento a quanto riportato all'interno di ciascuna *Relazione sul*

---

<sup>113</sup> Il FTSE MIB (*Financial Times Stock Exchange Milano Indice di Borsa*) è il più significativo indice azionario della Borsa italiana. Esso rappresenta il paniere che raggruppa le azioni delle quaranta società italiane quotate sul Mercato Telematico Azionario di Borsa Italiana S.p.A. con maggiore capitalizzazione, flottante e liquidità.

*governo societario e gli assetti proprietari, nonché alle Linee guida del Sistema di Controllo Interno e di Gestione dei Rischi (SCIGR).*

In primo luogo, l'analisi empirica ha previsto l'osservazione di elementi fondamentali quali le attribuzioni, le linee di riporto e i flussi di comunicazione. In merito alle attribuzioni, sono stati estratti e posti in evidenza i principali compiti attribuiti al Responsabile della Funzione, nonché i doveri riconducibili all'esercizio dell'incarico. Con riguardo alle linee di riporto, si è analizzata la nomina e il collocamento organizzativo della funzione, utile per l'attestazione della presenza del requisito dell'indipendenza nonché in grado di anticipare il prossimo elemento. Infatti, nell'analizzare i flussi informativi è stata posta particolare enfasi agli organi con cui si rapporta la funzione Audit nonché alla periodicità delle comunicazioni con tali organi. In un momento successivo, sono stati osservati ulteriori elementi sulla base dei quali è stato possibile ricevere segnali importanti sulle divergenze tra le imprese appartenenti al settore industriale e quelle riconducibili al settore finanziario. Tra questi elementi, il primo è relativo all'attività di auditing sul processo di gestione delle segnalazioni di violazioni di normative esterne e del Codice Etico aziendale (c.d. *Whistleblowing*). Questo aspetto è legato alla recente introduzione, tra i reati presupposto ex D.Lgs. 231/2001, del reato legato alla mancata adozione di un sistema di tutela del *whistleblower* che consenta un'azione di segnalazione anonima ed efficace degli illeciti.

Altro aspetto considerato riguarda la periodicità della reportistica. In tal senso, è stato approfondito il tema dei rapporti tra la Direzione Audit e i vari organi aziendali, con particolare riferimento ai flussi informativi esistenti. Tra questi, è emersa l'esistenza di alcuni obblighi di riporto verso alcuni di tali organi e quindi di termini prefissati entro i quali sia resa necessaria la comunicazione dei risultati e dell'andamento dell'attività di auditing svolta. Infine, si è posta l'esigenza di considerare come ultimo elemento l'esplicita menzione, all'interno della documentazione analizzata (cfr. Relazione sul governo societario...), della presenza dello svolgimento di attività di fraud auditing, quale attività il cui scopo è quello di prevenire ed individuare le frodi aziendali. Da tale ultimo aspetto sarà necessario ripartire, nel capitolo successivo, per

un approfondimento del tema delle frodi e di come l'attività di revisione interna siano in grado di prevenire tali eventi.

Dall'analisi svolta è emerso un generale allineamento rispetto ai principi discussi e agli argomenti trattati nei primi due capitoli. In particolare, con riferimento ai *driver* fondamentali (attribuzioni, linee di riporto, flussi di comunicazione) di cui si è tenuto conto nello studio delle società sopraelencate, è stata predisposta la seguente tabella:

SOCIETA'		CARATTERISTICHE INTERNAL AUDIT		
Nome	Settore	Attribuzioni	Linee di Riporto	Flussi di Comunicazione
ATLANTIA	Industriale	L'IA verifica che il SCIGR sia funzionante e adeguato, attestandone l'operatività e l'idoneità. Il responsabile della funzione ha accesso diretto a tutte le strutture e alla relativa documentazione. Verifica l'affidabilità dei sistemi informativi. L'attività di audit è svolta nei confronti di Atlantia e delle sue controllate.	Il Responsabile della funzione IA, l'Ing. Concetta Testa, non è responsabile di alcuna area operativa e dipende gerarchicamente dal Cda. È nominato dal Cda, previo parere del Comitato Controllo, Rischi e Corporate Governance, sentito il CS e su proposta dell'Amministratore Incaricato.	Il Responsabile della Funzione comunica, mediante relazioni periodiche, l'attività svolta e lo stato di avanzamento dei lavori. Inoltre, comunica tempestivamente ogni evento di particolare rilevanza. Inoltre, è previsto un continuo dialogo tra il Responsabile della funzione e il Presidente del Cda, l'AD, il CCR e il CS della holding e delle controllate. Infine, il Responsabile Audit partecipa a tutte le riunioni del CCR.
BANCO BPM	Finanziario	La funzione Audit ha la responsabilità, da un lato, di controllare il regolare andamento dell'operatività e l'evoluzione dei rischi e, dall'altro, di valutare la completezza, l'adeguatezza, la funzionalità e l'affidabilità del sistema dei controlli interni, rappresentando agli organi aziendali i possibili miglioramenti al processo di gestione, misurazione e	Il Responsabile della funzione Audit è Paolo Testi, il quale è anche responsabile del Sistema Interno di Segnalazione delle Violazioni. Paolo Testi è anche Preposto al Controllo Interno. Egli è nominato dal Cda e ne dipende gerarchicamente.	N/A

		controllo dei rischi e facendosi parte attiva nella loro realizzazione.		
BPER BANCA	Finanziario	La Direzione Revisione Interna deve individuare violazioni delle procedure e della regolamentazione nonché valutare periodicamente la completezza, l'adeguatezza, la funzionalità e l'affidabilità del SCI e del sistema informativo (ICT audit), con cadenza prefissata in relazione alla natura e all'intensità dei rischi. Il Responsabile della Funzione ha poteri di accesso a tutte le informazioni aziendali.	Il Responsabile della funzione è Andrea Tassi, nominato dal Cda su proposta dell'AD e alla presenza di tutti i componenti del CS. Egli riporta direttamente al Cda per tramite del Presidente del Cda.	Il consultivo dell'attività svolta viene presentato al Cda, al CS, al CCR e al vertice esecutivo della capogruppo.
CAMPARI	Industriale	La Funzione Audit ha il compito di verificare l'operatività e l'idoneità del SCIGR. Il Responsabile ha accesso diretto a tutte le strutture e alla relativa documentazione. Ha predisposto relazioni periodiche con gli organi sociali. Verifica e gestisce le segnalazioni di violazioni del Codice Etico e del MOG.	Il Responsabile della Funzione è Antonio Zucchetti e non dipende da alcuna area operativa, ma dal Presidente del Cda.	Il Responsabile della funzione di IA ha instaurato flussi informativi con i Presidenti del CS, del CCR, del Cda e con l'Amministratore Incaricato.

ENEL	Industriale	<p>La Funzione Audit ha il compito di verificare la struttura e la funzionalità del SCIGR. Il Responsabile Audit svolge attività di verifica specifiche, qualora lo ritenga opportuno ovvero su richiesta di Cda, CS, CCR e Amministratore Incaricato del SCIGR. Ha diretto accesso a tutte le informazioni utili ai fini dello svolgimento dell'incarico.</p>	<p>Il Responsabile della Funzione Audit è Silvia Fiori. Nominata dal Cda, sul proposta dell'Amministratore Incaricato, di intesa con il Presidente del Cda. Dipende gerarchicamente dal Cda e funzionalmente dall'Amministratore Incaricato. L'attività di audit è svolta alle dipendenze dirette dell'AD. Mentre al Presidente del Cda spetta il ruolo di supervisore delle attività di auditing.</p>	<p>È richiesta la partecipazione del Responsabile della funzione Audit alle riunioni del CCR. Il Responsabile informa il Presidente del Cda, il Presidente del CS e l'Amministratore incaricato del SCIGR circa i risultati dell'attività svolta. Ulteriori flussi informativi sono previsti tra i controlli di secondo livello e l'Internal Audit.</p>
ENI	Industriale	<p>La Funzione Audit ha il compito di verificare l'operatività e l'idoneità del SCIGR fornendo valutazioni e raccomandazioni e fornire supporto specialistico al vertice aziendale in materia di SCIGR per promuovere e favorire l'efficienza, l'efficacia e l'integrazione dei controlli aziendali. Il Responsabile Audit: svolge attività di vigilanza per conto dell'OdV; assicura la gestione delle attività di istruttoria per le segnalazioni di mancato rispetto delle normative esterne; svolge attività propedeutiche al conferimento dell'incarico di revisione legale.</p>	<p>Il ruolo di Responsabile della Direzione IA è ricoperto da Marco Petracchini, su nomina del Cda, previo parere favorevole del Comitato Controllo e Rischi, del Collegio Sindacale e del Comitato per le Nomine. Marco Petracchini è anche membro dell'OdV. Il Direttore Internal Audit dipende gerarchicamente dal Cda, che ne approva il piano sentito il parere del Presidente, del AD e del Comitato Controllo e Rischi, e dal Presidente del Cda e funzionalmente dal Comitato Controllo e Rischi e dall'AD</p>	<p>Le comunicazioni sono gestite dalla Direzione IA e avvengono periodicamente verso il Presidente del Cda, l'AD, gli organi di controllo e vigilanza di ENI e delle controllate. Comunica con l'OdV per conto dell'attività di vigilanza svolta. Il Responsabile della funzione comunica gli audit report a, in ordine: Presidente Cda, AD, CFO, Comitato Controllo e Rischi. Relazioni di Audit sono inviate a tali soggetti con cadenza almeno semestrale</p>
FINECOBANK	Finanziario	<p>L'attività svolta può essere riassunta come segue: audit di processo, per accertare l'efficiente svolgimento dell'attività aziendale; audit sui Consulenti Finanziari; accertamenti particolari non pianificati, volti a</p>	<p>Il Responsabile della funzione di IA è indipendente rispetto a ogni area operativa, e ha obbligo di riporto al solo Cda e CS. L'attività di IA è stata affidata in outsourcing a UniCredit, tramite contratto di appalto di servizi.</p>	<p>Il Responsabile della Funzione relaziona al Cda e al CS in merito agli esiti dell'attività svolta con periodicità trimestrale. Inoltre, il Responsabile IA è di norma presente alle riunioni (mensili) del</p>

		identificare le cause e le responsabilità di specifici eventi (frodi o infedeltà).		Comitato Rischi e Parti Correlate.
GENERALI	Finanziario	Il Group Audit valuta e monitora l'efficacia, l'efficienza e l'adeguatezza del SCIGR. Ha inoltre libero accesso a tutte le unità organizzative aziendali e alla relativa documentazione. Il Group Audit può svolgere anche attività di Advisory relativamente a temi come Risk Management, governance e controlli.	La funzione IA è affidata a una struttura organizzativa indipendente chiamata "Group Audit". Il responsabile della funzione non dipende gerarchicamente da aree operative ma dal Cda.	Il Responsabile Group Audit collabora attivamente con le autorità di vigilanza. Con cadenza almeno annuale deve sottoporre al Cda, previo parere del Comitato Controllo e Rischi, un piano di audit. È inoltre prevista una reportistica almeno trimestrale verso il Comitato Controllo e Rischi. In caso si riscontrano eventi gravi, il Responsabile ne informa immediatamente il Cda, il CCR e il CS.
INTESA SANPAOLO	Finanziario	Il Responsabile Audit ha accesso a tutte le attività presso tutte le strutture. Valuta la funzionalità complessiva del sistema dei controlli, con riferimento al RAF e al processo di gestione dei rischi. Valuta, inoltre, l'efficacia del processo di definizione del RAF. Supporta la governance fornendo ai vertici aziendali una continua e puntuale informativa sullo stato del sistema.	Il Responsabile Audit è posto alle dirette dipendenze del Cda e del Presidente del Cda. Funzionalmente riporta invece al Comitato per il Controllo sulla Gestione. Al Chief Audit Officer del gruppo riportano tutte le strutture di IA dell'intero gruppo.	Il Chief Audit Officer sottopone il piano al Comitato per il Controllo sulla Gestione e, successivamente al Cda, almeno una volta l'anno.
ITALGAS	Industriale	Al Responsabile Audit spetta il compito di verificare l'operatività e l'idoneità del SCIGR. Il Responsabile Audit ha accesso a tutte le informazioni utili per l'espletamento dell'incarico. Egli predispone relazioni periodiche e svolge, su richiesta di Cda, Amministratore	Il Responsabile della funzione è Agostino Limonta, che dipende dal Cda.	Il Responsabile della funzione trasmette le relazioni periodiche al CS, CCROPC, Cda e all'Amministratore Incaricato.

