LUISS

Corso di laurea in Amministrazione, finanza e controllo

Cattedra Corporate governance e internal auditing

Il cambiamento del C.d.A. e della governance a seguito di scandali contabili o societari nelle società quotata

Chiar.mo Prof. Bozzolan Saverio

RELATORE

Chiar.mo Prof. Ricci Sante

CORRELATORE

Antonella Moschetta
Matr. 780311

CANDIDATO

Anno Accademico 2024/2025

INDICE

Introduzione

Nel corso degli ultimi decenni, il panorama economico e finanziario internazionale è stato profondamente scosso da una serie di gravi scandali contabili e societari che hanno avuto una forte risonanza mediatica e impatti devastanti sul tessuto economico. Tra i casi più emblematici si possono citare i fallimenti clamorosi di colossi come Enron e WorldCom negli Stati Uniti, e lo scandalo Parmalat in Italia. Questi eventi hanno rappresentato un vero e proprio campanello d'allarme per le istituzioni e i mercati, evidenziando in modo drammatico le fragilità e le inefficienze presenti nei sistemi di governance delle società quotate.

Tali scandali hanno messo in luce criticità strutturali significative, tra cui la mancanza di trasparenza nei processi decisionali aziendali, l'insufficiente indipendenza e autonomia del Consiglio di Amministrazione (CdA), e la debolezza dei meccanismi di controllo interno. Queste carenze hanno favorito, se non direttamente agevolato, comportamenti opportunistici e pratiche illecite da parte dei vertici aziendali, minando in modo sostanziale la fiducia degli investitori e compromettendo la stabilità e la credibilità dei mercati finanziari a livello globale.

In risposta a tali fallimenti sistemici, i legislatori nazionali e internazionali, le autorità di regolamentazione e vigilanza, nonché gli stessi mercati finanziari, hanno avviato una serie di interventi normativi e riforme strutturali. Queste misure sono state finalizzate al rafforzamento del sistema di controlli aziendali, alla ridefinizione delle responsabilità degli amministratori e all'introduzione di best practice di governance societaria, volte a prevenire il ripetersi di simili crisi.

L'obiettivo principale di questa tesi è quello di esaminare in che modo tali scandali abbiano influenzato in profondità la composizione e le funzioni del Consiglio di Amministrazione, determinando un'evoluzione nelle pratiche di

corporate governance tanto in ambito italiano quanto nel contesto internazionale. In particolare, si intende analizzare come la governance delle società quotate si sia trasformata per rispondere alla crescente esigenza di trasparenza, accountability e tutela degli stakeholder.

Il lavoro si articola in più capitoli, a partire da un primo capitolo di inquadramento teorico e normativo, che analizza il ruolo del sistema di controllo interno all'interno delle organizzazioni. In questo contesto, si mettono in evidenza le funzioni fondamentali legate alla gestione dei rischi e alle attività di audit interno, ponendo in risalto la funzione di presidio che tali meccanismi svolgono nel prevenire e contrastare condotte fraudolente e scorrette.

Nel secondo capitolo si procede a un approfondimento del fenomeno delle frodi aziendali, partendo da una definizione concettuale di "frode" e analizzando le principali categorie di illeciti che si possono verificare all'interno di un'impresa. Vengono inoltre analizzati i fattori di rischio che ne favoriscono l'insorgenza, come ad esempio conflitti di interesse, pressioni per il raggiungimento di obiettivi economici, carenze nei controlli interni e cultura aziendale inadeguata. La parte conclusiva del capitolo propone un'analisi delle misure preventive, con particolare attenzione al Decreto Legislativo 231/2001, che ha introdotto in Italia la responsabilità amministrativa delle persone giuridiche per determinati reati commessi nel loro interesse o vantaggio.

Questa tesi si conclude con il terzo capitolo, nel quale viene effettuata l'analisi del caso aziendale Bio-On. Una startup bolognese attiva nel settore delle bioplastiche, un tempo celebrata come "unicorno" per aver superato il miliardo di euro di valutazione, è crollata nel 2019 sotto il peso di gravi accuse giudiziarie. L'azienda, che prometteva innovazioni rivoluzionarie nei materiali sostenibili, è finita al centro di un'indagine condotta dalla Procura di Bologna, che ha portato alla luce una realtà ben diversa: brevetti mai registrati o inesistenti, fatturati irrisori e debiti per circa 70 milioni di euro. Il tracollo si è rivelato inevitabile.

Il fondatore Marco Astorri e il vicepresidente Guido Cicognani sono stati riconosciuti colpevoli di bancarotta fraudolenta e altri reati, ricevendo rispettivamente condanne a cinque anni e due mesi di reclusione. Il caso, che aveva suscitato grande clamore nel mercato AIM di Piazza Affari, si è chiuso con otto condanne, un’assoluzione e numerosi strascichi legali ed etici.

DISPOSIZIONI NORMATIVE ITALIANE E IL SISTEMA DI CONTROLLO INTERNO

1.1 Il Sistema di Controllo Interno e le Sue Funzioni

Il sistema di controllo interno si configura come l'insieme delle regole, procedure e strutture organizzative finalizzate a garantire un'efficace identificazione, misurazione, gestione e monitoraggio dei principali rischi, con l'obiettivo di contribuire al successo sostenibile dell'azienda.[1]

Il controllo interno è un processo continuo realizzato dal Consiglio di Amministrazione (CDA), dai manager e da tutti i membri dell'azienda nel tentativo di fornire una ragionevole sicurezza che gli obiettivi aziendali vengano raggiunti.[2]

In generale, tali obiettivi possono essere classificati nei seguenti tre gruppi:

- Efficacia ed efficienza delle attività operative (Operations),
- Affidabilità delle informazioni finanziarie (Financial reporting),
- Conformità alle leggi e regolamenti in vigore (Compliance).

Prima di entrare nella definizione di controllo interno, evidenziamo alcuni punti fondamentali per comprendere al meglio questo concetto:

→ è uno strumento per il raggiungimento di un fine: il controllo interno è un mezzo, finalizzato a garantire il buon funzionamento dell'organizzazione;

[1] La figura professionale dell'Internal Auditor (IA) e le fasi della sua attività; Alberto Oliva, Patrizia Riva

[2] Gli organi di controllo aziendale. I rapporti di collaborazione del sistema di controllo interno; Andrea Onori

→ prevede la responsabilità condivisa: non si tratta solo di un insieme di procedure e manuali, ma di un processo che coinvolge le risorse umane a ogni livello dell'organizzazione;

→ garantisce ragionevole certezza, non assoluta: il controllo interno può garantire un livello ragionevole di certezza sul raggiungimento degli obiettivi, ma non può fornire una sicurezza assoluta.

Il sistema di controllo interno è progettato per raggiungere gli obiettivi attraverso una o più categorie con alcune aree che possono sovrapporsi. I livelli di controllo[3] all'interno di questo sistema sono ampiamente categorizzati come segue:

- **Primo livello di controllo**: sono i controlli operativi (di linea) che si applicano ai singoli processi. Solitamente questi controlli sono mantenuti dai manager di diversi centri di responsabilità, e il loro scopo è garantire che le operazioni siano svolte nel modo giusto;

- **Secondo livello di controllo**: riguarda la supervisione del processo di gestione dei rischi e di controllo, assicurandosi che tali processi siano conformi agli obiettivi dell'azienda. Tra i controlli di secondo livello troviamo il *Risk Management* (che misura i rischi relativi alle diverse aree aziendali), la funzione di *Compliance* (che garantisce il rispetto delle normative e la correttezza delle procedure) e i dirigenti responsabili della redazione dei documenti contabili societari;

- **Terzo livello di controllo**: individua eventuali violazioni delle procedure e delle regolamentazioni. Inoltre, valuta periodicamente la completezza, l'adeguatezza, la funzionalità e l'affidabilità del sistema di controllo interno. La funzione di *Internal Audit* è fondamentale in

[3] I controlli sulle diverse tipologie di realtà e prospettive; Andrea Dello Strologo

questo contesto, poiché fornisce un'assurance indipendente sul disegno e sul funzionamento del sistema di controllo interno, in particolare sui livelli primo e secondo.

1.2 I Diversi Componenti del Sistema di Controllo Interno

Il Rapporto CoSO (*Committee of Sponsoring Organizations of the Treadway Commission*) e il relativo modello più aggiornato fino a ottobre 2023, Internal Control Integrated Framework definiscono componenti fondamentali per la creazione di un Sistema di Controllo Interno. Questi componenti sono tutti strettamente interconnessi agli obiettivi aziendali in termini di efficacia operativa, adeguatezza informativa e conformità alla normativa, e si articolano nei seguenti punti[4]:

-Ambiente di controllo (*Control Environment*): rappresenta la "cultura" dell'azienda e costituisce le fondamenta su cui si basano le altre componenti del sistema di controllo. Include valori etici, l'integrità del management e la filosofia di gestione del rischio. La cultura aziendale deve essere condivisa tra tutti i livelli dell'organizzazione, al fine di garantire una gestione uniforme e consapevole dei rischi;

-Valutazione del rischio (*Risk Assessment*): prevede identificazione dei rischi, valutazione del rischio e gestione del rischio;

[4] Manuale Internal Audit P.A.C. Compliant; Asur Marche

-Attività di controllo (*Control Activities*): si riferisce alle procedure e alle azioni attuate per raggiungere gli obiettivi aziendali e per garantire che i rischi siano gestiti in modo adeguato[5];

-Informazione e comunicazione (*Information and Communication*): coinvolge lo scambio di informazioni pertinenti all'interno dell'azienda per monitorare e controllare le attività aziendali, assicurando che le informazioni siano accurate e tempestive;

-Monitoraggio (*Monitoring*): è essenziale per assicurarsi che il sistema funzioni in modo efficace nel tempo, con un continuo adattamento a nuove circostanze e situazioni aziendali.

Ambiente di Controllo

L'ambiente di controllo ha un'importanza vitale perché influisce sulla determinazione delle strategie aziendali, sul disegno delle attività e sulla gestione dei rischi. Esso comprende diversi fattori:

-Filosofia della gestione del rischio →l'approccio dell'azienda nel trattare i rischi, che deve essere compreso e condiviso a tutti i livelli. Un atteggiamento coeso sulla gestione del rischio è fondamentale per evitare disallineamenti operativi e per mantenere la coerenza nella gestione del rischio;

-Integrità e valori etici del management →è un elemento determinante per definire una cultura aziendale forte e per garantire che le politiche aziendali siano seguite correttamente. Un codice etico deve andare oltre la semplice osservanza della legge, e la sua applicazione deve essere accompagnata da sanzioni per violazioni;

[5] Risk management e analisi dei processi; Università degli Studi di Teramo- Massimo De Angelis

-Rischio accettabile →riguarda il livello di rischio che l'azienda è disposta ad assumere per raggiungere i propri obiettivi. Questo livello guida la formulazione delle strategie aziendali;

-Composizione e ruolo del Consiglio di Amministrazione (CDA) →un CDA competente, indipendente e con un forte senso etico ha il compito di supervisionare e garantire l'efficacia del sistema di controllo interno. La sua responsabilità include l'assicurare che la gestione del rischio rimanga efficace nel tempo;

-Struttura organizzativa →definisce la gerarchia e le responsabilità, oltre alle modalità con cui le attività sono pianificate, attuate e verificate. Una struttura adeguata facilita l'efficacia del sistema di controllo;

-Deleghe di potere e responsabilità → la definizione chiara dei ruoli, delle responsabilità e delle linee gerarchiche è fondamentale per un'efficace gestione operativa. La delega di poteri permette una maggiore iniziativa da parte del personale, ma deve essere accompagnata da un sistema di monitoraggio per verificare i risultati;

-Competenza e risorse umane →le politiche relative alle risorse umane, comprese assunzioni, formazione e valutazione, sono cruciali per garantire che il personale possieda le competenze necessarie per svolgere i propri compiti in modo efficace. La formazione continua è fondamentale per preparare il personale a rispondere ai cambiamenti dell'ambiente economico e tecnologico.

Valutazione del Rischio

Le considerazioni relative alla valutazione dei rischi nel CoSO Report, sebbene originariamente applicabili al contesto statunitense, sono tuttora rilevanti e condivisibili anche nel contesto italiano. Tuttavia, esistono differenze significative nella concezione del rischio e nell'approccio ad esso tra le due realtà. In particolare, la cultura del rischio è fondamentalmente una cultura manageriale, ampiamente diffusa negli Stati Uniti, ma ancora poco sviluppata in molte organizzazioni italiane, sia pubbliche che private.

Nel contesto italiano, infatti, l'approccio al rischio risulta ancora parziale e incompleto, poiché si concentra principalmente su alcune categorie di rischi, soprattutto quelli di natura patrimoniale e finanziaria, trascurando rischi legati alla gestione operativa quotidiana dell'azienda. Questa focalizzazione sui rischi patrimoniali e finanziari si spiega in gran parte con il rapporto tra debito e patrimonio tipico della cultura aziendale italiana, tedesca e giapponese, in contrasto con la realtà anglosassone e francese, dove le imprese tendono a presentare un'esposizione debitoria più equilibrata rispetto al capitale di rischio.

Le osservazioni eseguite nel Rapporto CoSO riguardo alla valutazione dei rischi delle aziende italiane possono quindi rivelarsi utili, non solo rispetto all'avere sistemi di controllo interno più efficaci, ma anche rispetto all'allargamento della concezione di rischio, considerandolo in un contesto più ampio ed integrato.

Per quanto concerne la seconda componente del sistema di controllo interno, il Framework parte dalla proposta di un processo di identificazione e definizione degli obiettivi aziendali, che è un prerequisito per poter avere una discussione significativa sul rischio. In altre parole, un rischio può essere riconosciuto e analizzato solo in termini del fatto che gli obiettivi che erano stati designati per essere raggiunti non siano stati raggiunti. Sebbene la definizione degli obiettivi non sia effettivamente considerata nei componenti del controllo interno, è un presupposto essenziale.

Gli obiettivi aziendali possono essere rappresentati sia esplicitamente che implicitamente, e sono spesso catturati nella mission aziendale e nei valori aziendali. Ciascuno di tali obiettivi può essere ulteriormente delineato in più obiettivi:

- **Obiettivi operativi**, legati all'efficacia ed efficienza delle attività aziendali influenzati dalle decisioni manageriali sulla struttura e sulle prestazioni.

- **Obiettivi informativi**, relativi alla preparazione di dichiarazioni fattuali e affidabili di posizione finanziaria, principalmente guidati da mandati esterni.
- **Obiettivi di conformità**, che riguardano se l'azienda è conforme alle leggi e regolamenti applicabili come determinato da parti esterne, come la legislazione ambientale.

Dopo aver definito gli obiettivi, a livello di entità e per ogni attività, si procede con l'identificazione, valutazione e analisi dei rischi in un processo continuo e iterativo, che è una parte chiave del sistema di controllo interno. La fase di identificazione dovrebbe includere sia minacce interne (competenza del personale, cambiamenti nei ruoli, natura delle attività aziendali, qualità dei sistemi IT) che esterne (cambiamenti tecnologici, cambiamenti dei bisogni dei consumatori, concorrenti, ambiente naturale ed eventi economici). Entrambi i fattori possono avere un impatto su qualsiasi obiettivo aziendale, esplicito o implicito.

Esistono diverse tecniche per identificare i rischi, molte delle quali utilizzano tecniche quantitative e qualitative per determinare le priorità e identificare le aree di alto rischio. L'analisi dei fattori economici e industriali che influenzano l'attività aziendale, la revisione di un piano strategico e l'analisi del settore sono tecniche comunemente utilizzate. Ciò che è importante, tuttavia, è che l'attenzione specifica sia diretta ai determinanti e alle cause che possono aggravare un rischio. Alcuni fattori da considerare includono:

- Mancato raggiungimento degli obiettivi precedenti.
- Competenza del personale.
- Cambiamenti nelle condizioni di business.
- Posizione geografica delle attività.
- Attività specifiche che contano per l'azienda.
- La complessità di alcuni dei processi.

Dopo aver identificato i principali rischi è possibile valutarli su diversi parametri, come la significatività del rischio, la possibilità che si materializzi e le azioni necessarie per affrontarlo, comprese quali interventi implementare.

Tuttavia, la valutazione del rischio deve essere differenziata dalla gestione del rischio, il passo successivo nel processo. Sebbene la valutazione sia un elemento chiave del controllo interno, le azioni specifiche intraprese per controllare i rischi sono incluse nel processo manageriale ma non costituiscono alcun componente del controllo interno.

Per valutare con precisione i rischi di un'impresa, le organizzazioni devono dotarsi di un meccanismo che possa percepire i cambiamenti nell'ecosistema di un'impresa che possono influire sulla sua capacità di raggiungere gli obiettivi dell'azienda. Pertanto, è necessario disporre di un sistema informativo che consenta di monitorare gli eventi e le attività che possono richiedere una risposta specifica da parte dell'azienda.

Infine, nelle piccole e medie imprese italiane, dove la formalizzazione degli obiettivi è spesso meno chiara e la struttura è più centralizzata, la valutazione dei rischi può essere più dinamica e strettamente legata alle operazioni quotidiane. In questi contesti, la valutazione dei rischi tende a essere più informale, ma ugualmente efficace, poiché coinvolge i dirigenti direttamente nelle attività operative. Questo approccio consente una valutazione più pratica dei rischi, grazie alla conoscenza diretta delle informazioni e delle problematiche aziendali.

Attività di controllo

Le attività di controllo sono l’insieme delle politiche e delle procedure attuate per garantire al management che le sue direttive vengano eseguite correttamente. Queste sono essenziali per mitigare i rischi che potrebbero influire sul raggiungimento degli obiettivi aziendali e possono essere classificate in tre ampie funzioni:

1. attività di controllo relative agli aspetti operativi;
2. attività di controllo sulle informazioni di bilancio;
3. attività di controllo sul rispetto delle normative legali e regolamentari.

La natura delle attività di controllo dipende dalla realtà aziendale specifica, considerando il settore in cui l'impresa opera, la sua dimensione, la missione e gli obiettivi, nonché i rischi connessi. Il Rapporto CoSO offre una panoramica di alto livello su alcune azioni di controllo e queste azioni possono essere personalizzate alle esigenze della singola organizzazione. Tra queste, possiamo citare:

-controlli preventivi, simultanei e successivi: che comprendono, ad esempio, l'analisi gestionale delle prestazioni aziendali rispetto ai budget o alle proiezioni o ai risultati precedenti;

-controlli manuali o automatizzati: i controlli manuali, in particolare, devono enfatizzare il principio della separazione dei compiti per minimizzare il potenziale di errori o irregolarità. Ad esempio, è importante che le attività di autorizzazione delle operazioni, contabilizzazione e gestione dei beni siano svolte da persone diverse. Un esempio pratico è quello in cui la persona che autorizza le vendite a credito non debba essere la stessa che si occupa della contabilità clienti e degli incassi;

- controlli manageriali e tecnico-operativi: riguardanti il monitoraggio delle operazioni e delle risorse aziendali;

- controlli fisici e basati sugli indicatori: i controlli fisici comprendono attività come l'inventario di attrezzature e scorte, mentre quelli basati su indicatori sono utili per analizzare comparativamente dati operativi o finanziari;

-controlli di processo e dei dati: mirano a verificare l'accuratezza, la completezza e la registrazione corretta delle operazioni aziendali. I dati inseriti nei sistemi informatici sono sottoposti a procedure automatiche di controllo e confrontati con archivi di verifica approvati;

- controlli delle procedure di autorizzazione: possono essere generali, se riguardano operazioni simili, o specifici, se concernono singole operazioni particolari

Uno dei capitoli del CoSO Framework è completamente dedicato ai sistemi informativi, facendo notare le differenze tra i controlli applicabili ai sistemi manuali e quelli computerizzati, pur sottolineando che i concetti di controllo restano sostanzialmente gli stessi. In generale, i controlli sui sistemi informativi possono essere suddivisi in controlli generali e controlli applicativi. I controlli generali riguardano operazioni come l'acquisto, lo sviluppo e la manutenzione del software di sistema e la protezione degli accessi, mentre i controlli applicativi si concentrano sulle procedure automatizzate e manuali per monitorare l'elaborazione delle operazioni.

Tuttavia, in Italia, le attività di controllo dei sistemi informativi sono spesso ridotte a semplici operazioni, come quelle di natura operativa (ad esempio, le attività di accesso e backup). Al contrario, i controlli di ordine superiore, come il frequente aggiornamento delle password o la creazione di piani di ripristino in caso di disastro IT, restano trascurati. Ciò può verificarsi anche nelle piccole e medie imprese, nelle quali alcune attività di controllo non vengono applicate, poiché la direzione può comunque dirigere il controllo in modo efficace. In questi ambienti, alcune attività di controllo saranno difficili da applicare e alcune potrebbero non essere praticabili all'interno di una struttura più piccola, come la separazione dei compiti. In questi casi, una soluzione può essere rappresentata dalla supervisione diretta del titolare dell'impresa, che assicura comunque il necessario controllo.