		Incaricato, CCROPC, CS, dandone comunicazione, verifiche su specifiche aree operative.		
LEONARDO	Industriale	Al Group Internal Audit è attribuita la funzione di supportare il Cda e gli altri organi nell'attività di valutazione del SCIGR dell'intero gruppo; verificare l'operatività e l'idoneità del SCIGR; accedere a tutte le informazioni utili per lo svolgimento dell'incarico; predisporre relazioni periodiche sulla propria attività, sulle modalità con cui vengono gestiti i rischi, e sulla valutazione del SCIGR.	L'amministratore incaricato al SCIGR è l'AD. Il Responsabile della funzione Group Internal Audit è Marco di Capua. Egli dipende gerarchicamente dal Cda e dal Presidente del Cda. Qualora siano attribuite deleghe operative, dipende dal Comitato Controllo e Rischi e dal suo Presidente.	Comunica e trasmette le relazioni ai Presidenti di Cda, CS, Comitato Controllo e Rischi, nonché all'Amministratore Incaricato del SCIGR.
MEDIOBANCA	Finanziario	La funzione di Audit è accentrata in Mediobanca ma operativa per l'intero Gruppo, è strutturata per verificare e assicurare l'adeguatezza, in termini di efficacia ed efficienza, del SCI.	Il Responsabile della funzione Audit dell'intero gruppo è Giorgio Paleari, che dipende dal Cda.	Il Responsabile della Funzione partecipa alle riunioni del Comitato Rischi. Semestralmente fornisce una relazione al Cda e al Comitato Rischi, per riferire le attività svolte e aggiornare sullo stato del SCIGR.
PIRELLI	Industriale	La Funzione Audit ha il compito di valutare l'adeguatezza e la funzionalità dei processi di controllo, gestione dei rischi e corporate governance. Inoltre, verifica l'operatività e l'adeguatezza del SCIGR; svolge verifiche su specifiche aree operative; predispone relazioni periodiche; fornisce supporto agli Organismi di Vigilanza.	Funzione di cui è il Responsabile Maurizio Bonzi, nominato dal Cda, da cui la Funzione dipende gerarchicamente.	Trasmissione delle relazioni periodiche con cadenza almeno trimestrale verso: CS, Comitato Controlli, Rischi, Sostenibilità e Corporate Governance, Amministratore incaricato e, almeno semestralmente, Cda.

<p>POSTE ITALIANE</p>	<p>Finanziario</p>	<p>Poste Italiane ha istituito due funzioni di internal audit: Controllo Interno di Poste Italiane e Revisione Interna di Banco Posta. Controllo Interno svolge audit sui processi significativi dell'intero gruppo, Revisione Interna solo ai processi che hanno ad oggetto il patrimonio di Banco Posta. Hanno accesso a tutte le informazioni, valutano la completezza, l'adeguatezza, l'affidabilità e la funzionalità del SCIGR, ne verificano l'operatività, verificano l'affidabilità dei sistemi informativi. La sola funzione Revisione Interna valuta: l'efficacia del processo di definizione del RAF, l'adeguatezza e l'efficacia delle funzioni Risk Management e Compliance, l'adeguatezza del processo ICAAP, la continuità operativa aziendale.</p>	<p>La funzione Controllo Interno di Poste Italiane riporta gerarchicamente al Cda, attraverso il suo Presidente, e funzionalmente al CCRS e all'AD, in qualità di amministratore incaricato. La funzione Revisione Interna di BancoPosta riferisce direttamente al Cda e al CS di Poste Italiane.</p>	<p>Incontri trimestrali con gli organi di governo per riferire sulle attività svolte e sullo stato del SCIGR. Inoltre, almeno annualmente deve essere inviata una relazione contenente l'attività svolta, le modalità e i risultati ottenuti.</p>
<p>PRYSMIAN</p>	<p>Industriale</p>	<p>Il Responsabile Audit relaziona periodicamente sul risultato dell'attività svolta, fornisce valutazioni sul SCIGR e sulle aree oggetto di apposite verifiche.</p>	<p>Il Responsabile Audit è Laurida Sayed, che fa diretto riferimento a Alessandro Nespoli, Responsabile Audit&amp;Compliance, il quale riporta a sua volta al Cda. Quest' ultimo è anche segretario del Comitato Controllo e Rischi</p>	<p>Risultano programmate apposite riunioni tra IA, Comitato Controllo e Rischi e CS ai fini di aggiornare tali organi sullo svolgimento dell'incarico di audit. Relazioni periodiche sono trasmesse a: Presidente CS, Presidente Comitato Controllo e Rischi, Amministratore Incaricato del SCIGR.</p>

SAIPEM	Industriale	La Funzione Audit ha il compito di verificare l'operatività e l'idoneità del SCIGR di SAIPEM e delle società controllate. Deve inoltre fornire supporto specialistico al management in materia di SCIGR e verso il CCR e il CS per l'ottenimento di informazioni per l'espletamento dei rispettivi incarichi.	Il Responsabile IA è Luigi Siri, il quale dipende gerarchicamente dal Cda e per esso dal Presidente, fatta salva la dipendenza funzionale dal CCR e dall'AD, in qualità di Amministratore Incaricato di sovrintendere il SCIGR.	Si richiede che siano mantenuti attivati i rapporti e i flussi informativi tra IA e OdV, CCR e CS. La trasmissione delle relazioni periodiche avviene con cadenza almeno trimestrale.
TELECOM ITALIA	Industriale	Alla Funzione Audit spetta il compito di verificare l'operatività e l'idoneità del SCIGR. Il Responsabile della funzione ha accesso diretto a tutte le informazioni utili per lo svolgimento dell'incarico; predispone relazioni periodiche sull'attività svolta e contenenti una valutazione complessiva del SCIGR. La direzione Audit svolge inoltre attività di Whistleblowing, cioè ricezione, trattamento, analisi e archiviazione delle segnalazioni di violazioni.	Il Responsabile della funzione IA è Daniele Gulinatti, il quale dipende gerarchicamente dal Cda e funzionalmente dall'AD, in quanto Amministratore Incaricato.	Comunica al Comitato controllo e rischi e al CS circa lo stato di avanzamento dell'attività di audit e le valutazioni effettuate. Riferisce direttamente ai Presidenti del Cda e del CS, al Comitato Controllo e Rischi e all'AD su eventi di particolare rilevanza.
UBI BANCA	Finanziario	La figura del Responsabile della funzione è ricoperta da Stefano Maria Tortellotti. Egli opera come Chief Audit Officer dell'intero gruppo, svolgendo attività di controllo di terzo livello su tutte le controllate. L'IA verifica la regolare operatività del SCIGR e contribuisce a migliorarlo.	Il Responsabile della funzione IA dipende e viene nominato dal Consiglio di Sorveglianza, previo parere favorevole del CCR.	Sono comunicati i risultati delle singole attività di audit ai vertici aziendali. Inoltre, è prevista una rendicontazione periodica a favore dei Cda e dei CS delle società controllate e al Consiglio di Gestione e al Consiglio di Sorveglianza della Capogruppo, nella quale viene menzionata l'attività svolta e lo stato di avanzamento

UNICREDIT	Finanziario	La funzione Audit riferisce direttamente, o tramite il CCR, al Cda con cadenza almeno annuale, sull'efficacia, sull'effettivo funzionamento e sull'adeguatezza del SCIGR. Inoltre, svolge special investigation in Unicredit e nel gruppo, informando dei risultati il Senior Management e gli organi aziendali.	Il Responsabile della funzione IA è Serenella De Candia, che riporta al Cda il quale, a sua volta, indirizza, coordina e supervisiona le attività di internal audit del gruppo.	Il responsabile della funzione predispone un'informativa trimestrale agli organi aziendali e al Senior Management. In particolare, sono previste comunicazioni con Cda, Comitato per i Controlli interni e Rischi.
UNIPOL	Finanziario	La funzione Audit valuta la completezza, la funzionalità, l'affidabilità e l'adeguatezza del SCIGR. È garantito l'accesso a tutte le strutture aziendali e alla relativa documentazione.	Il Responsabile della funzione Andrea Alessandri non è responsabile di alcuna area operativa e riporta gerarchicamente al Cda. È prevista la condivisione della propria struttura con quella delle unità relative alle funzioni Risk Management e Compliance.	La Funzione Audit collabora con il CCR, la società di Revisione, il CS e l'OdV. A seguito di ogni intervento viene comunicato il relativo report al Cda. In situazioni di gravità e urgenza, il fatto viene comunicato al Cda, al CS, al CCR e all'Amministratore Incaricato. A questi soggetti è inoltre destinata una relazione semestrale sull'attività svolta.

*Tabella 1 - L'attività di Internal Audit nelle principali aziende nazionali: caratteristiche fondamentali. Fonte: elaborazione propria*

Dalla tabella di cui sopra si evince, con riguardo alle attribuzioni, come le funzioni di internal auditing delle società analizzate facciano esplicito riferimento ai compiti, ruoli, poteri e doveri attribuitigli dagli Standard Internazionali della Professione. Infatti, nella stragrande maggioranza dei casi, nella relazione sulla corporate governance si legge che l'Internal Audit assolve alla funzione di “valutare l’operatività e l’idoneità del Sistema di Controllo Interno e di Gestione dei Rischi”. Altra attribuzione che accomuna tutte le società analizzate consiste nel potere di accesso a tutte le strutture e alla documentazione della società oggetto di analisi e di tutte le società controllate da essa. Non mancano comunque alcune differenze: ad esempio,

nelle sole banche è prevista altresì la valutazione del processo di definizione del Risk Appetite Framework (RAF), nonché del RAF stesso, e soltanto in alcune società viene attribuita all'Internal Audit il compito di valutare il processo di gestione delle segnalazioni di illeciti, come si vedrà più avanti.

Altro elemento su cui occorre soffermarsi è la gestione centralizzata delle attività di auditing, fattore riscontrato nella quasi totalità dei casi esaminati. Infatti, ad eccezione di FinecoBank, la cui attività di internal auditing viene gestita in outsourcing da UniCredit e comunque attraverso una struttura centralizzata, in tutti gli altri casi si sviluppa una Direzione Generale di Audit nella capogruppo, la quale svolge la propria attività verso tutte le società controllate, o perlomeno verso le società del gruppo che non dispongono di un proprio Internal Audit. Tuttavia, questo aspetto non sembra essere pienamente in linea col principio per il quale l'audit debba calarsi nella singola realtà aziendale di riferimento e in quanto tale assumere una particolare conformazione. Infatti, i grandi gruppi aziendali possono essere caratterizzati da un'eterogeneità di business e possono svolgere un numero elevato di attività diverse tra loro, per cui si renderebbe necessaria la presenza di funzioni e strutture di controllo distinte. Inoltre, gli studi effettuati sulle strutture centralizzate delle Funzioni di Internal Audit hanno mostrato un crescere dei costi burocratici legati alla gestione di un numero elevato di catene di autorizzazione che si vengono in tal modo a costituire. Sulla base delle evidenze riscontrate attraverso le informazioni a disposizione, quindi, è possibile affermare che le principali società italiane presentano un eccessivo grado di centralizzazione delle strutture di audit, da cui potrebbe derivare una minore attenzione alle attività di controllo svolte a livello locale, maggiori ritardi nell'attuazione di azioni, minore autonomia decisionale delle unità di audit presenti nelle strutture operative locali. Tale scelta organizzativa presenta comunque numerosi vantaggi, tra cui la possibilità di esprimere un unico indirizzo strategico, garantendo omogeneità all'azione di audit nell'intero gruppo, nonché la capacità di mantenere un maggiore livello di indipendenza.

Per quanto riguarda le linee di riporto, anche in questo caso è emersa una generale attitudine all'assecondare gli standard internazionali e, in particolare, il Codice di Autodisciplina delle società quotate di Borsa Italiana S.p.A. Infatti, nelle società che

adottano un sistema di governance tradizionale (90% dei casi esaminati) il Responsabile della Funzione Internal Audit ha obbligo di riporto gerarchico verso il Consiglio di Amministrazione e, nello specifico, verso il Presidente del CdA, rapporto necessario ai fini del mantenimento delle condizioni di indipendenza. A tal riguardo, si fa esplicitamente riferimento al fatto che la Direzione Audit non è in alcun modo dipendente dalle unità operative aziendali. Importante è inoltre il ruolo ricoperto dal Comitato Controllo e Rischi (CCR) e dall'Amministratore Incaricato del Sistema di Controllo Interno e di Gestione dei Rischi (nella prassi ruolo ricoperto dall'Amministratore Delegato), in quanto elementi di raccordo tra il CdA e la funzione oggetto di analisi, tra cui si crea un rapporto di tipo funzionale. Nelle società in cui non si adotta il modello tradizionale emergono le seguenti fattispecie:

- Laddove venga adottato il sistema monistico (es. Intesa SanPaolo), è previsto un riporto funzionale verso il Comitato per il Controllo sulla Gestione, al quale viene sottoposto annualmente, oltre che al Consiglio di Amministrazione, il piano di audit;
- Laddove venga invece adottato il sistema dualistico (es. UBI Banca), è prevista una dipendenza gerarchica dal Consiglio di Sorveglianza, organo che ha il potere di nominare, revocare e stabilire la remunerazione del Responsabile Audit.

Altro elemento di condivisione tra tutte le società analizzate riguarda l'approvazione (annuale) del piano di audit: il piano è approvato dal Consiglio di Amministrazione, sentito il parere del Presidente, dell'Amministratore Delegato e del Comitato Controllo e Rischi.

Con riguardo al terzo *driver* contenuto nella tabella 1, dall'analisi si evince l'esistenza di flussi di comunicazione periodici tra la Funzione e i seguenti organi sociali: Presidente del Consiglio di Amministrazione e Presidente del Collegio Sindacale, Comitato Controllo e Rischi e Amministratore Incaricato del SCIGR. Inoltre, l'attività di internal auditing spesso si presta all'esecuzione di specifiche verifiche a supporto di tali organi, a cui seguono altrettanto specifiche relazioni. Tale attività di verifica viene svolta anche a supporto dell'Organismo di Vigilanza, di cui spesso il Responsabile

della Funzione è un componente, e rispetto al quale la funzione si presta a esserne il “braccio operativo”.

In merito alla periodicità dei flussi informativi sono state raccolte le seguenti informazioni circa gli intervalli temporali massimi entro i quali si richiede l’invio di report da parte del Responsabile della Funzione Audit verso gli organi aziendali. I risultati dell’analisi sono stati riassunti all’interno del seguente grafico:

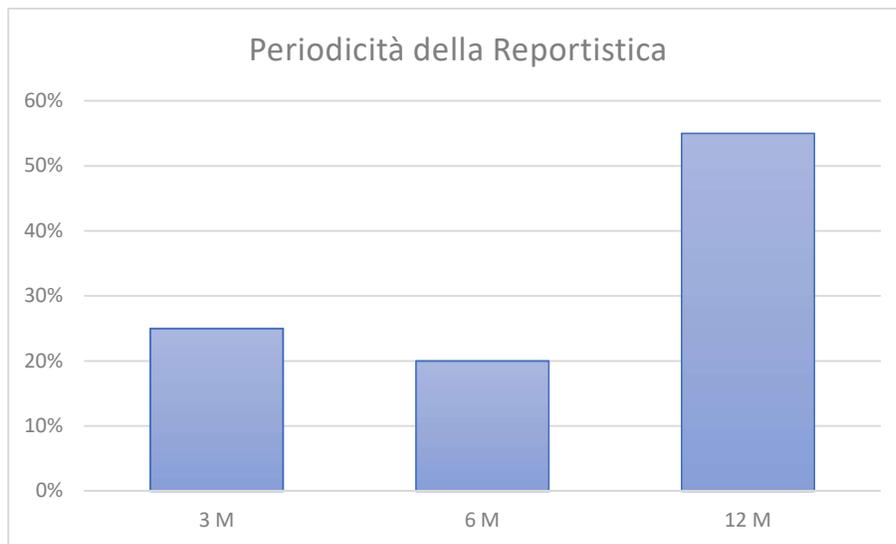


Grafico 1 - La periodicità della reportistica verso gli organi aziendali. Fonte: elaborazione propria

Nell’interpretazione di tali dati, occorre tener conto del fatto che laddove la Relazione sul governo societario non rendesse nota una periodicità della reportistica di audit, è stato convenzionalmente pattuito il termine di un anno (periodicità relativa alla discussione e all’approvazione del piano di audit). Per tale motivo il dato più rilevante sembra mostrare un intervallo temporale annuale, ma che di fatto non offre un’evidenza concreta ai fini della nostra analisi. Il dato più interessante sembra piuttosto essere offerto dall’esplicito riferimento all’utilizzo di una periodicità trimestrale, presente in un numero di casi maggiore rispetto a quella semestrale. Tuttavia, questo dato sembra essere fortemente influenzato dalla presenza, nel campione, di società appartenenti al ramo finanziario. Infatti, nel grafico successivo

(grafico 2) si può notare come la periodicità media delle comunicazioni è inferiore nelle società finanziarie, rispetto a quanto emerge nel gruppo *industrial*, ed è pari a una durata di 7,5 mesi tra l'invio di un report e l'altro. Tale dato può essere giustificato dal fatto che nel settore finanziario è presente un maggiore livello di regolamentazione e ciò induce le società del settore a presentare una reportistica più frequente nell'espletamento delle attività di audit. Nel leggere tali dati occorre ricordare che la periodicità della reportistica non determina, se non parzialmente, tutti i flussi informativi esistenti tra il Responsabile della Funzione e gli organi sociali. Ad esempio, in Enel, è prevista la partecipazione del Responsabile Audit a tutte le riunioni del Comitato Controllo e Rischi. Inoltre, il dato è stato ricostruito sulla base di quanto riportato nelle Relazioni sulla corporate governance e, come si è detto in precedenza, molte società hanno deciso di non comunicare agli stakeholder tale informazione, alterando parzialmente i risultati dell'analisi effettuata.

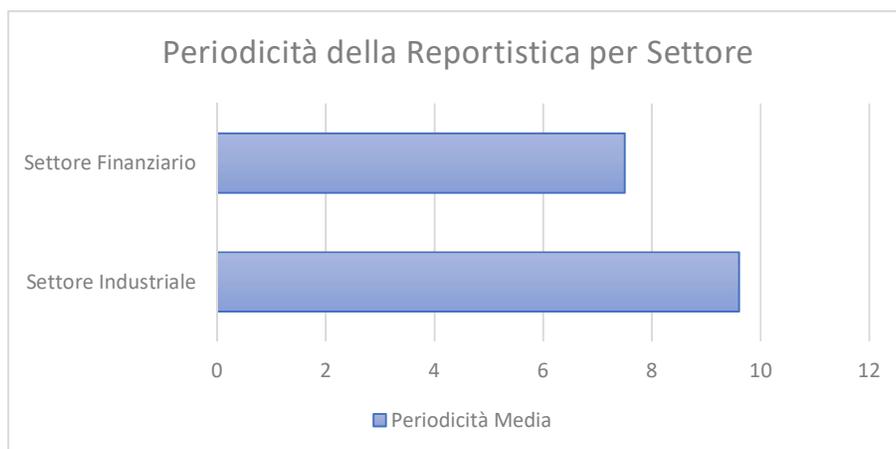
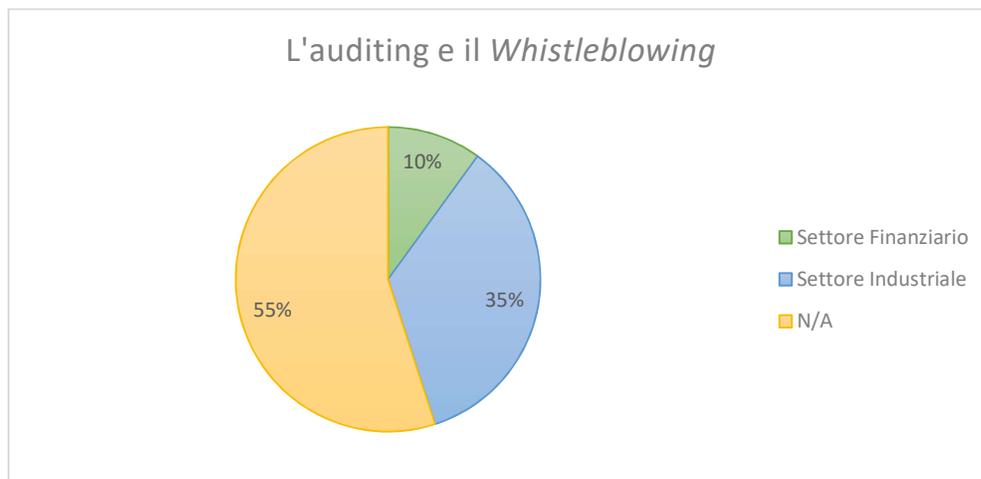


Grafico 2 - Periodicità della reportistica per settore di appartenenza. Fonte: elaborazione propria

Nel corso dell'indagine è inoltre emerso il tema della gestione delle segnalazioni, attività identificata con il termine *Whistleblowing*, in quanto viene spesso attribuito alla funzione Internal Audit il compito di valutare il corretto svolgimento del processo di gestione delle segnalazioni di eventuali violazioni di normative esterne o del Codice

Etico. In particolare, tra le società analizzate, nel 45% di esse si fa esplicito riferimento all'attribuzione di tale mansione all'Internal Audit. Anche in questo caso, come nel precedente, la mancata evidenza all'interno della Relazione sulla corporate governance non è indice della totale assenza di tale attività nello svolgimento dell'incarico di audit. Piuttosto, il dato può essere interpretato come una semplice assenza di tale informativa all'interno di suddetta relazione.



*Grafico 3 - L'attività di auditing sul processo di gestione delle segnalazioni. Fonte: elaborazione propria*

Tuttavia, elaborando i dati sotto un'altra ottica e restringendo l'analisi alle sole società industriali, è possibile notare come in questo caso il 70% di esse presenti, tra le attribuzioni della Direzione Audit, quella di esprimere un parere sul processo di gestione delle segnalazioni. Di seguito uno schema riassuntivo sui risultati in entrambi i settori:

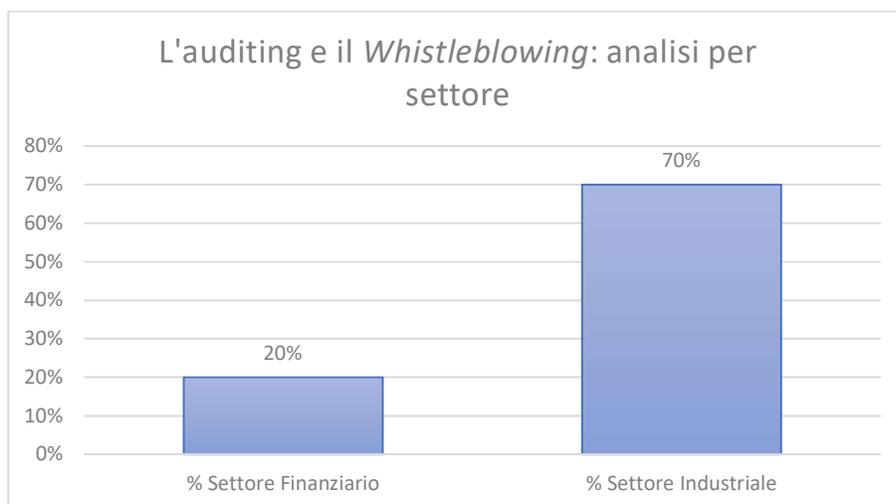


Grafico 4 - L'auditing sul processo di gestione delle segnalazioni: un'analisi per settore. Fonte: elaborazione propria

Interpretando contemporaneamente i grafici 3 e 4 è possibile ricercare una risposta a tali dati nell'appartenenza a un settore piuttosto che all'altro. Infatti, se nel primo grafico è emerso come quasi la metà delle società analizzate esponga in Relazione sulla governance lo svolgimento di attività di audit sul processo di gestione delle segnalazioni, nel secondo è possibile vedere come quel numero è in gran parte costituito da società industriali. Ciò può essere quindi determinato dalle differenze presenti nelle regolamentazioni settoriali.

Per concludere, durante lo svolgimento dell'analisi è stata posta particolare attenzione alla presenza o meno di riferimenti in merito allo svolgimento di attività di fraud auditing. In particolare, se attraverso le verifiche sul corretto funzionamento del processo di gestione delle segnalazioni la funzione Audit è in grado di condurre a un *improvement*, seppur indiretto, del Sistema di Controllo, la riduzione del più generale rischio di frode passa necessariamente attraverso l'attività di fraud auditing. Rispetto al campione esaminato, è emerso che solo il 25% delle società (Telecom, Leonardo, Generali, Unipol, Fineco) ponga in essere (o meglio lo esponga all'interno della propria Relazione) l'attività di individuazione e prevenzione delle frodi aziendali e il dato, seppur non necessariamente indicativo dell'assenza del concreto svolgimento di

tale attività, appare comunque non soddisfacente rispetto all'importanza che le frodi ricoprono in tema di controllo interno e *risk management*. Tuttavia, va tenuto a mente che le informazioni fornite nella presente ricerca sono estrapolate dall'informativa resa pubblica dalle società esaminate e non costituiscono, pertanto, un dato esauriente circa l'effettivo impegno dell'Internal Audit nella lotta alle frodi aziendali. Per tale motivo, il paragrafo successivo presenterà il caso di un'azienda e delle modalità attraverso le quali è stato gestito internamente un evento riconducibile al fenomeno delle frodi.