Ad esempio, in caso di rischi relativi a pagamenti irregolari, può accadere che il titolare sia l'unico autorizzato a firmare assegni o che la banca invii gli estratti conto mensili in busta chiusa per consentire una verifica diretta. Nelle piccole e medie imprese si riscontrano anche difficoltà nei controlli sui sistemi informativi, soprattutto a causa della scarsa formalizzazione dei processi di verifica. Una possibile soluzione potrebbe derivare dal maggiore coinvolgimento dei vertici aziendali nelle operazioni quotidiane.

Questo approccio consentirebbe ai responsabili di accedere e valutare più frequentemente le informazioni prodotte dai sistemi informativi, utilizzando la loro conoscenza diretta dell'attività per identificare potenziali errori con maggiore sicurezza.

Il controllo interno non è ancora molto avanzato, in generale, in Italia. Quelle procedure sono state generalmente adottate in reazione a crisi e, in quanto tali, sono sovrapposte le une alle altre in modo disordinato e senza molta coordinazione efficace. Concezione e implementazione di un tale approccio implica un rinnovamento concettuale: le aziende italiane dovrebbero considerare se e quanto devono adattare le loro attività di controllo, abbandonando processi inutili, ridondanti o obsoleti e concentrando l'attenzione su quelle aree che sono meno protette di quanto dovrebbero essere.

Informazione e comunicazione

Le informazioni sono essenziali per la gestione dell'azienda, poiché consentono di monitorare e controllare tutti i processi aziendali e di tenere sotto controllo le variabili esterne che influenzano l'impresa. La qualità e la quantità delle informazioni condivise all'interno di un'organizzazione sono determinanti per valutare l'efficacia e l'efficienza della gestione, la correttezza delle informazioni di bilancio e la conformità alle normative. Una delle principali problematiche legate a questa componente del sistema di controllo interno riguarda da un lato la qualità delle informazioni, intesa come contenuto, puntualità, aggiornamento, precisione e chiarezza, e dall'altro l'efficienza nell'elaborazione dei dati. Il contesto italiano non si discosta molto da quello di altri Paesi, come gli Stati Uniti, e presenta ampi margini di miglioramento in quest'area.

Un aspetto cruciale da considerare quando si esamina la componente informativa di un sistema di controllo interno è la tempestività con cui vengono forniti i dati agli utenti aziendali. Infatti, se le informazioni arrivano troppo tardi, con tempi non allineati con il processo o il periodo di riferimento, esse diventano inutili e inefficaci. Ad esempio, non sarà possibile intervenire su eventi passati se i dati arrivano in ritardo. Un sistema

informativo lento rischia di produrre solo informazioni ridondanti e inefficaci per la direzione e per chi è coinvolto nel processo di controllo.

Per questo motivo, è fondamentale non solo identificare chiaramente le informazioni necessarie, ma anche progettare l'intero sistema informativo, assicurandosi che sia coerente con gli obiettivi, le strategie e i fattori critici di successo dell'azienda.
Purtroppo, in Italia e in altri Paesi, il concetto di sistema informativo è spesso confuso con quello di tecnologia. Questo porta molte imprese a concentrarsi più sull'adozione delle ultime novità tecnologiche che sulla creazione di un sistema veramente adatto alle proprie esigenze aziendali. A volte si commette l'errore di pensare che le nuove tecnologie, solo per il fatto di essere moderne, possano garantire un controllo migliore o una gestione più efficiente delle informazioni. In alcune realtà, invece, un sistema più vecchio, ma consolidato e progettato su misura per le esigenze specifiche dell'impresa, può rivelarsi più efficace.

Oltre alle informazioni, un altro elemento essenziale è la comunicazione. Questa è una funzione intrinseca dei sistemi informativi e può riguardare tanto gli interlocutori interni quanto quelli esterni. Nel primo caso, la comunicazione ha l'obiettivo di far comprendere a ciascun membro dell'organizzazione le sue responsabilità e le aspettative nei suoi confronti, consentendo così di segnalare eventuali problemi relativi alla sua attività, in particolare rispetto al sistema di controllo. La comunicazione deve essere continua e fluire in tutte le direzioni: dall'alto verso il basso, dal basso verso l'alto, e in modo trasversale. Un'indagine condotta in alcune grandi organizzazioni, comprese quelle italiane, ha mostrato che le reti di comunicazione informali sono spesso più efficaci e consolidate rispetto a quelle formali, che seguono la gerarchia aziendale. Lo studio ha quindi sottolineato l'importanza di riconoscere anche questi canali informali, che non devono essere ignorati, poiché possono essere utili per sviluppare un sistema di comunicazione adeguato alle necessità di controllo e gestione dell'impresa.

Anche la comunicazione verso l'esterno gioca un ruolo cruciale. In questo caso, non si fa riferimento solo alle informazioni destinate a soci, autorità, analisti e media, ma anche ai dati forniti a clienti, fornitori e banche, ovvero agli interlocutori quotidiani dell'impresa. La comunicazione esterna deve essere attentamente pianificata, valutando

non solo i contenuti, ma anche i canali, le modalità e i tempi. Può essere migliorata aumentando la quantità di informazioni riguardanti bilanci e relazioni periodiche, aumentando la trasparenza, o richiedendo incontri più frequenti con soggetti esterni interessati, non solo a livello societario, per consolidare il controllo aziendale e arricchire il sistema in cui l'impresa opera.

Le comunicazioni aziendali possono assumere varie forme, come manuali, bollettini, promemoria, fogli in bacheca, messaggi vocali o videomessaggi, con un'importante attenzione al tono della voce e alla gestualità. Nelle piccole imprese, i sistemi informativi sono generalmente meno formali rispetto a quelli adottati nelle grandi organizzazioni, ma il loro ruolo rimane comunque significativo. Tuttavia, grazie alle moderne tecnologie informatiche, la formulazione dei dati interni è altrettanto efficace in molte piccole imprese, indipendentemente dalle dimensioni. Le piccole imprese possono beneficiare di un vantaggio rispetto alle grandi organizzazioni, ovvero una comunicazione interna più agevole tra la direzione e i dipendenti. Questo vantaggio deriva dalla minore complessità organizzativa, dalla limitata gerarchia e dalla maggiore presenza e disponibilità del top management. I contatti interpersonali frequenti nelle piccole imprese sopperiscono spesso alla mancanza di un sistema di comunicazione formale, e pertanto vanno considerati con attenzione quando si valuta questa componente del sistema di controllo interno.

Monitoraggio

Le condizioni per le quali i sistemi di controllo interno sono stati originariamente progettati cambiano nel tempo, così come questi stessi sistemi. Pertanto, la direzione dovrebbe periodicamente assicurarsi che la struttura di controllo esistente sia adeguata e pertinente alla gestione del rischio.
Il monitoraggio è la parte del sistema che garantisce che il controllo interno rimanga funzionante. È un esercizio vitale nella valutazione della progettazione del controllo, del timing di esecuzione e dei meccanismi mediante i quali le azioni correttive necessarie vengono adottate.

Ci sono due forme di attività di monitoraggio: attività di monitoraggio continuo e interventi di valutazione specifica.

Il monitoraggio continuo si riferisce alle procedure di controllo che vengono eseguite automaticamente dal sistema e che sono integrate nelle normali operazioni aziendali. Poiché queste operazioni vengono svolte in tempo reale, consentono di rispondere immediatamente a cambiamenti interni ed esterni, risultando così più efficaci rispetto al monitoraggio effettuato tramite valutazioni separate. Più il monitoraggio continuo è efficiente, minore sarà la necessità di ricorrere a strumenti di valutazione specifici.

Tra i controlli continuativi che un'impresa può adottare vi sono attività di supervisione e gestione ordinaria, analisi comparative e riconciliazioni effettuate con documenti di terze parti. Sebbene il monitoraggio continuo offra preziose informazioni sul funzionamento del sistema di controllo interno, è comunque necessario concentrarsi periodicamente sull'efficacia complessiva del sistema, eseguendo valutazioni più approfondite.

Le valutazioni periodiche sono generalmente autovalutazioni, attraverso le quali i responsabili delle singole unità aziendali determinano l'efficacia dei controlli all'interno delle proprie attività. Chi esegue la valutazione deve cercare di comprendere ogni singola attività dell'impresa e ciascun componente del sistema di controllo interno, interagendo con le persone che quotidianamente si confrontano con le procedure aziendali e sono direttamente coinvolte nei controlli. Esistono diversi strumenti di valutazione, come check-list, questionari o diagrammi di flusso, e alcune imprese utilizzano benchmark di riferimento, confrontando la loro situazione con quella di altre aziende che considerano un modello ideale.

Quando i responsabili per la valutazione del sistema di controllo interno si trovano ad affrontare questa attività per la prima volta, possono seguire una procedura che illustra l'approccio da adottare:

-definire le categorie di obiettivi, le componenti del controllo interno e le attività da esaminare, andando a delineare il campo di azione della valutazione;

-identificare le attività di monitoraggio continuo che confermano il corretto funzionamento del sistema di controllo interno;

-valutare l'analisi dei controlli eseguite dai revisori interni, oltre ai rilievi emersi dagli interventi dei revisori esterni;

-determinare le priorità per le aree ad alto rischio che richiedono attenzione immediata;

-sulla base dei risultati ottenuti, elaborare un programma di valutazione, con interventi a breve e lungo termine;

-riunire i soggetti coinvolti nella valutazione, definendo con il team non solo l'ambito e i tempi, ma anche la metodologia, gli strumenti, le informazioni fornite dai revisori interni e dalle autorità, i mezzi per comunicare i rilievi e la documentazione da produrre;

-monitorare l'avanzamento della valutazione e esaminare i risultati ottenuti;

-verificare se sono state adottate azioni correttive e, se necessario, apportare modifiche al programma di valutazione.

Quando, durante il monitoraggio, emergono carenze o potenziali aree di miglioramento, è essenziale che il valutatore segnali tempestivamente tali problemi al responsabile aziendale con il potere di intraprendere le azioni correttive adeguate.

Il grado di formalità del processo di monitoraggio dipende dalla cultura e dalle dimensioni dell'impresa, ma in generale la valutazione del sistema segue le stesse linee guida in tutte le organizzazioni. Le indicazioni raccolte durante il processo rappresentano delle linee guida per il monitoraggio del sistema di controllo interno, che si integrano con il procedimento descritto.

1.3 Le funzioni del comitato in relazione al controllo interno e alla gestione del rischio

L'organo responsabile della supervisione sul corretto funzionamento del Sistema di Controllo e dell'attività di Internal Auditing è il Consiglio di Amministrazione (CdA)[6]. In modo specifico, il CdA è responsabile per l'approvazione, tra le altre cose, della valutazione del rischio e del piano di audit redatto dalla Revisione Interna e la nomina e la rimozione dei responsabili di questa funzione. Pertanto, decidono anche sulla remunerazione del capo, li monitorano per il corretto svolgimento dell'attività di revisione e il budget disponibile per svolgere il mandato.

Tra il Consiglio di Amministrazione e l'Internal Auditing, esiste una figura di raccordo: il Comitato Controllo e Rischi[7], questo comitato è una componente fondamentale del Sistema di Controllo Interno (SCI). Secondo le normative e la regolamentazione, l'adozione di assetti organizzativi e di governo societario adeguati ed efficaci è essenziale per il raggiungimento degli obiettivi aziendali. In questo contesto, il Codice di Corporate Governance stabilisce che ogni impresa debba dotarsi di un sistema di controllo interno e di gestione dei rischi, costituito da regole, procedure e strutture organizzative che consentano l'identificazione, la misurazione e il monitoraggio dei principali rischi.

I controlli, nelle società, sono strettamente legati ai rischi aziendali. L'organizzazione di un sistema di controllo non solo consente di gestire i rischi, ma implica anche la loro identificazione e valutazione iniziali, seguite dal monitoraggio continuo, in modo da garantire una gestione aziendale coerente con gli obiettivi definiti dal management.

Un sistema di controllo interno e di gestione dei rischi può essere considerato efficace se contribuisce a guidare l'impresa in modo allineato agli obiettivi aziendali definiti dal Consiglio di Amministrazione, assicurando, in particolare, la salvaguardia del

[6] Il ruolo del Consiglio di Amministrazione; Patrizia Riva, Giorgio Corno
[7] Il Comitato di Controllo e Rischi: ruolo, funzioni e agenda per un'efficace governance; Ned Comunity (2021)

patrimonio sociale, l'efficienza dei processi aziendali, l'affidabilità dell'informazione finanziaria, e il rispetto delle normative legali, regolamenti interni e dello statuto sociale[8].

Il Comitato Controllo e Rischi supporta il Consiglio di Amministrazione nelle questioni relative ai rischi e al sistema di controlli interni. Più specificamente, il Comitato svolge attività di valutazione, in collaborazione con il dirigente responsabile della redazione dei documenti contabili, il revisore legale e il collegio sindacale, per garantire l'applicazione corretta dei principi contabili, anche in caso di gruppi societari. Inoltre, il Comitato esprime pareri su specifici aspetti dei principali rischi aziendali, esamina le relazioni periodiche relative alla valutazione del sistema di controllo e della gestione dei rischi e ha il potere di sollecitare e promuovere azioni nei confronti dei responsabili delle diverse funzioni aziendali. Monitora anche l'autonomia, l'efficacia e l'efficienza della funzione di internal audit, può richiedere specifiche verifiche su aree operative e riferisce al Consiglio di Amministrazione sull'attività svolta, almeno semestralmente, in occasione della revisione della relazione finanziaria annuale e semestrale. Infine, supporta il Consiglio nelle valutazioni e decisioni relative alla gestione dei rischi derivanti da eventi che possano compromettere l'azienda.

Per quanto riguarda il rischio d'impresa, esso è definito come l'insieme degli effetti, positivi o negativi, che derivano da eventi imprevisti, influenzando la situazione economica, finanziaria o patrimoniale dell'impresa[9]. I rischi aziendali possono essere di diverso tipo, tra cui i rischi strategici, finanziari e operativi:

1. I rischi strategici nascono da cambiamenti nel contesto operativo o da decisioni aziendali che non rispondono adeguatamente ai cambiamenti del mercato o della concorrenza.
2. I rischi finanziari sono legati alle fluttuazioni dei prezzi degli strumenti finanziari.
3. I rischi operativi derivano da perdite causate da risorse umane inadeguate o da sistemi interni mal funzionanti.

[8] Gestione del Rischio e Controllo interno; ODEC Milano
[9] Sistema di Controllo interno e Gestione dei rischi; Gruppo Acea

Il sistema di controllo interno e di gestione dei rischi è costituito da un insieme di regole, procedure e strutture organizzative finalizzate a garantire l'identificazione, la misurazione, la gestione e il monitoraggio dei principali rischi aziendali. L'obiettivo di questo sistema è contribuire al successo sostenibile dell'impresa[10].

Oggi, il sistema di controllo interno è un sistema dinamico che si occupa della gestione dei rischi, in particolare in relazione a due concetti chiave: il Risk Tolerance e il Risk Appetite. Il Risk Tolerance rappresenta la capacità dell'azienda di mantenere i rischi entro limiti accettabili, ossia la quantità di rischio che l'impresa è disposta ad accettare per raggiungere determinati livelli di performance. Il Risk Appetite, invece, definisce la propensione dell'impresa a prendere rischi per raggiungere gli obiettivi di business, tenendo conto delle opportunità e minacce esterne. Una volta stabiliti i livelli di Risk Tolerance e Risk Appetite, l'azienda determina anche il Risk Target, cioè il livello di rischio che è disposta ad assumere per il raggiungimento dei propri obiettivi strategici.

1.4 L'enterprise risk management

L'Enterprise Risk Management (ERM) è il processo attraverso il quale un'organizzazione identifica, analizza, quantifica, mitiga e monitora i rischi che potrebbero compromettere il raggiungimento degli obiettivi strategici. Il Consiglio di Amministrazione (CdA) deve focalizzarsi sulla creazione di valore per gli azionisti in un orizzonte temporale medio-lungo, definendo la natura e il livello di rischio compatibile con gli obiettivi strategici dell'impresa. Nella sua valutazione, il CdA considera tutti i rischi che possono influire sulla sostenibilità delle attività aziendali nel medio-lungo periodo.

Nel 2017, è stata avviata una revisione del framework di ERM, con l'intento di integrarlo pienamente nelle strategie aziendali per il raggiungimento della performance.

[10] Sistema di Controllo interno e Gestione dei rischi; ENAV

Da questa revisione è emerso il CoSO Report 2017, che propone un modello innovativo di sistema di controllo, diventando uno standard internazionale riconosciuto nel campo dei modelli di ERM. Questo modello è divenuto il riferimento per il controllo interno utilizzato dai codici di autodisciplina (oggi Codice di Corporate Governance), definiti da varie associazioni di categoria, e dalla normativa nazionale e internazionale sulla Corporate Governance.

Una struttura rivisitata del framework prevede cinque componenti e venti principi, che si allineano al ciclo di vita dell'impresa.

Fonte: Enterprise Risk Management: Applying ERM to environmental, social, and governance-related risks
https://www.riskcompliance.it/news/sostenibilita-come-gestire-i-rischi-esg-environment-social-e-governance/

Attraverso l'immagina è chiaro notare diverse caratteristiche:
-gestione integrata dei rischi, in cui i rischi aziendali sono collegati alla strategia e all'operatività, permettendo di applicare i principi dell'ERM a supporto della creazione e preservazione di valore;

-maggiore focus sulla cultura aziendale, che aiuta le imprese a prendere decisioni più responsabili e consapevoli, considerando i cambiamenti nella domanda e nelle aspettative del mercato;
-utilizzo dei benefici derivanti dall'ERM, che vanno dalla mitigazione delle perdite alla consulenza strategica, fino a un processo decisionale più efficace;
-integrazione della tecnologia dell'informazione, che influenza sia la strategia aziendale sia il contesto operativo, migliorando la gestione del rischio.

Il Rapporto CoSO del 2017 elenca anche venti principi, ciascuno correlato a uno dei cinque componenti del modello (Governance e Cultura, Strategia e Definizione degli Obiettivi, Performance, Revisione e Revisione, Comunicazione e Reportistica delle Informazioni). Tra i principi più significativi vi sono quelli che stabiliscono che il Consiglio di Amministrazione deve assumere la supervisione dei rischi, definendo la struttura operativa e la cultura aziendale desiderata. Inoltre, è fondamentale che prima di definire gli obiettivi operativi venga stabilito il risk appetite, e che il sistema di gestione del rischio venga costantemente migliorato, attraverso l'identificazione, la valutazione, la prioritizzazione e la gestione dei rischi.

1.5 Internal Audit

La gestione delle organizzazioni imprenditoriali ha originato la creazione di un servizio di controllo all'interno delle stesse. Inizialmente, questo servizio si concentrava principalmente sulla protezione contro frodi relative ai salari, alla perdita di liquidità e altre problematiche simili. Tuttavia, ben presto, l'ambito della revisione contabile si è esteso alla verifica di quasi tutte le transazioni finanziarie. È negli Stati Uniti che nasce l'Institute of Internal Auditors (IIA), come risultato della convinzione dei revisori interni che fosse necessaria una struttura organizzativa per sviluppare la professione di auditing[11] interno all'interno del contesto giuridico e professionale degli Stati Uniti. Nei primi anni di vita dell'IIA, la revisione contabile interna veniva ancora considerata

[11] La figura professionale dell'Internal Auditor e le fasi della sua attività; Alberto Oliva, Patrizia Riva

come una funzione strettamente collegata al lavoro dei revisori esterni, con un ruolo piuttosto limitato all'interno delle organizzazioni.
Con il passare del tempo, l'audit interno ha assunto un ruolo sempre più operativo, occupandosi anche dell'esame della validità delle dichiarazioni aziendali. I suoi compiti sono così diventati molto più ampi, coprendo una vasta gamma di problematiche in cui il rapporto con i conti è solo uno degli aspetti. Poiché il revisore interno è parte integrante dell'azienda, ha un interesse diretto in tutte le operazioni aziendali e, di conseguenza, è maggiormente impegnato a contribuire a rendere tali operazioni più redditizie. Nel 1947, l'IIA emette la dichiarazione di responsabilità dell'Internal Auditor, che chiarisce che, sebbene la revisione interna fosse in passato focalizzata principalmente su questioni contabili e finanziarie, anche le problematiche di natura operativa rientrano nel suo ambito di competenza.

Nel 1957, questa dichiarazione di responsabilità viene ampliata includendo numerosi servizi a supporto della direzione, come ad esempio:

-revisione e la valutazione della solidità, dell'adeguatezza e dell'applicazione dei controlli contabili, finanziari e operativi;

-verifica del grado di conformità con politiche, piani e procedure aziendali;

-protezione delle attività aziendali da potenziali perdite;

-valutazione dell'affidabilità dei dati contabili e di altri dati sviluppati all'interno dell'organizzazione;

-valutazione delle prestazioni nel raggiungimento delle responsabilità assegnate.