#### **4.2. Il ruolo del revisore interno in un caso italiano di frode**

L'analisi condotta nelle pagine precedenti ha fornito un'immagine più completa e realistica circa l'effettiva predisposizione delle strutture di Internal Audit all'interno delle aziende. Inoltre, è stato possibile effettuare alcune importanti considerazioni riguardo l'impegno di tali strutture in ambito di prevenzione ed individuazione delle frodi aziendali. Il risultato di questi test ha portato a concludere che, soprattutto nelle imprese appartenenti al settore industriale, è molto presente la fattispecie per la quale la funzione di Internal Audit debba esprimersi in merito alla corretta predisposizione ed attuazione del processo di gestione delle segnalazioni anonime. Altro risultato, non propriamente convincente, indica che solo in un'azienda su quattro vengono poste in essere regolarmente attività di fraud auditing da parte della funzione di revisione interna. Ricordando, ancora una volta, che tali dati non sono indicativi del reale impegno delle imprese nel contrasto al fenomeno delle frodi aziendali, risulta opportuno presentare un caso di frode al fine di comprendere le modalità con le quali esso è stato gestito dalla società e il contributo offerto dall'Internal Audit.

Nello specifico, il caso analizzato ha ad oggetto una frode, con delle ripercussioni di natura contabile, commessa all'interno di una Società per azioni appartenente al settore industriale di cui non si menzionerà il nome per ragioni di riservatezza. Al fine di contestualizzare, quanto più è possibile, le circostanze all'interno delle quali si è realizzato l'evento, segue una descrizione dettagliata della funzione di Internal Audit di tale società.

Nell'anno durante il quale la frode si è realizzata, il gruppo aziendale era dotato di una funzione di Internal Audit centralizzata, il cui responsabile era stato nominato dal Consiglio di Amministrazione, che ne ha altresì stabilito la remunerazione, su proposta dell'amministratore incaricato di sovrintendere il Sistema di Controllo Interno e di Gestione dei Rischi, sentito il parere del Comitato Controllo e Rischi. Alla Funzione è stato attribuito il compito di verificare, in conformità con gli IPPF, l'adeguatezza e l'effettivo funzionamento del Sistema di Controllo Interno e di Gestione dei Rischi, mettendo in atto un Piano di Audit, successivamente approvato dal Consiglio di Amministrazione. Al Responsabile della Funzione è stato concesso l'accesso diretto a tutte le informazioni utili per lo svolgimento dell'incarico ed è stato pattuito l'obbligo di riporto, circa il proprio operato, al Presidente del Collegio Sindacale, al Presidente del Comitato Controllo e Rischi e al Presidente del Consiglio di Amministrazione, oltre che all'amministratore incaricato del sistema di controllo interno e di gestione dei rischi. La figura qui rappresentata rivestiva inoltre l'incarico di Segretario del Comitato Controllo e Rischi e, di conseguenza, ha partecipato a tutte le sue riunioni. Inoltre, egli riferiva trimestralmente circa i risultati raggiunti al Collegio Sindacale, laddove gli venisse richiesto. Infine, la Funzione di Internal Audit oggetto di analisi aveva responsabilità in materia di fraud auditing, svolgendo attività di natura investigativa su presunti casi di comportamenti illeciti, violazioni di leggi o regolamenti interni.

Negli esercizi successivi a quello nel quale è stato compiuto l'illecito, la funzione di revisione interna ha subito alcuni cambiamenti di natura strutturale, rafforzando i rapporti tra la Funzione di Internal Audit e le altre funzioni di controllo aziendale. L'attività posta in essere dalla nuova funzione di Audit interno risulta pressoché identica rispetto a quella eseguita negli esercizi precedenti, essendo improntata su un processo di Enterprise Risk Management e avendo maggior riguardo, rispetto alla struttura precedente, alla verifica dell'affidabilità dei sistemi di rilevazione contabile e dei sistemi informativi. Con riguardo alle restanti attribuzioni e agli obblighi di riporto, resta ferma la piena conformità agli Standard Internazionali della Professione.

Come anticipato nelle righe precedenti, la Funzione appena descritta è stata impegnata recentemente nella gestione interna di un caso di frode. In particolare, la vicenda trae origine da alcune operazioni di M&A poste in essere dal Gruppo e dall'occultamento

di importanti informazioni aziendali riguardanti l'acquisizione di una società che da ora in avanti verrà definita Target. Quest'ultima, al momento della sua acquisizione, vantava due grandi progetti, che per semplicità espositiva verranno definiti Progetto 1 e Progetto 2, sui quali Target vantava dei crediti. La causa principale del problema va rintracciata in un lungo "braccio di ferro" tra i dirigenti di Target e le controparti interessate in merito alla determinazione del prezzo per l'estinzione del debito di tali questi ultimi. Infine, la vicenda è stata caratterizzata dalla pressione degli organi di vigilanza che, in prossimità delle date di chiusura dei bilanci del Gruppo e della società Target, richiedevano un accordo definitivo. Tali pressioni hanno portato alla contrattazione di un accordo preliminare, il quale prevedeva l'estinzione del debito attraverso il pagamento di cifra pattuita, di importo inferiore a quanto inizialmente richiesto.

La scoperta della frode è dovuta al fatto che un soggetto apicale di Target, d'ora in avanti indicato con l'appellativo "Dirigente", nel tentativo di occultare l'importo pattuito in sede di accordo preliminare, ha alterato l'informativa contenuta in tale documento fornendo agli organi di vigilanza, a fronte delle continue richieste, una documentazione falsa con impatti rilevanti sui bilanci di Target. Nello specifico, la frode è stata scoperta dopo che il Dirigente ha inviato due volte la medesima mail, ma con allegati differenti: al primo invio il contenuto della mail includeva una versione falsa del documento, dove l'importo pattuito per l'estinzione del debito era stato sostituito con la sigla "T.B.C." (*To Be Confirmed*); al secondo invio, invece, all'interno della mail vi era la versione originale, la quale riportava il valore preventivamente concordato.

Appurata la differenza tra i documenti inviati, gli organi di controllo della società hanno provveduto a convocare un *meeting* con gli esponenti del top management aziendale, incluse le persone coinvolte nella vicenda. A questo punto la Società ha richiesto l'intervento della funzione di Internal Audit al fine di chiarire la vicenda e accertare le responsabilità di ciascuna persona coinvolta. In particolare, è stato richiesto all'Internal Audit di:

- a) Eseguire una attenta analisi del contesto nel quale si è svolta la vicenda, facendo particolare riferimento all'acquisizione di Target, ai crediti vantati da

questa nei confronti dei contratti stipulati in merito al Progetto 1 e al Progetto 2, all'accordo preliminare stipulato tra Target e le controparti in merito all'estinzione della situazione debitoria di tali soggetti;

- b) Ricostruire la cronologia degli eventi, in modo da poter comprendere a fondo le azioni poste in essere dal soggetto responsabile della frode;
- c) Identificare le altre persone coinvolte nella vicenda e, qualora fossero presenti, individuarne i ruoli e le responsabilità;
- d) Valutare gli impatti potenziali della frode in termini di alterazione dei dati contabili e dei risultati finanziari della Target e dell'intero Gruppo;
- e) Comprendere i potenziali impatti della frode in termini di incentivi personali, bonus e remunerazione delle persone coinvolte nella vicenda;
- f) Verificare e ricercare altre potenziali "alterazioni" di documenti non riscontrate in precedenza, siano esse legate o meno alla vicenda;
- g) Qualora siano riscontrate nuove alterazioni, definire i ruoli e le responsabilità delle persone coinvolte nei nuovi fatti riscontrati.

Al fine di fornire un *output* in merito a tali richieste, la funzione di Internal Audit del Gruppo ha deciso di far ricorso all'assistenza e al coinvolgimento di personale esterno altamente qualificato in materia di *fraud investigation* con l'obiettivo di:

1. Svolgere un'analisi sui computer aziendali (*e-Discovery*) delle persone coinvolte nella vicenda. L'attività ha previsto la raccolta di informazioni digitali attraverso l'utilizzo di appositi software, attraverso i quali è possibile estrarre dati di diverso genere dai notebook, dai server e dalla posta elettronica.
2. Analizzare e valutare la frode e i relativi impatti, partendo dallo svolgimento di interviste con le persone coinvolte nella vicenda al fine di ricostruire la cronologia degli eventi, fino ad arrivare alla comprensione dei ruoli e delle responsabilità nel compimento dell'illecito, nonché del possibile impatto che esso avrebbe avuto sui bilanci della società qualora non fosse stato scoperto.
3. Analizzare ulteriori potenziali alterazioni dell'informativa aziendale attraverso il confronto tra gli ulteriori documenti inviati dalla società presenti nelle mail con la documentazione originale estratta dai computer, e verificando, attraverso appositi programmi, se la stessa documentazione ha subito particolari modifiche nel tempo.

In sintesi, a seguito delle analisi effettuate dagli esperti del *forensic*, la funzione di Internal Audit è pervenuta alle seguenti conclusioni.

In primo luogo, è stato attribuito alla persona responsabile del “doppio invio” della documentazione incriminata il ruolo di principale esecutore dell’azione fraudolenta. L’addebito di tale responsabilità è principalmente dovuto alla confessione di costui in sede di intervista. Inoltre, attraverso le analisi condotte sul suo laptop, sono emerse delle conversazioni tra lui e un altro soggetto aziendale in cui si scherzava sul rischio di finire in prigione con l’accusa di falsificazione dei documenti contabili.

Successivamente, sono state svolte una serie di *Scenario Analysis* al fine di comprendere l’impatto che tale manipolazione avrebbe avuto sul bilancio qualora essa non fosse stata scoperta. In relazione a tale aspetto, bisogna considerare la scarsa portata dell’evento se si tengono in considerazione le soglie di materialità dell’intero Gruppo, mentre va confermata la significatività del potenziale errore in relazione alla sola *entity* considerata. In particolare, senza entrare in dettaglio dell’analisi sui riflessi contabili dell’operazione, va detto che l’evidenza di uno specifico importo all’interno di un accordo preliminare, seppur non definitivo, avrebbe aumentato la probabilità di perdita legata alla mancata recuperabilità del credito e, di conseguenza, una svalutazione dello stesso in bilancio attraverso la costituzione di un fondo svalutativo.

Infine, dall’analisi delle motivazioni alla base del comportamento fraudolento, si evince l’assenza di elementi in grado di condizionare l’operato del dirigente. Attraverso lo studio dei piani di incentivazione posti in essere all’interno dell’esercizio in corso è emerso come questi, alla data del compimento dell’illecito, non avrebbero garantito alcun guadagno extra a prescindere dal risultato dell’operazione in questione. Infatti, l’EBITDA del Gruppo e di Target non soddisfaceva i requisiti minimi per l’accesso ad eventuali bonus. Pertanto, sono da escludere ogni tipo di interesse personale del dirigente con la vicenda.

Attraverso lo studio di questa vicenda è stato possibile dimostrare come un singolo individuo sia in grado, anche in assenza di particolari interessi o vantaggi personali, di aggirare i controlli e i modelli organizzativi interni e di porre in essere comportamenti in contrasto con la legge o con i regolamenti aziendali. In particolare, la vicenda narrata pone in rilievo le caratteristiche tipiche del frodatore economico. Infatti, come è stato

visto all'interno del precedente capitolo, le capacità tecniche da egli possedute creano i presupposti per il compimento della frode e la fiducia e l'onorabilità che vanta verso gli altri fanno sì che il comportamento illecito passi inosservato.

In ogni modo, nel caso esaminato è possibile valutare positivamente l'azione sinergica dei controlli aziendali, dalle prime linee nella comunicazione dell'errore riscontrato fino alla gestione successiva da parte della funzione di Internal Audit, la quale ha permesso l'individuazione della frode e la prontezza della risposta con la quale sono state accertate le responsabilità e poste in essere le dovute azioni correttive.

## Considerazioni finali

L'analisi condotta sul fenomeno delle frodi aziendali e l'ipotesi per la quale la funzione di Internal Audit costituisca un'unità aziendale idonea a contrastarlo può concludersi con un esito positivo. Si può quindi definitivamente affermare che le attività di internal auditing assumono un ruolo rilevante in termini di prevenzione, individuazione e gestione delle diverse fattispecie di illecito aziendale.

In particolare, è possibile affermare che le attività di auditing hanno efficacia massima nella fase di prevenzione delle frodi, in virtù della conoscibilità degli internal auditor dell'impresa, in generale, e del Sistema di Controllo Interno, nello specifico. Infatti, la funzione di revisione interna rappresenta, come è stato affrontato in precedenza, il braccio operativo dell'Organismo di Vigilanza e in quanto tale sono ad essa demandate le attività di risk assessment e di ispezione al fine di individuare le criticità all'interno del sistema dei controlli e di ridurre il rischio di commissione del reato ad un livello ritenuto accettabile. In questi termini, si conferma la rilevanza del contributo offerto dal legislatore italiano mediante il Decreto Legislativo n. 231/2001 in materia di responsabilità amministrativa degli enti, con il quale le imprese sono state poste in prima linea, di fianco alle autorità nazionali, nella lotta alle frodi aziendali. Quindi, mediante una visione "dall'alto" dell'impresa, l'Internal Audit è in grado di individuare le "aree grigie" del Sistema di Controllo Interno e di promuovere azioni di implementazione di nuovi controlli o di miglioramento dei controlli esistenti in tali aree, rafforzando i meccanismi di controllo e di prevenzione dei rischi di frode.

Inoltre, come è stato visto durante la trattazione del caso aziendale, l'Internal Audit rappresenta la funzione alla quale il top management attribuisce il compito di indagare su eventuali sospetti di illeciti. Le indagini poste in essere dalla Funzione si pongono come obiettivo quello di accertare le responsabilità di chi ha compiuto l'illecito, quantificare i danni e gli impatti della frode sulla società e su terzi e promuovere miglioramenti al Sistema di Controllo Interno. Nello svolgimento di questa attività, tuttavia, si richiede all'Internal Audit il possesso di conoscenze e competenze

specifiche in materia di frodi. In particolare, gli internal auditor dovranno conoscere a fondo le dinamiche fraudolente e le diverse modalità con le quali il fenomeno si realizza, dovranno conoscere le modalità attraverso cui si esegue un'attività di *fraud investigation* e dovranno saper utilizzare particolari software per lo svolgimento dell'incarico. Il possesso di tali competenze è in genere avvalorato dal conseguimento di un'apposita certificazione, la quale attribuisce agli internal auditor il titolo di *Certified Fraud Examiner (CFE)*.

Nel caso in cui la funzione di Internal Audit non possieda al suo interno un adeguato livello di conoscenza in materia di frodi, è prassi diffusa, e confermata dall'analisi del caso aziendale visto precedentemente, quella di ricorrere a soggetti esterni specializzati in *forensic and anti-fraud services*. Anche in tal caso, però, la funzione di revisione interna mantiene un ruolo di gestione dell'intera dinamica di frode e di coordinamento dell'intero team di azione, internalizzando quelle competenze necessarie per l'assolvimento dell'incarico. Inoltre, il ricorso a persone esterne permette alla funzione di Internal Audit di aumentare il livello di indipendenza nel suo giudizio che, se già ritenuto imprescindibile, risulta ancor più importante nel momento in cui deve essere gestito internamente un reato societario.

## Bibliografia

- ALBRECHT W.S., HOWE K.R., ROMNEY M.B., *Deterring fraud: the internal auditor's perspective*, Altomonte, 1984
- ALLEGRINI M., D'ONZA G., MANCINI D., GARZELLA S., *Le frodi aziendali: frodi amministrative, alterazione di bilancio e computer crime*, Franco Angeli, 2007
- ANACLERIO M., MIGLIETTA A., SQUAIELLA S., *Internal Audit: dalla teoria alla pratica*, Wolters Kluwer, IPSOA, 2007
- ASSOCIAZIONE ITALIANA INTERNAL AUDITORS (AIIA), *Approccio integrato al sistema di controllo interno: gli organi e le funzioni preposte al controllo interno aziendale e le loro relazioni*, Corporate Governance Paper
- ASSOCIAZIONE ITALIANA INTERNAL AUDITORS (AIIA), *Legge sulla Tutela del Risparmio*, Position Paper, marzo 2006
- ASSOCIAZIONE NAZIONALE DEI DIRETTORI AMMINISTRATIVI E FINANZIARI (ANDAF), *Il dirigente preposto alla redazione dei documenti contabili societari*, Position Paper ANDAF, maggio 2007
- ASSONIME, *Il dirigente preposto alla redazione dei documenti contabili nel sistema dei controlli societari*, Circolare 44, novembre 2009
- BANCA D'ITALIA, *Istruzioni di Vigilanza per le banche: Attività di revisione interna*, 2006
- BIANCHINI N., DI NOLA C., *I controlli societari: molte regole, nessun sistema*, Milano, EGEA, 2010
- BORSA ITALIANA S.p.A., *Codice di autodisciplina*, Comitato per la Corporate Governance, 2018
- CHIAPPETTA F., *Diritto del governo societario*, Wolters Kluwer Italia, CEDAM, 2017
- CNDC, *Principi di comportamento del Collegio Sindacale nelle società di capitali con azioni quotate nei mercati regolamentati*, Norme di comportamento del Collegio Sindacale, settembre 2015

- COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO), *Enterprise Risk Management, Integrated Framework*, 2004; ed. it. a cura di AIIA e PwC, *La gestione del rischio aziendale*, Milano, Il Sole 24 Ore, 2006
- COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO), *Enterprise Risk Management, Integrating with strategy and performance*, 2017
- CRESSEY D.R., *Other people's money: a study in the social psychology of embezzlement*, Tree Prees, Glencoe, Illinois, 1953
- D.Lgs. 24 febbraio 1998, n. 58, in materia di “*Testo Unico delle disposizioni in materia di intermediazione finanziaria*”
- D.Lgs. 8 giugno 2001, n. 231, in materia di “*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica a norma dell'art. 11 della legge 29 settembre 2000, n.300*”
- DITTMER C., *Internal Auditing: chiave per la corporate governance*, EGEA, 2011
- ECIIA, *L'Internal Auditing in Europa*, Position Paper, 2005
- GIANNINI M.S., *Diritto Amministrativo*, I, Milano, 1970
- GLEIM I.N., *CIA Review*, Gleim Publications, 2004
- GROSSI C. G., *Internal Auditing: l'inizio di una nuova avventura*, Milano, AIIA, 2002
- INSTITUTE OF INTERNAL AUDITORS (IIA), *International Professional Practices Framework (IPPF)*, 1999
- INTERNATIONAL AUDITING AND ASSURANCE STANDARDS BOARD (IAASB), *Principio di Revisione Internazionale (ISA Italia) 200*, 2010
- ISVAP, Regolamento n. 20/2008
- Legge 28 dicembre 2005, n. 262, in materia di “*Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari*”
- MOELLER R., *Brink's modern internal auditing: a common body of knowledge*, John Wiley & Sons, 2016

- POGLIANI G., PECCHIARI N., MARIANI M., *Frodi aziendali: forensic accounting, fraud auditing e litigation*, EGEA, 2012
- PRAWITT D.F., SHARP N.Y., WOOD D.A., *Internal audit quality and earnings management*, The Accounting Review, Vol. 84
- Public Law 30 luglio 2002, n. 107-204, USA, cd. Sarbanes-Oxley Act
- PWC, *Global Economic Crime and Fraud Survey 2018: Pulling Fraud Out of The Shadows*, 2018
- WOLFE D.T., HERMANSON D.R., *The Fraud Diamond: Considering the Four Elements of Fraud*, CPA Journal, 2004
- ZAIN M.M., ZAMAN M., MOHAMED Z., *The Effect of Internal Audit Function Quality and Internal Audit Contribution to External Audit on Audit Fees*, International Journal of Auditing, 2015
- ZANDA G., *La funzione direzionale del controllo*, Cagliari, 1967

## Sitografia

- [www.ilsole24ore.com](http://www.ilsole24ore.com)
- [www.treccani.it](http://www.treccani.it)
- [www.solofinanza.it](http://www.solofinanza.it)
- [www.portale231.com](http://www.portale231.com)

## Riassunto

Il presente lavoro è volto ad analizzare la relazione intercorrente tra la corretta predisposizione e attuazione della Funzione di Internal Audit e la conseguente riduzione del rischio di frode, in termini di individuazione e prevenzione dell'illecito.

La ricerca parte dalla constatazione degli effetti che uno scandalo societario può provocare nei confronti dell'azienda all'interno della quale è compiuto l'illecito, nonché verso la grande platea di interlocutori sociali che hanno un interesse nei confronti dell'organizzazione. Non solo, l'impatto di una frode agisce altresì sulla reputazione di chi la compie e di ciò che ne ruota attorno, provocando forti cambiamenti in un particolare mercato o in un'area geografica. Ne è un esempio recente e di portata internazionale lo scandalo che ha coinvolto il leader del settore automobilistico Volkswagen (cd. *Dieselgate*): il “disastro economico”, come cita il Sole 24 Ore in un recente articolo, conta un numero di circa 11 milioni di veicoli richiamati e un ammontare di spese che si aggira intorno ai 20 miliardi di euro. Inoltre, a partire dal 18 Settembre 2015 è crollata completamente la reputazione del motore diesel, con conseguenze che hanno riguardato anche gli altri *player* del mercato automobilistico. Infatti, l'evento appena citato ha agito da catalizzatore dell'elettrificazione dei motori, spostando il baricentro del mercato dell'automobile verso l'area asiatica.

Senza soffermarci ulteriormente sullo scandalo appena citato, va detto che le frodi aziendali rappresentano una minaccia per il mondo dell'economia-aziendale, a prescindere dalla portata dell'evento. Infatti, secondo alcune ricerche, un'azienda su due dichiara di aver subito negli ultimi 24 mesi un reato di natura economico-finanziaria, con perdite che in un'azienda italiana su quattro sono state superiori al milione di dollari. Questi dati dimostrano l'importanza del fenomeno in termini di frequenza e impatto, e giustificano l'intensificarsi degli studi di corporate governance che mirano a creare un sistema dei controlli aziendali più strutturato al fine di ridurre il rischio di accadimento.

Partendo dal presupposto che realtà ben strutturate già dispongono di adeguate procedure e processi aziendali atti a minimizzare il rischio di incorrere in perdite finanziarie e reputazionali derivanti dalla commissione di illeciti, e che nelle medesime società sia costituita una funzione che svolga attività di revisione interna su tali processi, lo scopo del seguente lavoro è quello di analizzare le modalità attraverso cui tale funzione agisce al fine di prevenire ed individuare una frode aziendale.

Il presente elaborato affronta questo tema partendo dall'illustrazione del concetto di Sistema di Controllo Interno, facendo particolare riferimento alla sua funzione all'interno dell'organizzazione e agli attori coinvolti e presenti nel suo disegno. Infatti, il mondo dei controlli aziendali è oggi composto da un'eterogeneità di attori, ciascuno

dei quali con una funzione specifica, talvolta sovrapponibili, talvolta ben distinta dagli altri, da cui si evidenzia l'esigenza di esercitare un monitoraggio costante sull'operato degli organi esecutivi al fine di indirizzare la gestione verso il perseguimento della creazione di valore. Il Sistema di Controllo Interno, in sintesi, può definirsi nel seguente modo: *“Il controllo interno è un processo, svolto dal Consiglio di Amministrazione, dai dirigenti e da tutto il personale aziendale, finalizzato a fornire una ragionevole certezza sul raggiungimento degli obiettivi aziendali che rientrano in particolare nelle seguenti categorie:*

- *Efficacia ed efficienza delle attività operative (Operations);*
- *Attendibilità delle informazioni di bilancio (Financial reporting);*
- *Conformità alle leggi e regolamenti in vigore (Compliance).*

Una volta definito il concetto di Sistema di Controllo Interno e chiarita la funzione che esso ha all'interno dell'organizzazione aziendale, il presente lavoro introduce la Funzione di Internal Audit quale funzione di controllo di terzo livello, a cui spetta il giudizio sulla corretta predisposizione ed attuazione dei controlli aziendali. Infatti, i controlli interni possono distinguersi in tre categorie:

- 4) Controlli di primo livello: vengono altresì definiti come controlli “di linea” e consistono nei controlli effettuati dai manager dei singoli centri di responsabilità o unità organizzative.
- 5) Controlli di secondo livello: questi si possono definire come dei controlli trasversali sui rischi e sulla conformità e sono svolti da appositi organi aziendali, che concorrono a definire il sistema di controllo interno (es. Risk Management e Compliance).
- 6) Controlli di terzo livello, in cui vi rientra l'Internal Audit.

Per poter comprendere al meglio la natura della funzione di Internal Audit, tuttavia, occorre approfondire la materia del Sistema di Controllo Interno e analizzare quali elementi esso deve possedere al fine di esercitare una concreta riduzione del livello di rischio aziendale complessivo. Per tale motivo, vanno menzionati i modelli internazionali di riferimento per l'attuazione di un Sistema di Controllo Interno. Il primo, tra questi, è stato il CoSO Report, che costituisce un “framework contenente delle *best practices* professionali per la realizzazione di processi e sistemi di business volti a promuovere un efficace ed efficiente controllo interno”. Secondo questo modello, le componenti di un buon SCI devono essere: l'ambiente di controllo, la valutazione dei rischi, le attività di controllo, la comunicazione, il monitoraggio.

Negli anni successivi, la prima versione del CoSO Report fu superata dal CoSO Enterprise Risk Management (ERM). Le principali differenze tra i due modelli sono le seguenti:

- L'Enterprise Risk Management Framework costituisce un'evoluzione del CoSO Report e in quanto tale non se ne distacca in merito alle finalità, quanto

piuttosto in merito alle modalità attuative di un sistema di controllo interno efficace ed efficiente, che si manifesta nel nuovo modello attraverso un approccio maggiormente basato sul rischio;

- Gli obiettivi di reporting: mentre nell'ERM Framework per reporting si fa riferimento ad informazioni di diversa natura il suo predecessore guarda all'obiettivo di reporting esclusivamente nell'ottica della affidabilità della reportistica economico-finanziaria;
- Il CoSO ERM aggiunge una nuova categoria agli obiettivi, cioè quella di natura strategica;
- Risk management: l'attività di gestione dei rischi viene affrontata in entrambi i modelli, ma in maniera decisamente più approfondita nel secondo;
- Informazione e comunicazione: nell'ambito di tale componente, il nuovo approccio palesa la necessità di divulgare, tra le varie informazioni, anche quelle relative a dati previsionali.