Nel corso degli anni, la Dichiarazione di responsabilità è stata rivista nel 1976, 1981 e 1990 per riflettere l'evoluzione continua e rapida della professione di revisore interno.
Nel 1978, l'IIA ha formalmente approvato i principi per la pratica professionale dell'audit interno, con i seguenti obiettivi:

1. Comunicare il ruolo, la portata, le prestazioni e gli obiettivi dell'audit interno;
2. Unificare i controlli interni a livello globale;
3. Promuovere un migliore controllo interno;
4. Stabilire basi per una valutazione coerente delle operazioni di audit interno;
5. Riconoscere il controllo interno come una professione.

I principi contenuti nella dichiarazione definiscono l'audit interno come un'attività di valutazione indipendente all'interno di un'organizzazione, concepita come un servizio di supporto. Il suo obiettivo principale è esaminare e valutare l'adeguatezza e l'efficacia dei controlli esistenti, aiutando i membri dell'organizzazione nell'assolvere le loro responsabilità. Per raggiungere questo scopo, l'audit interno fornisce analisi, valutazioni, raccomandazioni e informazioni sulle attività esaminate, contribuendo così a promuovere un controllo efficace a costi ragionevoli.

Con il tempo, i revisori interni hanno ampliato le loro competenze in settori specifici, come l'assistenza sanitaria, il petrolio, il gas, l'energia, la difesa, i servizi finanziari, i trasporti, il commercio, la tecnologia, le telecomunicazioni, i media, l'intrattenimento, il governo e le organizzazioni non profit, l'istruzione, e altri. Il personale incaricato del controllo interno ha iniziato a provenire da contesti diversi, con una crescente presenza di laureati in discipline non contabili, e una maggiore partecipazione delle donne nella professione. Inoltre, i revisori interni hanno acquisito una visione internazionale e, in molti casi, hanno cominciato a partecipare attivamente a "progetti speciali" su base emergenziale, assumendo ruoli di responsabilità come responsabili del rischio, della conformità o etici, a seconda delle necessità.

1.5.1. Le funzioni dell'Internal Audit

I cambiamenti rapidi e rivoluzionari nel contesto aziendale hanno avuto significative implicazioni per le organizzazioni in tutto il mondo dal 2023 in poi. La concorrenza globale ha stimolato l'introduzione di migliori iniziative nella gestione della qualità e

del rischio, portando alla riprogettazione di strutture e processi aziendali, con l'obiettivo di generare maggiore responsabilità. Questi cambiamenti hanno reso essenziale l'adozione di informazioni tempestive, affidabili e pertinenti per supportare il processo decisionale.

L' Internal Auditing è un'attività indipendente e obiettiva che fornisce assurance e consulenza per aggiungere valore e affinare i processi di gestione del rischio, controllo e governance all'interno di un'organizzazione. La revisione interna fornisce valore valutando sistematicamente e migliorando l'efficacia della gestione del rischio, del controllo e dei processi di governance nell'organizzazione. In altre parole, la presenza della Revisione Interna assicura che questi processi siano efficaci nel soddisfare gli obiettivi aziendali e li prescrive anche su come migliorare[12].

Vediamo ora nel dettaglio il ruolo dell'Internal Auditing nelle seguenti aree:

-Risk Management → l'Internal Auditing aiuta l'organizzazione nell'identificare e valutare le esposizioni ai rischi, contribuendo al miglioramento dei sistemi di gestione del rischio. Per valutare l'adeguatezza dei processi di Risk Management, l'Internal Audit si basa su cinque obiettivi fondamentali che il Risk Management deve perseguire: identificare e prioritizzare i rischi, determinare i rischi accettabili, attuare strategie per gestire o evitare i rischi, monitorare il processo di gestione e fornire relazioni periodiche al management. L'Internal Audit verifica che questi obiettivi siano adeguatamente trattati e, se necessario, segnala l'assenza di un processo di Risk Management, suggerendo l'adozione di uno.

Controllo → l'Internal Auditing supporta l'organizzazione nel garantire che i controlli siano efficienti ed efficaci, cercando di migliorarli continuamente. L'audit valuta l'adeguatezza e l'efficacia dei controlli in ambito governance, operazioni e sistemi informativi dell'organizzazione, in relazione all'affidabilità delle informazioni finanziarie e operative, all'efficienza delle operazioni e alla conformità alle leggi, regolamenti e contratti. Attraverso attività annuali di audit, viene emesso un giudizio

[12] Manuale Internal Audit P.A.C. Compliant; Asur Marche

complessivo sul Risk Management e sul Sistema di Controllo Interno (SCI). Questo giudizio può essere positivo o negativo, fornendo al board e al management un'analisi dettagliata sull'adeguatezza dei controlli interni. Se il giudizio è positivo, si fornisce una valutazione complessiva dell'adeguatezza dei controlli, mentre se il giudizio è negativo, non si garantisce sull'efficacia dei controlli, e l'auditor non assume responsabilità riguardo la copertura dell'audit.

Governance → il ruolo dell'Internal Auditing nel processo di governance è quello di fornire suggerimenti utili per migliorare il raggiungimento degli obiettivi aziendali, come lo sviluppo di valori etici, il miglioramento dell'efficacia della gestione operativa e il monitoraggio del coordinamento delle informazioni tra il board, l'audit e il management. Inoltre, l'Internal Audit si occupa di comunicare le informazioni relative ai rischi.

I controlli che esistono all'interno delle organizzazioni oggi sono radicalmente diversi da quelli delle aziende tradizionali del XX secolo. In questo paesaggio di trasformazione, la Revisione Interna si è evoluta come funzione chiave di supporto alla gestione, al comitato di audit, al consiglio di amministrazione, ai revisori esterni e ai principali stakeholder. Se correttamente concepita e implementata, l'attività di audit interno può svolgere un ruolo fondamentale nel promuovere e supportare una governance efficace. Con l'aumento della consapevolezza riguardo ai rischi che le imprese multinazionali devono affrontare, la domanda di professionisti specializzati nella gestione del rischio è aumentata considerevolmente.

Un aspetto significativo che i revisori interni possono sviluppare è la "collaborazione" con il management nella creazione e monitoraggio dei processi aziendali per la valutazione e la gestione dei rischi, nonché nell'implementazione di iniziative di gestione del rischio. I moderni approcci di audit interno, basati sul rischio, consentono di collegare i rischi agli obiettivi aziendali. Di fatto, l'audit interno può facilitare i processi attraverso i quali le business unit sviluppano valutazioni di rischio di alta qualità, rendendo il lavoro dell'audit più efficace e migliorando la qualità delle informazioni utili per le decisioni, riducendo al contempo la duplicazione degli sforzi.

Infine, la presenza di una funzione di Internal Audit forte e ben strutturata può avere un impatto determinante nel supportare una governance organizzativa efficace. Quando l'Internal Audit acquisisce la fiducia del management e delle altre figure coinvolte nella governance, può fornire prestazioni eccezionali, utilizzando la vasta esperienza e conoscenza del suo personale nelle migliori pratiche di controllo, monitoraggio dei rischi e governance. In conclusione, nel XXI secolo, la professione di revisore interno offre opportunità di crescita senza precedenti, ma gli sviluppi nella pratica richiedono un'attenta analisi da parte degli accademici, affinché un corpus di conoscenze possa essere costruito e trasmesso alle future generazioni di professionisti.

1.5.2. Il Processo di Audit

L'Internal Auditing è un'attività indipendente e obiettiva di assurance e consulenza, mirata al miglioramento dell'efficacia e dell'efficienza organizzativa. Essa supporta l'organizzazione nel raggiungimento dei propri obiettivi mediante un approccio professionale e sistematico, creando valore aggiunto attraverso la valutazione e il miglioramento dei processi di gestione dei rischi, di controllo e di governance.

Sebbene l'attività di audit venga generalmente condotta in modo standardizzato, è importante sottolineare che gli auditor interni dispongono di una certa discrezionalità nell'attuazione di tali attività.

Il processo di audit è comunemente suddiviso in quattro fasi principali:

Pianificazione: il processo di audit inizia con una lettera di notifica, che informa i responsabili delle aree aziendali dell'inizio dell'attività, consentendo loro di prepararsi ad accogliere gli auditor. Successivamente, si effettua un'analisi preliminare per raccogliere informazioni sui processi da esaminare. Durante un incontro di avvio (Kick-off meeting) tra il team di audit e il management, vengono definiti gli obiettivi principali dell'intervento e le metodologie da applicare.

La fase di pianificazione consiste in un'analisi più approfondita del processo, in cui vengono identificati gli oggetti dell'audit e stabilita la priorità di verifica. Questo processo avviene tramite un Risk Assessment, una valutazione sistematica degli eventi che potrebbero influenzare il raggiungimento degli obiettivi aziendali, sia in ambito esterno (come l'economia, la normativa e la concorrenza) che interno (persone, processi e infrastrutture). Il rischio è definito come la possibilità che un evento comprometta negativamente il raggiungimento degli obiettivi strategici e/o operativi. La valutazione del rischio viene effettuata in base a impatto e probabilità di accadimento, considerando anche l'ambiente di controllo.

Esecuzione dei test: in questa fase, l'internal auditor identifica, analizza, valuta e registra le informazioni necessarie per raggiungere gli obiettivi prefissati. Le informazioni raccolte devono essere sufficienti, affidabili, rilevanti e utili per il raggiungimento degli obiettivi. Le prove raccolte devono essere adeguate, concrete e convincenti, e la documentazione dell'audit deve essere tale da consentire a un revisore esperto, non necessariamente familiare con l'incarico, di comprendere: la natura, la tempistica e l'estensione delle procedure di revisione svolte; i risultati delle procedure di revisione e gli elementi probativi raccolti; gli aspetti significativi emersi durante il lavoro di revisione.

A seconda dell'area analizzata, i test di audit possono differire e si distinguono in:

→Operational Audit: Audit focalizzati sull'efficacia e sull'efficienza dei processi e sul presidio dei rischi.
→Financial Audit: Audit che verificano il Sistema di Controllo Interno riguardo a processi amministrativo-contabili e bilancio.
→Compliance Audit: Audit che esaminano la conformità alle norme interne ed esterne applicabili.

→Fraud Audit: Audit finalizzati all'identificazione di frodi o comportamenti illeciti, come ad esempio alterazioni nelle gare tra fornitori o l'inserimento di fornitori fittizi in anagrafica.