Infine, nel mese di Giugno 2017 è stato pubblicato un nuovo modello, definito "*ERM Integrating with strategy and performance*", il quale pone particolare enfasi agli aspetti della definizione della strategia e valutazione della performance.

In questo contesto, la Funzione di Internal Audit esercita un ruolo di fondamentale importanza. Infatti, secondo il Codice di Autodisciplina delle società quotate il Preposto al controllo interno, che di fatto coincide con il Responsabile della Funzione di Internal Audit, è incaricato di verificare che il sistema di controllo interno sia sempre adeguato, pienamente operativo e funzionante; non è responsabile di alcuna area operativa, ivi inclusa l'area Amministrazione, Finanza e Controllo; ha accesso diretto a tutte le informazioni utili per lo svolgimento del proprio incarico; dispone di mezzi adeguati allo svolgimento della funzione assegnata; riferisce del proprio operato al comitato per il controllo interno ed al collegio sindacale e può inoltre essere previsto che riferisca anche all'amministratore esecutivo incaricato di sovrintendere alla funzionalità del sistema di controllo interno.

L'International Professional Practices Framework (IPPF), uno schema concettuale con il quale vengono organizzate un insieme di linee guida per la realizzazione di un efficiente internal auditing, invece, definisce l'IA come "l'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". Questo Framework internazionale, se correttamente applicato, consente alle imprese di ogni dimensione e complessità di predisporre una efficiente Funzione di Internal Audit. Oltre alla Definizione, esso è composto da Principi Fondamentali, Codice Etico e Standard Internazionali, ove i Principi e il Codice Etico rappresentano la chiave al fine di mantenere salda l'efficacia

e l'integrità della Funzione, oltre che diffondere la cultura etica all'interno dell'organizzazione. Tra gli Standard, invece, occorre distinguere quelli di "connotazione" da quelli di "prestazione". I primi riguardano i "connotati" che deve possedere l'internal auditor e si distinguono in 4 macro-aree, tra cui Finalità autorità e responsabilità, indipendenza e obiettività, competenza e diligenza professionale, programma di miglioramento della qualità. Gli Standard di prestazione, invece, hanno ad oggetto principalmente lo svolgimento dell'incarico e la natura dell'attività, generalmente intese.

Con riguardo al processo di Audit, è possibile individuarne quattro fasi: pianificazione, esecuzione, reporting e follow-up. Durante la fase di pianificazione gli internal auditor raccolgono le informazioni generali e definiscono l'*Audit Universe*, cioè l'insieme degli elementi che possono essere o saranno oggetto di audit. Successivamente, con l'aumentare del livello di dettaglio e di conoscenza dei rischi insiti nelle varie aree, si passerà a considerare esclusivamente gli oggetti maggiormente a rischio, che verranno sottoposti ad un *risk assessment*. Infine, verrà creato un piano di audit. Nella fase successiva, invece, viene disposto un piano di lavoro e verranno eseguiti i primi controlli determinati in sede di definizione del piano di audit, attraverso i quali si otterranno le principali informazioni per l'emanazione del giudizio. La terza fase è rappresentata dalla stesura di un Report di audit e dalla comunicazione dei risultati ottenuti al management aziendale, attraverso cui il responsabile della funzione di Internal Audit suggerisce le azioni correttive da porre in essere. Infine, si ritiene necessaria una fase conclusiva e continuativa di follow-up, necessaria ad accertare il rispetto e la messa in atto del piano di azione concordato con il management e a monitorare il livello di rischio complessivo dell'impresa auditata. Va sottolineato che questa fase aggiunge valore assoluto al processo, incentivando l'aggiornamento dei sistemi di controllo e la risoluzione delle problematiche evidenziate. Tale incentivo è legato soprattutto al rispetto, da parte del management, delle scadenze pattuite in sede di comunicazione dei risultati. In questo modo è in grado di generare un circolo vizioso di *continuous improvement* con un impatto positivo sul raggiungimento di un sistema di controllo ottimale e quindi con il miglioramento dei risultati aziendali sia nel breve ma soprattutto nel medio-lungo termine.

Occorre pertanto chiedersi se la professione dell'internal auditor ha un impatto rilevante nella creazione di valore di impresa o va inquadrata esclusivamente nel suo ruolo passivo di "controllore". La chiave di risposta va ricercata soprattutto nell'accezione "consulenziale" dell'attività di internal auditing. Infatti, come precisato nella definizione degli IPPF, l'Internal Audit rappresenta un'attività che non si limita a fornire assurance sul sistema di controllo, né si qualifica come un processo il cui output è la mera emanazione di un giudizio, bensì contempla un'azione propositiva per il miglioramento della corporate governance, della gestione del rischio e del sistema di controllo interno, il cui fine ultimo è quello di creare valore per l'impresa. Tale finalità può definirsi raggiunta nel momento in cui l'internal auditor estende

l'orizzonte temporale dell'intervento anche successivamente alla comunicazione del giudizio al board e al senior management aziendale e in questi termini la fase di follow-up rappresenta un momento cruciale dell'intero processo.

Dopo aver fornito un quadro generale utile per la comprensione del fenomeno del Sistema di Controllo Interno e della funzione di Internal Audit si è ritenuto opportuno analizzare le interazioni effettivamente esistenti tra questa e le restanti funzioni di controllo. Rispetto al Consiglio di Amministrazione, ad esempio, l'Internal Audit è in grado di fornire "assurance sull'efficacia dei processi di governance, gestione dei rischi e controllo interno, prendendo in considerazione i rischi strategici, di reputazione, di mercato, creditizi, operativi e finanziari", informazioni indispensabili per l'attuazione di strategie da parte del CdA in grado di creare valore per l'impresa nel medio e lungo termine. Proprio in relazione alla necessità, da parte dell'Organo direzionale, di attingere a determinate informazioni per svolgere al meglio il proprio incarico, si considera lo stesso come unico responsabile del buon funzionamento del Sistema di Controllo Interno e in quanto tale, come promotore per l'implementazione di una efficace ed efficiente attività di internal auditing. È proprio il CdA che stabilisce la frequenza e la natura delle comunicazioni tra le due funzioni, definisce i ruoli e i compensi, e sottoscrive il Mandato della Funzione, definito Audit Charter.

Con il crescere delle dimensioni e della complessità aziendale, il Consiglio di Amministrazione sviluppa al suo interno alcuni comitati non esecutivi. In particolare, il Codice di Autodisciplina prevede che venga creato un Comitato Controllo e Rischi, con responsabilità in materia di Sistema di Controllo Interno e Gestione dei Rischi. In questo modo, si crea un ponte tra il CdA e le funzioni di controllo, attribuendo al CCR le seguenti attività: esprimere un parere su specifici temi circa l'identificazione e la gestione dei rischi aziendali; esaminare le relazioni periodiche in tema di gestione dei rischi e in particolare quelle fornite dalla funzione di Internal Audit; monitorare l'adeguatezza, l'efficienza e l'efficacia dell'attività di internal auditing; richiedere alla funzione di internal audit lo svolgimento di verifiche su aree operative specifiche, dandone comunicazione al presidente del collegio sindacale; riferire al Consiglio di Amministrazione circa l'adeguatezza del Sistema di Controllo Interno. Appare evidente la stretta collaborazione tra il Responsabile della funzione di internal audit e i consiglieri che compongono il CCR. In particolare, si ritiene necessario un continuo scambio di flussi informativi che hanno a oggetto: le aspettative e gli obiettivi del vertice, gli aggiornamenti sull'attività di auditing svolta, la valutazione complessiva del livello di rischio aziendale.

Rispetto al Collegio Sindacale bisogna evidenziare la differenza principale tra le due funzioni: il Collegio Sindacale svolge un tipo di controllo prettamente amministrativo, l'Internal Audit svolge una valutazione del Sistema di Controllo Interno. Nonostante ciò, non mancano punti di raccordo tra le due funzioni: in primis, il Responsabile della Funzione di Internal Audit ha il dovere di riferire al Collegio Sindacale tutte le

informazioni ritenute necessarie per lo svolgimento dell'incarico di tali organi; in secondo luogo, secondo il TUF, lo stesso Collegio Sindacale deve vigilare sul corretto funzionamento dei controlli aziendali.

In merito ai rapporti tra l'IA e l'Organismo di Vigilanza ex D.Lgs. 231/2001, si può affermare che l'OdV si qualifica, nella prassi, come un organo collegiale, con apposite garanzie di indipendenza, qualificazione professionale ed efficienza. In merito alla sua composizione, è previsto che esso sia composto indistintamente da soggetti appartenenti all'ente, tra cui generalmente rientra il Responsabile della Funzione di Internal Audit. La funzione di Internal Audit, in ogni caso, si qualifica come il "braccio operativo" del OdV, con il dovere di svolgere l'attività di risk assessment per l'identificazione delle attività potenzialmente sensibili alla commissione dei reati di cui al D.Lgs. 231/2001; le verifiche di audit per la valutazione dell'adeguatezza dei presidi aziendali esistenti e il loro effettivo funzionamento.

Infine, si è ritenuto opportuno evidenziare i rapporti tra la Funzione e il Revisore Legale. Quest'ultimo ha il compito di "esprimere, attraverso un parere (*opinion*) sul bilancio sottoposto a revisione, se i fatti di gestione sono correttamente rilevati nelle scritture contabili, se il bilancio corrisponde alle risultanze di tali scritture e se esso risulta conforme alle norme che ne disciplinano la redazione". Dalla definizione appena fornita è possibile notare come la revisione interna è completamente differente dalla revisione legale esterna, nonostante ci siano degli elementi in comune. Pertanto, si ritiene che le attività siano distinte ma complementari, in quanto l'IA valuta, all'interno del Sistema di Controllo Interno, anche i controlli effettuati internamente sul processo amministrativo-contabili, il cui output è il bilancio di esercizio. Di conseguenza, una efficace attività di internal auditing è in grado di fornire una maggiore assurance sulla correttezza delle informazioni contenute in bilancio permettendo al revisore esterno di svolgere le proprie attività in maniera più efficiente e a una *fee* ridotta. Altri studi più recenti dimostrano invece come non sia tanto la *reliance* sul corretto operato della funzione di revisione interna a ridurre le *fee* della società di audit, quanto più la diretta assistenza prestata dagli internal auditor nei confronti dei revisori legali.

Sulla base di quanto fin qui affermato si può affermare che la funzione di Internal Audit sia vista come una attività di supporto, benché indipendente, rispetto alla presa di decisioni strategiche in tema di Sistema di Controllo Interno, da un lato, e rispetto allo svolgimento delle attività del Collegio Sindacale, del Dirigente preposto e della società di revisione esterna, dall'altro. Occorre tuttavia individuare con chiarezza le aree di competenza oggetto dei vari controlli al fine di limitare le situazioni di *over-auditing* e raggiungere una maggiore copertura sulle aree aziendali auditate.

Partendo dal presupposto che il Sistema di Controllo Interno assolve alla funzione di sostenere la crescita dell'impresa mediante un'efficace gestione dei rischi aziendali, va da sé che l'attenzione dell'Internal Audit sia rivolta verso ogni tipologia di rischio.

Tra queste, assume rilievo il rischio di frode, che diviene quindi oggetto di attenzione della Funzione di revisione interna per via dell'impatto che un evento fraudolento può provocare all'interno dell'Organizzazione. Il tema delle frodi, infatti, ha visto crescere notevolmente la sua importanza all'interno degli studi sulla corporate governance, specialmente a seguito dei principali scandali societari che si sono susseguiti agli inizi degli anni duemila. Infatti, le esperienze di Enron, Tyco, WorldCom, Parmalat, fino alla più recente Volkswagen, hanno via via condotto i legislatori nazionali e la letteratura manageriale verso un maggiore impegno ad analizzare e studiare tali comportamenti fraudolenti e, di conseguenza, migliorare le strutture aziendali atte a prevenire il compimento di questi reati.

In primo luogo, potremmo interpretare la frode come un atto di appropriazione illecita con il quale si ottiene un vantaggio per sé o per altri. Nonostante il nostro ordinamento non fornisca una definizione condivisa di frode, essa si configura sempre attraverso il seguente schema: l'attore (soggetto attivo), attraverso artifici e raggiri, induce in errore la vittima (soggetto passivo) e procura a sé stesso o ad altri un vantaggio ingiusto congiuntamente ad un altrettanto ingiusto danno per la vittima o per altri. All'interno delle aziende il fenomeno è oggi molto diffuso e ciò è dovuto al fatto che il frodatore trae beneficio dallo schermo costituito dall'attività economica che viene svolta o dall'intera organizzazione, che rende il fatto illecito scarsamente percettibile agli occhi di terzi; sfrutta il bagaglio di competenze tecniche posseduto al fine di rendere l'inganno posto in essere un complesso e sofisticato insieme di azioni; approfitta degli effetti (negativi) a lungo termine che la frode comporta per le vittime. Inoltre, la vittima spesso non si identifica con un singolo soggetto ma è rappresentata da una categoria sociale o dalla comunità in generale e, in quanto tale, rende l'impatto sul singolo individuo di difficile misurazione.

In merito alle ragioni che spingono gli individui verso il compimento di illeciti, il contributo più importante è riconducibile agli studi al criminologo Donald R. Cressey, che formulò le sue teorie più importanti, come il Triangolo della Frode, verso la fine degli anni '50. Dopo aver intervistato un campione di 200 persone accusate di appropriazione illecita, Cressey arrivò alla conclusione per cui ogni individuo è spinto dal compiere un crimine economico solo se sono presenti contemporaneamente tre fattori (da cui il cd. Triangolo della Frode): necessità di soddisfare bisogni (finanziari) percepiti e pressanti; consapevolezza di avere l'opportunità (percepita) di compiere e di occultare l'illecito; considerazione del proprio comportamento come atto non criminoso, definibile anche come razionalizzazione atta a rendere il comportamento come soggettivamente accettabile.

Le teorie di Cressey sono state poi oggetto di modifiche e rivisitazioni. Tra le più importanti, si segnala la teoria della Diamante della Frode, riconducibile agli studiosi David Wolfe e Dana Hermanson. In particolare, fermo restando la funzionale coesistenza dei precedenti tre elementi ai fini del compimento della frode si aggiunge

un quarto elemento, rappresentato dalla *capability*, in quanto l'atto criminale non può avvenire senza che l'attore possieda le dovute conoscenze e competenze professionali nel porlo in essere, specialmente per quelle frodi caratterizzate da un elevato tasso di complessità. In altri termini, se la "pressione percepita" e la "razionalizzazione" forniscono a un individuo la motivazione ad agire, la "capacità" è l'elemento che permette a tale soggetto di riconoscere "l'opportunità" che il compimento di un determinato illecito rappresenta, legata al vantaggio che ne consegue, e di porre in essere il reato.

Occorre inoltre precisare che le frodi possono avvenire con modalità molto diverse tra loro, pur mantenendo gli elementi essenziali appena descritti. Esse, infatti, possono essere interne o esterne. Le prime si manifestano all'interno del contesto organizzativo della società, dove i principali attori sono gli amministratori o i dipendenti della stessa. Le frodi esterne invece si qualificano per la presenza esterna degli attori, i quali possono essere clienti o fornitori della società. Le frodi possono avere natura contabile (*on the book*) o extra-contabile (*off the book*). Secondo alcune ricerche condotte, è possibile delineare il seguente scenario circa le frodi più comuni commesse nei nostri giorni: appropriazione indebita, falso in bilancio, corruzione, infrazioni fiscali, agiotaggio, insider trading e frode informatica.

La recente diffusione del fenomeno non ha di certo lasciato indifferenti i legislatori di tutto il mondo. Infatti, soprattutto a seguito dei principali scandali finanziari avvenuti verso gli inizi degli anni duemila, numerose sono le normative prodotte attraverso le quali si è cercato di arginare il fenomeno. Tra queste, di fondamentale importanza sono il Sarbanes-Oxley Act (cd. "SOX") negli USA, e la Legge sul Risparmio, conosciuta come la "SOX italiana". L'obiettivo delle due normative era quello di porre in risalto il tema della corporate governance, migliorando il sistema dei controlli societari, attribuendo maggiori responsabilità ai diversi attori sociali e tutelando, quanto più possibile, non soltanto gli interessi degli azionisti ma di tutti gli stakeholder aziendali, tra cui le banche, i fornitori e i partner commerciali, i clienti, le autorità di vigilanza e i dipendenti aziendali. Ad esempio, gli elementi fondanti della SOX sono l'indipendenza della società di revisione contabile e la vigilanza sul suo operato, la maggiore attendibilità dell'informativa finanziaria e maggiori controlli sul processo contabile, l'attribuzione di maggiori poteri alla Security Exchange Commission. Inoltre, la SOX ha previsto un inasprimento delle sanzioni dovute all'alterazione dei documenti finanziari e contabili. La Legge n. 262/2005 o "Legge sul Risparmio", invece, oltre alla disciplina dell'attività di revisione legale e all'inasprimento delle sanzioni per i dirigenti aziendali in caso di falsa informativa contabile, ha introdotto un nuovo elemento rappresentato dalla figura del Dirigente Preposto alla redazione dei documenti contabili societari, il cui compito principale è quello di istituire e sovrintendere l'intero processo amministrativo-contabile e di redazione del bilancio di esercizio.

Infine, grande contributo in materia di illeciti aziendali è stato offerto dall'introduzione, nel nostro ordinamento, del D.Lgs. 231/2001. In particolare, il Decreto ha ad oggetto la responsabilità amministrativa delle società e degli enti, e mira a disincentivare il compimento di reati aziendali che abbiano l'effetto di favorire in modo ingiusto le organizzazioni aziendali. Con l'introduzione del concetto di responsabilità amministrativa dell'ente, l'intera organizzazione è maggiormente coinvolta nell'individuazione e prevenzione delle frodi societarie, al fine di evitare le conseguenze (sanzioni pecuniarie, sanzioni interdittive, ecc.) che derivano dall'applicazione della norma. Tale coinvolgimento è riscontrabile nella emersione di un Modello Organizzativo efficace e che permetta una piena diffusione dei valori etici e del controllo all'interno dell'organizzazione aziendale. L'impatto della legge 231 è stato notevole in termini di incentivo alle imprese nella messa in atto di attività di gestione dei rischi di reato e di prevenzione e individuazione delle frodi societarie. Infatti, con essa molte grandi organizzazioni hanno dovuto affrontare il tema della gestione di tali rischi, implementando apposite strutture di governance e migliorando il Sistema di Controllo Interno nel suo complesso. In conclusione, l'implementazione dei controlli fin qui discussi ha permesso alle aziende di evitare il rischio di incorrere in sanzioni, derivanti dall'applicazione della normativa sulla responsabilità amministrativa, disincentivare le pratiche corruttive all'interno dell'organizzazione, migliorare la reputazione aziendale e di conseguenza l'*appeal* dell'impresa in termini competitivi, conservare il valore del patrimonio aziendale.

In linea con quanto appena affermato, l'impegno delle imprese nel disporre Sistemi di Controllo in grado di prevenire il compimento di reati e le relative conseguenze, è confermato dallo svolgimento di attività di fraud auditing e la funzione di Internal Audit, rivolgendosi nella sua analisi al più ampio Sistema dei Controlli aziendali, sembra essere la figura più idonea allo svolgimento di attività di *fraud prevention and detection*. Come si è detto, ogni frode aziendale è rappresentata dall'aggiramento del sistema dei controlli interni o dallo sfruttamento di debolezze di tale sistema attraverso cui si attenta al patrimonio della società, e l'Internal Audit costituisce la funzione cui spetta fornire un'assurance sulla corretta predisposizione ed attuazione dei controlli. Ovviamente, partendo dal presupposto che per un internal auditor non sia possibile eliminare completamente il rischio di frode, scovando ogni possibile comportamento illecito, è comunque auspicabile che attraverso un'attenta analisi sull'adeguatezza del Sistema di Controllo Interno, si possa fornire una maggiore garanzia affinché la frode non avvenga. A tal riguardo, il fraud auditing si può suddividere in tre tipologie di attività:

- 4) Auditing per il rafforzamento del sistema di controllo preventivo;
- 5) Auditing di tipo ispettivo per l'individuazione di atti sospetti;
- 6) Investigazione di gravi sospetti di atti illeciti al fine di determinare le responsabilità e i danni subiti.

In merito alla prima forma di fraud auditing, è chiaro come essa si svolga in via assolutamente preventiva al fine di ottenere un complessivo livello di assurance sul rischio di frode intrinseco nei processi aziendali. Infatti, l'attività si svolge nelle modalità dell'*operational audit* ed ha l'obiettivo di individuare le aree grigie aziendali dove è maggiore la probabilità che si realizzi un caso di frode. Successivamente, l'Internal Audit può svolgere, al fine di identificare e prevenire il compimento di illeciti, un monitoraggio sui cosiddetti *red flag*. I red flag, o segnali di allarme, rappresentano segnali di possibili azioni fraudolente che possono emergere ad ogni livello del controllo e da cui è possibile partire per valutare se occorre approfondire o meno l'anomalia rilevata. Infine, l'attività di fraud auditing entra nel vivo qualora vi siano gravi sospetti circa il compimento di atti illeciti. In tal caso, è richiesta all'auditor una conoscenza delle diverse forme di frode e delle modalità con cui esse si realizzano. L'internal auditor deve altresì possedere le competenze necessarie alla gestione di un caso di frode, così come previsto dagli Standard della Professione, e qualora queste non siano sufficienti deve richiedere il supporto di specialisti esterni.

In accordo con quanto esaminato nelle pagine precedenti, è possibile dunque sostenere che l'internal auditing costituisce una funzione chiave per il corretto funzionamento del Sistema di Controllo Interno, oltre che per la rilevanza strategica che esso assume in sede di definizione del livello di rischio residuo. Si è altresì insistito sull'importanza della generazione di un circolo vizioso positivo che la Funzione è in grado di avviare attraverso il processo di *follow-up*, e non limitando il suo ruolo alla sola emanazione di un giudizio di assurance, bensì arricchendolo fornendo al senior management la propria consulenza in materia di Governance, Controllo Interno e Risk Management. Ancora, si è detto che l'esercizio dell'attività di auditing è possibile solo se viene mantenuta salda l'indipendenza del revisore interno, sia che la Funzione venga svolta internamente sia che venga svolta in *outsourcing*, e che il suo giudizio sia frutto di una valutazione obiettiva e non condizionata da fattori esterni.

Tuttavia, occorre ricordare che quanto fin qui emerso è frutto di testi teorici e, pertanto, si è ritenuto opportuno approfondire la ricerca con un'analisi empirica delle funzioni di Internal Audit all'interno delle società quotate. Nel farlo, è stato selezionato un campione casuale di venti società (dieci delle quali riconducibili al ramo *industrial*, e dieci al settore *financial*) tra quelle che compongono il FTSE MIB. Di queste società è stata analizzata la struttura fondamentale della Funzione di Internal Audit facendo riferimento a quanto riportato all'interno di ciascuna *Relazione sul governo societario e gli assetti proprietari*, nonché alle *Linee guida del Sistema di Controllo Interno e di Gestione dei Rischi (SCIGR)*.

In primo luogo, l'analisi empirica ha previsto l'osservazione di elementi fondamentali quali le attribuzioni, le linee di riporto e i flussi di comunicazione. In un momento successivo, sono stati osservati ulteriori elementi, tra cui la presenza o meno

dell'attività di auditing sul processo di gestione delle segnalazioni (cd. *Whistleblowing*) e la periodicità della reportistica di internal auditing. Infine, si è ritenuto essenziale considerare la presenza, tra le attività menzionate, dello svolgimento di fraud auditing, e quindi l'impegno a prevenire e individuare le frodi aziendali da parte della funzione di revisione interna.

Dall'analisi svolta è emerso un generale allineamento rispetto ai principi discussi e agli argomenti trattati nei primi due capitoli. In particolare, con riferimento ai *driver* fondamentali. Con riguardo alle attribuzioni, si evince come le funzioni di internal auditing delle società analizzate facciano esplicito riferimento ai compiti, ruoli, poteri e doveri attribuitigli dagli Standard Internazionali della Professione, con indicazione della funzione di "valutare l'operatività e l'idoneità del Sistema di Controllo Interno e di Gestione dei Rischi". L'unica differenza emerge nel settore finanziario, nel quale è prevista altresì la valutazione del processo di definizione del Risk Appetite Framework (RAF) e del RAF stesso. Altro elemento su cui occorre soffermarsi è la gestione centralizzata delle attività di auditing, fattore riscontrato nella quasi totalità dei casi esaminati. Infatti, ad eccezione di FinecoBank, la cui attività di internal auditing viene gestita in outsourcing da UniCredit e comunque attraverso una struttura centralizzata, in tutti gli altri casi si sviluppa una Direzione Generale di Audit nella capogruppo, la quale svolge la propria attività verso tutte le società controllate, o perlomeno verso le società del gruppo che non dispongono di un proprio Internal Audit. Tuttavia, questo aspetto non sembra essere pienamente in linea col principio per il quale l'audit debba calarsi nella singola realtà aziendale di riferimento e in quanto tale assumere una particolare conformazione. Infatti, i grandi gruppi aziendali possono essere caratterizzati da un'eterogeneità di business e possono svolgere un numero elevato di attività diverse tra loro, per cui si renderebbe necessaria la presenza di funzioni e strutture di controllo distinte.