Reporting: l'attività di audit si conclude generalmente con la stesura di un Audit Report, che riassume i risultati dell'attività svolta. Il report deve specificare chi è l'auditato (processo e management), gli obiettivi dell'audit e cosa è stato esaminato.
Al fine di garantire la piena consapevolezza da parte del management dei risultati e delle loro implicazioni, è consigliabile organizzare riunioni di chiusura dell'audit (exit meeting), durante le quali il management si impegna formalmente a risolvere le problematiche identificate e a rispettare i tempi di attuazione delle azioni correttive.

Il **follow-up** è l'attività di monitoraggio e documentazione della risoluzione delle carenze identificate e dell'implementazione delle azioni correttive da parte del management. Questa fase può essere documentale o prevedere una nuova esecuzione dei test per verificare l'efficacia delle modifiche apportate.
Il follow-up consente al Top Management e agli Organi di Governance di monitorare lo stato del Sistema di Controllo Interno e di valutarne la tempestività nell'intervento.
Inoltre, il follow-up è un elemento fondamentale del processo di "Continuous Improvement" del sistema di controllo e della gestione dei rischi. Il suo svolgimento periodico aiuta a sollecitare il management e gli owner delle azioni correttive a rispettare le scadenze predefinite, assicurando l'efficacia delle azioni intraprese.

2. LE FRODI AZIENDALI

2.1 Internal Audit

Nel capitolo precedente, è emersa l'importanza delle attività di Internal Auditing per il miglioramento del sistema di controllo interno delle aziende. Nello specifico, abbiamo evidenziato come uno dei principali obiettivi di tale sistema sia quello di supportare la crescita dell'impresa attraverso una gestione efficace dei rischi. Tra i diversi tipi di rischio, il rischio di frode emerge come uno dei più rilevanti e merita una particolare attenzione da parte della funzione di Inrternal Audit, poiché può avere un impatto molto importante sull'intera organizzazione.

Nel XXI secolo, di seguito a diversi scandali aziendali come quelli di Parmalat, Volkswagen e altri, è emerso un forte bisogno nel contrastare tali fenomeni fraudolenti, spingendo ad un'attenzione crescente nell'analisi e nello studio di tali comportamenti illeciti.
Sebbene il fenomeno della frode ritrovi le sue radici nelle prime forme di commercio dell'antichità, nel corso dei secoli la sua complessità è aumentata, adattandosi ai cambiamenti nelle strutture economiche e aziendali.

Nel presente capitolo, analizzeremo il fenomeno della frode in tutti i suoi aspetti, evidenziando le discipline e le metodologie per combatterlo, con un focus particolare sulla disciplina del Fraud Auditing[13].

2.2 Cos'è la frode e le relative caratteristiche

Il concetto di frode non è definito esplicitamente dalla legge, ma nel linguaggio comune e si riferisce a un'azione volta a danneggiare un diritto altrui attraverso l'inganno. In un

[13] La revisione di frodi e fatti illeciti; Revisione legale

contesto aziendale, la frode può essere intesa come qualsiasi comportamento non violento che, con modalità illecite, procura un vantaggio o beneficio, arrecando un danno ingiusto, anche in modo indiretto, ad altri[14].

Una possibile definizione di frode è la seguente: "Una serie di atti ingannevoli che mirano a ingannare la buona fede di un individuo al fine di appropriarsi illecitamente di ricchezze". In alternativa, può essere descritta come un "comportamento mirato a ledere i diritti di un'altra persona attraverso l'inganno".

Dal punto di vista giuridico, pur non essendoci una definizione esplicita di frode nel Codice penale, la legge prevede il reato di truffa, descrivendolo come un'azione in cui una o più persone, tramite raggiri, inducono in errore un soggetto, procurandosi così un profitto ingiusto a danno di altri.

Le definizioni finora proposte, tuttavia, risultano incomplete per una comprensione più precisa del fenomeno, poiché il nostro studio si concentrerà esclusivamente sulle frodi di natura economica. Questi comportamenti illeciti, legati all'attività imprenditoriale o professionale, sono conosciuti nella letteratura anglosassone con il termine *white collar crime.*

Gli elementi chiave[15] che caratterizzano un crimine economico sono i seguenti:

- Inganno: la realizzazione avviene mediante la falsificazione, l'occultamento o la manipolazione di documenti e fatti;

- Intenzionalità: un crimine economico si configura come tale solo quando è il risultato di un piano premeditato;

[14] Il rischio di frode aziendale; Dogma
[15] Introduzione all'economia; Università degli Studi di Napoli Federico II

- Violazione del rapporto fiduciario: le relazioni economiche si fondano generalmente sulla fiducia tra le parti. La frode avviene quando tale fiducia viene meno e quindi viene violata, abbassando così le difese delle vittime;

- Danno: la frode, come crimine appropriativo, comporta un vantaggio per l'autore del reato che è equivalente e opposto al danno subito dalla vittima;

- Occultamento: per rendere l'azione fraudolenta "invisibile", è fondamentale che la vittima o i soggetti incaricati di controllare non vengano a conoscenza del comportamento illecito;

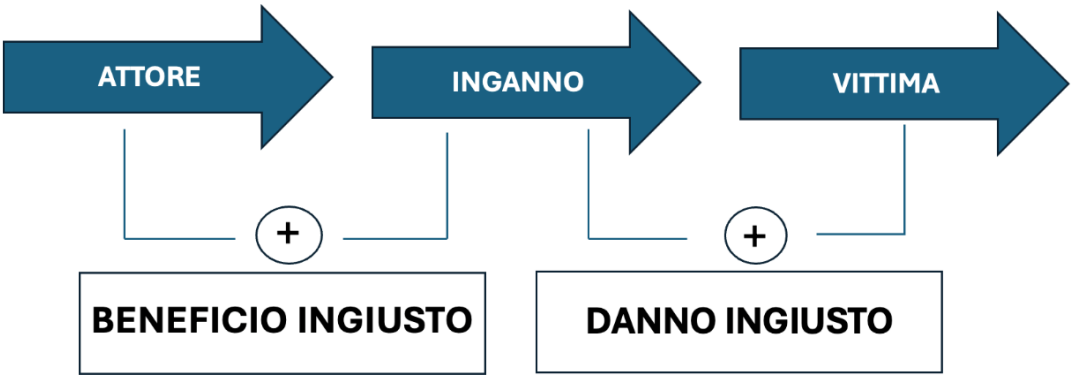
- Rispettabilità apparente: l'autore della frode, solitamente, gode di una posizione di rispetto sociale che lo rende più difficile da individuare;

- Vittima: la vittima, nella maggior parte dei casi, rimane inconsapevole dell'inganno, e l'assenza di interazione diretta tra il colpevole e la vittima giustifica, agli occhi del trasgressore, il compimento dell'illecito.

Dunque, la frode si configura come un comportamento in cui l'autore (chiamato soggetto attivo), attraverso l'uso di inganni, induce in errore la vittima (chiamata soggetto passivo) e ottiene per sé o per altri un vantaggio illecito, causandone contemporaneamente un danno ingiusto.

A partire da questa definizione, condivisa dalla maggior parte degli esperti, è possibile individuare gli elementi fondamentali che caratterizzano ogni caso di frode, ossia: l'autore, la vittima, l'inganno, il beneficio illecito e il danno ingiusto.

Questi elementi possono essere sintetizzati nel seguente schema:



2.3 Perché si commettono le frodi?

Analizzare le radici del comportamento fraudolento è essenziale, poiché in questo modo è possibile identificare le cause che spingono alcuni individui a commettere atti illeciti. Le teorie criminologiche sviluppate fin dal XIX secolo suggeriscono che i criminali siano esseri razionali, il cui obiettivo principale è quello di massimizzare il soddisfacimento dei propri bisogni e il proprio benessere.

Alcuni studiosi, come N. Shover e K.M. Bryant, hanno rilevato tre fattori chiave che guidano la decisione di un individuo nell' intraprendere un'azione criminale:

- la PRESSIONE percepita nel raggiungere determinati obiettivi;
- la percezione delle SANZIONI LEGALI come conseguenze negative possibili in caso di scoperta;
- la CULTURA DI RIFERIMENTO, che può facilitare l'accettazione di comportamenti illegali.

Le teorie criminologiche, nel corso dei decenni, inducono ad una conclusione ben precisa: alla base di ogni atto criminoso esiste una volontà consapevole e razionale di commettere il reato, basata sulla convinzione che il crimine possa essere vantaggioso. In altre parole, la decisione di commettere un illecito nasce da una valutazione razionale dei costi e dei benefici associati all'atto illecito, dunque "la condotta illegale origina dalla percezione della convenienza a delinquere".

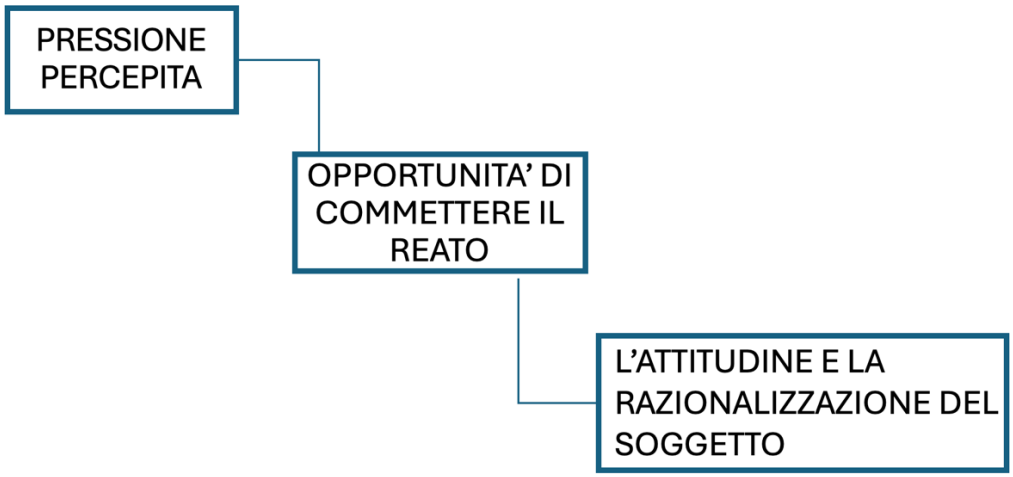
A metà del XX secolo, il criminologo Donald R. Cressey, in seguito a un'analisi su un campione di circa duecento individui condannati per appropriazione indebita, ha sviluppato un modello con l'obiettivo di classificare le circostanze che possono indurre un individuo a compiere azioni illegali. Dallo studio, Cressey ha identificato tre fattori principali che contribuiscono alla commissione di illeciti:

1. La manifestazione di problemi finanziari che l'individuo preferisce non condividere e risolvere autonomamente;

2. La possibilità di sfruttare una situazione di fiducia per risolvere questi problemi attraverso metodi illegittimi;

3. L'abilità dell'individuo di giustificare il comportamento illecito attraverso un processo di razionalizzazione, che gli permette di trovare scuse per la sua azione.