Per quanto riguarda le linee di riporto, anche in questo caso è emersa una generale attitudine all'assecondare gli standard internazionali e, in particolare, il Codice di Autodisciplina delle società quotate di Borsa Italiana S.p.A. Infatti, nelle società che adottano un sistema di governance tradizionale (90% dei casi esaminati) il Responsabile della Funzione Internal Audit ha obbligo di riporto gerarchico verso il Consiglio di Amministrazione e, nello specifico, verso il Presidente del CdA, rapporto necessario ai fini del mantenimento delle condizioni di indipendenza.

Con riguardo al terzo *driver*, dall'analisi si evince l'esistenza di flussi di comunicazione periodici tra la Funzione e i seguenti organi sociali: Presidente del Consiglio di Amministrazione e Presidente del Collegio Sindacale, Comitato Controllo e Rischi e Amministratore Incaricato del SCIGR. Inoltre, l'attività di internal auditing spesso si presta all'esecuzione di specifiche verifiche a supporto di tali organi, a cui seguono altrettanto specifiche relazioni. Tale attività di verifica viene svolta anche a supporto dell'Organismo di Vigilanza, di cui spesso il Responsabile della

Funzione è un componente, e rispetto al quale la funzione si presta a esserne il “braccio operativo”.

Con riguardo alla periodicità della reportistica, è emersa una maggiore frequenza nell’invio dei report sulle attività di audit svolte all’interno dei grandi gruppi finanziari. Tale dato può essere giustificato dal fatto che nel settore finanziario è presente un maggiore livello di regolamentazione e ciò induce le società del settore a presentare una reportistica più frequente nell’espletamento delle attività di audit. Quanto alla attività di audit sul processo di gestione delle segnalazioni, invece, esso appare più frequente nei gruppi industriali con dati che mostrano come 7 aziende su 10 vedono la funzione di Internal Audit impegnata su tale fronte, rispetto alle 2 aziende su 10 nel ramo finanziario.

Per concludere, durante lo svolgimento dell’analisi è stata posta particolare attenzione alla presenza o meno di riferimenti in merito allo svolgimento di attività di fraud auditing. In particolare, se attraverso le verifiche sul corretto funzionamento del processo di gestione delle segnalazioni la funzione Audit è in grado di condurre a un *improvement*, seppur indiretto, del Sistema di Controllo, la riduzione del più generale rischio di frode passa necessariamente attraverso l’attività di fraud auditing. Rispetto al campione esaminato, è emerso che solo il 25% delle società (Telecom, Leonardo, Generali, Unipol, Fineco) ponga in essere (o meglio lo esponga all’interno della propria Relazione) l’attività di individuazione e prevenzione delle frodi aziendali e il dato, seppur non necessariamente indicativo dell’assenza del concreto svolgimento di tale attività, appare comunque non soddisfacente rispetto all’importanza che le frodi ricoprono in tema di controllo interno e *risk management*. Tuttavia, va tenuto a mente che le informazioni fornite nella presente ricerca sono estrapolate dall’informativa resa pubblica dalle società esaminate e non costituiscono, pertanto, un dato esauriente circa l’effettivo impegno dell’Internal Audit nella lotta alle frodi aziendali.

Per tale motivo, è stato analizzato il caso di un’azienda e delle modalità attraverso le quali è stato gestito internamente un evento riconducibile al fenomeno delle frodi. Di tale società non potrà essere fatto esplicito riferimento né al suo nome, né agli attori coinvolti nell’illecito, per ragione di riservatezza.

Dopo aver appurato la corretta aderenza della funzione di Internal Audit agli Standard Internazionali, sia prima che dopo il compimento del reato, è stata analizzata a fondo la vicenda al fine di comprendere le modalità con le quali è stata compiuta la frode e le azioni poste in essere dall’Internal Audit al fine di gestire la situazione. In particolare, la vicenda trae origine da alcune operazioni di M&A poste in essere dal Gruppo e dall’occultamento di importanti informazioni aziendali riguardanti l’acquisizione di una società che da ora in avanti verrà definita Target. Quest’ultima, al momento della sua acquisizione, vantava due grandi progetti, che per semplicità espositiva verranno definiti Progetto 1 e Progetto 2, sui quali Target vantava dei crediti. La causa principale del problema va rintracciata in un lungo “braccio di ferro”

tra i dirigenti di Target e le controparti interessate in merito alla determinazione del prezzo per l'estinzione del debito di tali questi ultimi. Infine, la vicenda è stata caratterizzata dalla pressione degli organi di vigilanza che, in prossimità delle date di chiusura dei bilanci del Gruppo e della società Target, richiedevano un accordo definitivo. Tali pressioni hanno portato alla contrattazione di un accordo preliminare, il quale prevedeva l'estinzione del debito attraverso il pagamento di cifra pattuita, di importo inferiore a quanto inizialmente richiesto.

La scoperta della frode è dovuta al fatto che un soggetto apicale di Target, d'ora in avanti indicato con l'appellativo "Dirigente", nel tentativo di occultare l'importo pattuito in sede di accordo preliminare, ha alterato l'informativa contenuta in tale documento fornendo agli organi di vigilanza, a fronte delle continue richieste, una documentazione falsa con impatti rilevanti sui bilanci di Target. Nello specifico, la frode è stata scoperta dopo che il Dirigente ha inviato due volte la medesima mail, ma con allegati differenti: al primo invio il contenuto della mail includeva una versione falsa del documento, dove l'importo pattuito per l'estinzione del debito era stato sostituito con la sigla "T.B.C." (*To Be Confirmed*); al secondo invio, invece, all'interno della mail vi era la versione originale, la quale riportava il valore preventivamente concordato.

Appurata la differenza tra i documenti inviati, gli organi di controllo della società hanno provveduto a convocare un *meeting* con gli esponenti del top management aziendale, incluse le persone coinvolte nella vicenda. A questo punto la Società ha richiesto l'intervento della funzione di Internal Audit al fine di chiarire la vicenda e accertare le responsabilità di ciascuna persona coinvolta. In particolare, è stato richiesto all'Internal Audit di: eseguire un'analisi del contesto nel quale si è svolta la vicenda, ricostruire la cronologia degli eventi; identificare le altre persone coinvolte nella vicenda; valutare gli impatti potenziali della frode; verificare l'esistenza di ulteriori alterazioni e, in caso positivo, accertarne le responsabilità.

Al fine di fornire un *output* in merito a tali richieste, la funzione di Internal Audit del Gruppo ha deciso di far ricorso all'assistenza e al coinvolgimento di personale esterno altamente qualificato in materia di *fraud investigation* al fine di:

4. Svolgere un'analisi sui computer aziendali (*e-Discovery*) delle persone coinvolte nella vicenda. L'attività ha previsto la raccolta di informazioni digitali attraverso l'utilizzo di appositi software, attraverso i quali è possibile estrarre dati di diverso genere dai notebook, dai server e dalla posta elettronica.
5. Analizzare e valutare la frode e i relativi impatti, partendo dallo svolgimento di interviste con le persone coinvolte nella vicenda al fine di ricostruire la cronologia degli eventi, fino ad arrivare alla comprensione dei ruoli e delle responsabilità nel compimento dell'illecito, nonché del possibile impatto che esso avrebbe avuto sui bilanci della società qualora non fosse stato scoperto.

6. Analizzare ulteriori potenziali alterazioni dell'informativa aziendale attraverso il confronto tra gli ulteriori documenti inviati dalla società presenti nelle mail con la documentazione originale estratta dai computer, e verificando, attraverso appositi programmi, se la stessa documentazione ha subito particolari modifiche nel tempo.

In sintesi, a seguito delle analisi effettuate dagli esperti del *forensic*, la funzione di Internal Audit è pervenuta alle seguenti conclusioni: in primo luogo, è stato attribuito alla persona responsabile del “doppio invio” della documentazione incriminata il ruolo di principale esecutore dell'azione fraudolenta. L'addebito di tale responsabilità è principalmente dovuto alla confessione di costui in sede di intervista. Successivamente, sono state svolte una serie di *Scenario Analysis* al fine di comprendere l'impatto che tale manipolazione avrebbe avuto sul bilancio qualora essa non fosse stata scoperta. In particolare, senza entrare in dettaglio dell'analisi sui riflessi contabili dell'operazione, va detto che l'evidenza di uno specifico importo all'interno di un accordo preliminare, seppur non definitivo, avrebbe aumentato la probabilità di perdita legata alla mancata recuperabilità del credito e, di conseguenza, una svalutazione dello stesso in bilancio attraverso la costituzione di un fondo svalutativo.

Attraverso lo studio di questa vicenda è stato possibile dimostrare come un singolo individuo sia in grado, anche in assenza di particolari interessi o vantaggi personali, di aggirare i controlli e i modelli organizzativi interni e di porre in essere comportamenti in contrasto con la legge o con i regolamenti aziendali. In particolare, la vicenda narrata pone in rilievo le caratteristiche tipiche del frodatore economico. Infatti, come è stato visto all'interno del precedente capitolo, le capacità tecniche da egli possedute creano i presupposti per il compimento della frode e la fiducia e l'onorabilità che vanta verso gli altri fanno sì che il comportamento illecito passi inosservato.

In ogni modo, nel caso esaminato è possibile valutare positivamente l'azione sinergica dei controlli aziendali, dalle prime linee nella comunicazione dell'errore riscontrato fino alla gestione successiva da parte della funzione di Internal Audit, la quale ha permesso l'individuazione della frode e la prontezza della risposta con la quale sono state accertate le responsabilità e poste in essere le dovute azioni correttive.

L'analisi condotta sul fenomeno delle frodi aziendali e l'ipotesi per la quale la funzione di Internal Audit costituisca un'unità aziendale idonea a contrastarlo può concludersi con un esito positivo. Si può quindi definitivamente affermare che le attività di internal auditing assumono un ruolo rilevante in termini di prevenzione, individuazione e gestione delle diverse fattispecie di illecito aziendale.

In particolare, è possibile affermare che le attività di auditing hanno efficacia massima nella fase di prevenzione delle frodi, in virtù della conoscibilità degli internal auditor dell'impresa, in generale, e del Sistema di Controllo Interno, nello specifico. Infatti, la funzione di revisione interna rappresenta, come è stato affrontato in precedenza, il

braccio operativo dell'Organismo di Vigilanza e in quanto tale sono ad essa demandate le attività di risk assessment e di ispezione al fine di individuare le criticità all'interno del sistema dei controlli e di ridurre il rischio di commissione del reato ad un livello ritenuto accettabile. In questi termini, si conferma la rilevanza del contributo offerto dal legislatore italiano mediante il Decreto Legislativo n. 231/2001 in materia di responsabilità amministrativa degli enti, con il quale le imprese sono state poste in prima linea, di fianco alle autorità nazionali, nella lotta alle frodi aziendali. Quindi, mediante una visione "dall'alto" dell'impresa, l'Internal Audit è in grado di individuare le "aree grigie" del Sistema di Controllo Interno e di promuovere azioni di implementazione di nuovi controlli o di miglioramento dei controlli esistenti in tali aree, rafforzando i meccanismi di controllo e di prevenzione dei rischi di frode.

Inoltre, come è stato visto durante la trattazione del caso aziendale, l'Internal Audit rappresenta la funzione alla quale il top management attribuisce il compito di indagare su eventuali sospetti di illeciti. Le indagini poste in essere dalla Funzione si pongono come obiettivo quello di accertare le responsabilità di chi ha compiuto l'illecito, quantificare i danni e gli impatti della frode sulla società e su terzi e promuovere miglioramenti al Sistema di Controllo Interno. Nello svolgimento di questa attività, tuttavia, si richiede all'Internal Audit il possesso di conoscenze e competenze specifiche in materia di frodi. In particolare, gli internal auditor dovranno conoscere a fondo le dinamiche fraudolente e le diverse modalità con le quali il fenomeno si realizza, dovranno conoscere le modalità attraverso cui si esegue un'attività di *fraud investigation* e dovranno saper utilizzare particolari software per lo svolgimento dell'incarico. Il possesso di tali competenze è in genere avvalorato dal conseguimento di un'apposita certificazione, la quale attribuisce agli internal auditor il titolo di *Certified Fraud Examiner* (CFE).

Nel caso in cui la funzione di Internal Audit non posseda al suo interno un adeguato livello di conoscenza in materia di frodi, è prassi diffusa, e confermata dall'analisi del caso aziendale visto precedentemente, quella di ricorrere a soggetti esterni specializzati in *forensic and anti-fraud services*. Anche in tal caso, però, la funzione di revisione interna mantiene un ruolo di gestione dell'intera dinamica di frode e di coordinamento dell'intero team di azione, internalizzando quelle competenze necessarie per l'assolvimento dell'incarico. Inoltre, il ricorso a persone esterne permette alla funzione di Internal Audit di aumentare il livello di indipendenza nel suo giudizio che, se già ritenuto imprescindibile, risulta ancor più importante nel momento in cui deve essere gestito internamente un reato societario.