Di conseguenza, la possibilità che si verifichi una frode dipende dall'interazione di tre variabili principali:



Chiaramente la pressione eccessiva si classifica come una delle cause principali che spingono un individuo a compiere una frode. La pressione può avere origini interne all'organizzazione, come le aspettative irrealistiche nei confronti di determinati risultati aziendali, che possono portare i dirigenti a falsificare documenti contabili, specialmente quando i sistemi di remunerazione sono legati alle performance. Altre volte, la pressione può derivare da necessità personali, come un'urgenza finanziaria o la tendenza a vivere al di sopra dei propri mezzi.

Affinché una frode si realizzi, oltre alla pressione, l'individuo deve percepire anche l'opportunità di compiere l'atto illecito senza essere scoperto. Questa opportunità si manifesta quando l'autore del reato è consapevole delle lacune nel sistema di controllo interno dell'organizzazione, che gli permettono di compiere il crimine e nasconderlo senza incorrere in sanzioni.

Infine, il meccanismo della razionalizzazione gioca un ruolo cruciale. Questo processo consente all'individuo di giustificare l'atto illecito a sé stesso e, se scoperto, anche agli altri membri dell'organizzazione. Il frodatore non si percepisce come un criminale, ma tende a ritenere che la sua azione sia giustificabile, trovando motivazioni che gli consentano di considerarla un comportamento accettabile.

2.4 Fraud Auditing

Nel corso del tempo, il dibattito su quale sia la figura professionale più adatta alla prevenzione e all'individuazione delle frodi aziendali è stato ampio e articolato.
In passato, è emersa in particolare la figura del revisore esterno, il quale ha il compito di esaminare e verificare i rendiconti finanziari dell'impresa. Chiaramente le sue mansioni non si esauriscono nel solo controllo contabile: il revisore valuta anche la continuità aziendale e analizza l'impatto delle strategie gestionali adottate, oltre a individuare eventuali rischi operativi connessi alle attività verificate.

Nell'ambito della gestione delle frodi, è spesso opinione diffusa che il revisore esterno abbia il dovere di intervenire qualora riscontri comportamenti fraudolenti. In realtà, la sua funzione principale consiste nell'esprimere un giudizio professionale sulla presenza o meno di errori significativi nei bilanci, piuttosto che nel rilevare frodi vere e proprie. In tal senso, come chiarito dal principio di revisione internazionale ISA 200, lo scopo della revisione contabile è quello di ottenere sufficienti elementi probativi per stabilire se il bilancio, nel suo complesso, sia redatto in conformità al quadro normativo di riferimento. La ricerca di atti fraudolenti, quindi, non rappresenta l'obiettivo centrale della revisione esterna.

In questo contesto, si inserisce invece il ruolo dell'Internal Audit, che risulta maggiormente focalizzato sull'analisi dei rischi e sull'efficacia del sistema di controllo interno. Tale funzione, infatti, svolge un'attività più approfondita nella prevenzione e nell'individuazione delle frodi, rappresentando così una figura più adeguata ad affrontare tali tematiche.

È importante ricordare che ogni frode si realizza eludendo e raggirando i meccanismi di controllo predisposti dall'organizzazione. Pertanto, l'audit interno ha il compito di verificare se tali controlli siano stati effettivamente progettati e applicati in modo efficace, offrendo una garanzia sul corretto funzionamento del sistema di governance[16].

Le attività di fraud auditing possono essere distinte in tre categorie principali:

1. Prevenzione: si basa sull'identificazione delle aree aziendali più vulnerabili e sensibili a fenomeni fraudolenti, ipotizzando le modalità con cui potrebbero essere compiute le frodi. L'obiettivo è orientare l'organizzazione verso misure di contrasto proattive, attraverso valutazioni periodiche dei rischi e l'adozione di soluzioni tecnologiche, regolamentari e procedurali per ridurre le possibilità di comportamento illecito.

2. Individuazione (Detection): ha l'obiettivo di intercettare tempestivamente anomalie e segnali di possibili frodi, anche prima che esse si concretizzino. Questo avviene mediante strumenti e tecniche di monitoraggio che consentono di rilevare comportamenti sospetti e avviare azioni correttive in modo rapido.

3. Indagine (Investigation): consiste nell'analizzare i fattori che hanno permesso la realizzazione della frode, al fine di individuare le responsabilità e rafforzare il sistema di prevenzione. In questa fase, è fondamentale raccogliere informazioni specifiche e dettagliate sugli eventi sospetti, così da poter svolgere verifiche mirate e approfondite.

[16] Mappatura processi, analisi e classificazione del rischio- misure di contrasto; PIAO 2025-2027

In conclusione, l'attività investigativa che segue una segnalazione di potenziale frode dovrebbe essere svolta dall'Internal Audit, i cui membri devono possedere competenze adeguate ad affrontare situazioni di questo tipo. Nelle organizzazioni di maggiori dimensioni, è frequente la presenza di figure specializzate nella fraud investigation, capaci di supportare efficacemente i processi di prevenzione e rilevazione. In ogni caso, è raccomandabile che il management si avvalga di professionisti esperti in materia, dotati della preparazione necessaria per fronteggiare il fenomeno delle frodi in maniera sistematica e competente.

2.5 Le principali tipologie di frode aziendale

In ambito aziendale possono verificarsi diverse tipologie di frode, in questo paragrafo percorreremo le principali forme, analizzandole. L'obiettivo è sviluppare una panoramica chiara e dettagliata sulle modalità attraverso cui tali fenomeni si concretizzano.

Innanzitutto, è necessario distinguere le frodi in interne ed esterne, è una classificazione essenziale per comprendere i soggetti coinvolti.
Le frodi interne coinvolgono soggetti appartenenti all'organizzazione stessa, spesso con ruoli dirigenziali o di alta responsabilità. La posizione di rilievo e la conoscenza dettagliata e profonda dei meccanismi aziendali rendono questi individui più capaci di eludere controlli e attuare condotte fraudolente.
Le frodi esterne, invece, provengono da soggetti esterni all'azienda. Nella maggior parte dei casi si tratta di clienti (circa il 50%), hacker (circa il 30%) o intermediari, agenti e fornitori (20%). Nonostante questi ultimi siano legati all'azienda da relazioni fiduciarie e continuative, possono comunque rappresentare una minaccia.

2.5.1 Corruzione

Una prima forma di frode da analizzare è la corruzione, ovvero l'offerta o la promessa di vantaggi economici o di altra natura a pubblici ufficiali in cambio dell'adozione di atti contrari ai doveri d'ufficio.
Tale pratica, largamente diffusa a livello globale e trasversale a diversi settori economici, compromette l'integrità delle istituzioni e intacca il corretto funzionamento dell'economia. Un esempio emblematico è rappresentato dallo scandalo che ha coinvolto la FIFA.

Dal punto di vista giuridico, la corruzione è un reato che coinvolge due soggetti: il corrotto, necessariamente un pubblico ufficiale o un incaricato di pubblico servizio, e il corruttore, generalmente un privato.
È importante distinguere la corruzione da altri reati affini come la concussione, in cui il pubblico ufficiale abusa della propria posizione per costringere un soggetto a concedere denaro o vantaggi, e l'abuso d'ufficio, che si verifica quando un pubblico funzionario viola le norme per ottenere un vantaggio ingiusto a favore proprio o altrui[17].

2.5.2 Frode contabile

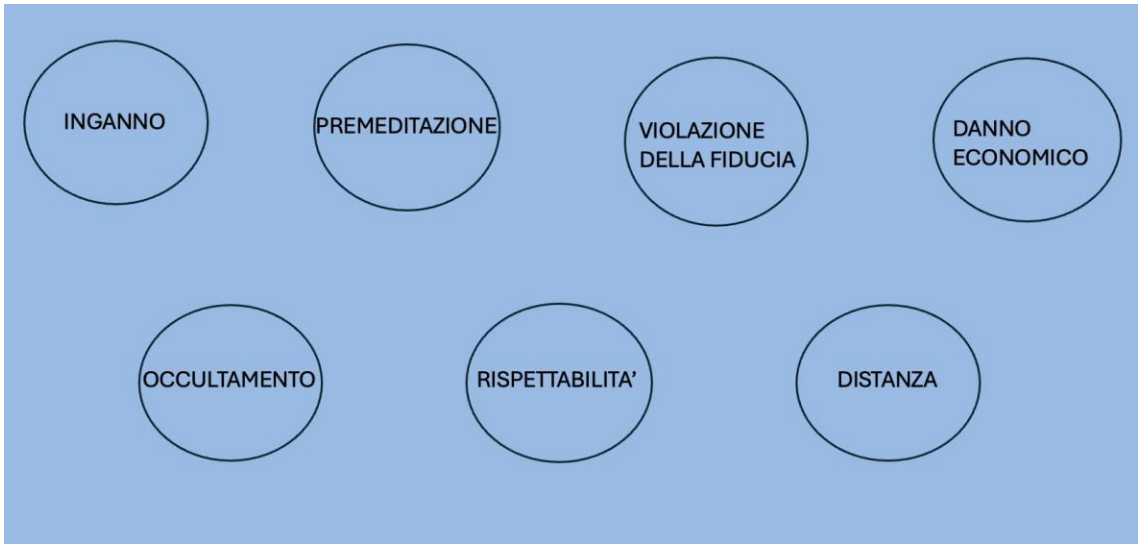
La frode contrabile, chiamata anche falso in bilancio, consiste nella modifica e alterazione intenzionale delle informazioni contenute nei bilanci aziendali e nei documenti contabili.
Il bilancio rappresenta un elemento essenziale per informare creditori, soci e soggetti esterni, dunque dev'essere redatto basandosi su fedeltà, trasparenza e chiarezza.
Qualsiasi forma di falsificazione viene considerata un illecito pensale in molti ordinamenti.

[17] Il reato di corruzione; Studio Cataldi

Pertanto, la frode si classifica come un comportamento fraudolento che mina la fiducia degli stakeholder e altera la percezione della reale situazione patrimoniale, economica e finanziaria dell'impresa.

I reati riconducibili alla frode contabile comprendono numerose fattispecie previste dal codice civile e penale, tra cui le false comunicazioni sociali (art. 2621 e 2622), l'impedito controllo (art. 2625), l'indebita distribuzione di utili (art. 2627), la formazione fittizia del capitale (art. 2632) e la corruzione tra privati (art. 2635). Tali reati possono essere commessi non solo dagli amministratori, ma anche da chi esercita funzioni equivalenti di fatto e da soggetti terzi coinvolti nella condotta.

I tratti distintivi della frode contabile includono:



Nell'immagine sono riportati le sette caratteristiche della frode contabile, seguirà un'analisi:

-l'inganno è la manipolazione e alterazione dei dati aziendali;

-la premeditazione è il segno della volontarietà e intenzionalità dell'azione;

-la violazione della fiducia riguarda in particolar modo il rapporto tra l'azienda e gli stakeholder;

-il danno economico è ciò che viene inflitto a soggetti terzi, a vantaggio e beneficio personale;

-l'occultamento dell'attività illecita;

-la rispettabilità è una caratteristica chiaramente apparente e riguarda l'autore, il quale sfrutta la sua posizione "credibile" per commettere la frode;

-la distanza psicologica della vittima, che permette la realizzazione del reato.

2.5.3 Appropriazione indebita

L'appropriazione indebita è stata introdotta dall'art. 646 del Codice Penale e si configura quando un soggetto si impossessa, per proprio profitto, di beni mobili o denaro altrui, che gli erano stati affidati legittimamente.
Citando il Codice Penale: "Chiunque(1), per procurare a sé o ad altri un ingiusto profitto(2), si appropria il denaro o la cosa mobile altrui(3) di cui abbia, a qualsiasi titolo, il possesso(4), è punito, a querela della persona offesa, con la reclusione da due a cinque anni e con la multa da euro 1.000 a euro 3.000."[18]

Gli elementi costitutivi della fattispecie relativa al reato di appropriazione indebita che devono essere necessariamente presenti ai fini della sua configurazione sono di seguito indicati:

[18] https://www.brocardi.it/codice-penale/libro-secondo/titolo-xiii/capo-ii/art646.html

1. Possesso legittimo: l'autore del reato deve avere il possesso o la detenzione del bene mobile in questione. Questo può avvenire per diverse ragioni quali, ad esempio, la consegna della cosa in capo all'autore del reato in qualità di depositario e/o custode.

2. Mancanza di consenso: l'appropriazione indebita si verifica quando l'autore del reato continua a detenere il bene senza il consenso del legittimo proprietario, violando così il diritto di proprietà di quest'ultimo.

3. Intento di trarre profitto ingiusto: è essenziale che il soggetto abbia l'intento (dolo specifico) di trarre un profitto ingiusto, per sé o per altri, utilizzando il bene di cui è in possesso. Questo elemento rappresenta l'elemento soggettivo della fattispecie, come detto, consistente in un dolo specifico, ovverosia nella consapevolezza e volontà di attuare un comportamento illegittimo per raggiungere una determinata finalità.

4. Atto di appropriazione: il reato è istantaneo nel momento in cui il soggetto compie l'atto di dominio sulla cosa, manifestando la volontà di considerare il bene come proprio, contrariamente al diritto del legittimo proprietario. Tale aspetto, è giuridicamente indicato con la locuzione interversione del possesso atta ad indicare, appunto, il mutamento della detenzione in possesso o del possesso corrispondente all'esercizio di un diritto reale su cosa altrui in possesso coincidente all'esercizio del diritto di proprietà.

5. Modalità di esecuzione: l'appropriazione indebita può manifestarsi in varie modalità, come la mancata restituzione di un prestito o di un deposito, l'uso improprio della cosa o la sua cessione a terzi senza autorizzazione. Ogni azione deve essere compiuta con l'intenzione di trarre un vantaggio personale o di terzi.[19]

A differenza del furto, in cui il bene è sottratto andando contro la volontà del legittimo proprietario, l'appropriazione indebita avviene dopo un trasferimento legittimo del possesso, che viene poi tradito dall'azione dell'autore.

[19] Lo studio legale LB esplicita le caratteristiche del fenomeno dell'appropriazione indebita. https://www.studiolegalelb.it/quando-si-configura-il-reato-di-appropriazione-indebita/

In ambito aziendale, questa condotta si manifesta spesso attraverso l'uso improprio di risorse aziendali – denaro, beni strumentali o anche materiali destinati allo smaltimento – per scopi personali[20].
Secondo una rilevazione condotta da PwC, l'appropriazione indebita rappresenta la forma più diffusa di frode aziendale a livello globale, superata solo recentemente dalle frodi informatiche.

2.5.4 Cybercrime

Il Cybercrime comprende tutte le forme di reato che prevedono l'uso illecito di sistemi informatici o telematici. Rientrano in questa categoria la violazione di dati sensibili, l'accesso abusivo a sistemi, la diffusione non autorizzata di codici di accesso, la creazione e distribuzione di software dannosi, nonché la falsificazione di documenti digitali e l'interferenza nelle comunicazioni online.

L'integrazione crescente delle tecnologie digitali nei processi aziendali ha moltiplicato le possibilità di attacco da parte dei cybercriminali, rendendo questi reati tra i più temuti per il futuro.
Le conseguenze dei cyberattacchi possono variare dalla compromissione delle operazioni aziendali alla sottrazione di informazioni strategiche, fino a veri e propri casi di estorsione.

Molte aziende stanno aumentando gli investimenti in cybersicurezza, consapevoli che la minaccia informatica rappresenta oggi una delle principali criticità da affrontare.
Sensibilizzazione, formazione, monitoraggio e audit sono le tecniche principali da utilizzare per cercare di prevenire i reati informatici.

[20] Quando si configura il reato di appropriazione indebita; Studio Legale LB

Tuttavia, ciò che realmente si sta sviluppando sempre più in seguito allo sviluppo di strumenti informatici è l'information security.
Per information si intende la capacità di garantire la riservatezza, l'integrità e la disponibilità dell'informazione elaborata dai sistemi informatici, memorizzata su archivi elettronici e trasmessa su reti di telecomunicazione. È importante, quindi, garantire l'autenticazione del soggetto che ha accesso al dispositivo, ed il controllo degli accessi limitandolo solo ai soggetti autorizzati. Nonostante i sistemi di information security aggiornati, però, nessun sistema informatico risulta sicuro al 100%. Infatti, nella sicurezza informatica ci sono vari livelli di sicurezza da analizzare e rispettare: la sicurezza fisica, logica e operativa. Se uno di questi elementi non è aggiornato o non è monitorato, tutto il sistema decade.

2.6 Quadro normativo e misure preventive contro le frodi societarie

Come accennato in precedenza, il fenomeno delle frodi ha origini molto antiche ed è sempre esistito in forme diverse nel corso della storia. Nonostante ciò, solo negli ultimi decenni il tema ha ricevuto una maggiore attenzione da parte della comunità scientifica, mentre l'intervento normativo da parte degli Stati è stato più tardivo e reattivo.
Infatti, è stato necessario il verificarsi di gravi scandali finanziari – come quello che ha coinvolto, in ambito italiano, il caso Parmalat – per spingere i legislatori a prendere coscienza della gravità del problema e ad adottare strumenti giuridici mirati alla prevenzione e al contrasto delle frodi in ambito aziendale.

Nel prosieguo verranno illustrate, in sintesi, le principali disposizioni normative adottate a livello nazionale per fronteggiare tali fenomeni.
In particolare, si farà riferimento al Decreto Legislativo 231/2001, che rappresenta il pilastro normativo italiano in materia di responsabilità amministrativa degli enti come risposta ai gravi casi di frode societaria.

2.6.1 Il Decreto Legislativo 231/2001

Il Decreto Legislativo 231/2001 disciplina la responsabilità amministrativa delle società, con l'obiettivo principale di prevenire la commissione di frodi. Questo provvedimento ha introdotto, per la prima volta in Italia, la responsabilità penale degli enti per determinati reati commessi nell'interesse o a vantaggio degli stessi, da individui che ricoprono ruoli di rappresentanza, amministrazione o direzione all'interno dell'ente o di sue unità organizzative autonome dal punto di vista finanziario e funzionale; nonché da coloro che, anche di fatto, gestiscono o controllano l'ente, e da chi è sottoposto alla direzione o supervisione di questi soggetti. Tale responsabilità si aggiunge a quella della persona fisica che ha materialmente compiuto l'illecito, rappresentando così un elemento innovativo.

Il Decreto Legislativo 231/2001[21] ha l'obiettivo di coinvolgere gli enti nella responsabilità per alcuni illeciti penali, colpendo anche il loro patrimonio se l'ente ha tratto beneficio dalla commissione dell'illecito. Per tutti i reati previsti dalla normativa, è prevista l'applicazione di una sanzione pecuniaria, mentre per le fattispecie più gravi sono stabilite misure interdittive, quali la sospensione o revoca di licenze, il divieto di contrarre con la Pubblica Amministrazione, l'interdizione dall'attività, la revoca di finanziamenti e contributi, e il divieto di pubblicizzare beni e servizi[22].

Per evitare la responsabilità amministrativa, l'ente deve dimostrare che:

1. Gli organi dirigenti hanno adottato e messo in atto modelli di organizzazione e gestione efficaci per prevenire reati simili a quello verificatosi, prima della commissione del fatto;

[21] La responsabilità amministrativa degli Enti; Studio Legale LBMG
[22] La responsabilità amministrativa degli Enti; Ministero della Giustizia

2. La vigilanza sul funzionamento e l'osservanza dei modelli e sul loro aggiornamento è stata affidata a un organismo dotato di poteri autonomi di iniziativa e controllo;

3. Le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e gestione;

4. Non vi è stata negligenza o insufficiente vigilanza da parte dell'organismo di controllo di cui al punto 2.

Con l'introduzione di questa normativa, molte organizzazioni hanno dovuto affrontare il tema della gestione dei rischi, creando strutture di governance dedicate e migliorando il Sistema di Controllo Interno complessivo. In conclusione, l'implementazione dei controlli ha permesso alle aziende di evitare sanzioni derivanti dall'applicazione delle disposizioni sulla responsabilità amministrativa, contrastando pratiche corruttive interne, migliorando la reputazione aziendale e potenziando la competitività dell'impresa.

L'art. 6 del d.lgs. 231/2001 prevede due condizioni fondamentali per l'esimente a favore dell'ente: l'adozione e l'efficace attuazione di un Modello di organizzazione, gestione e controllo; l'istituzione di un Organismo di Vigilanza interno, dotato di autonomi poteri di iniziativa e controllo, con il compito di vigilare sul corretto funzionamento e sull'osservanza del Modello.
Tuttavia, il legislatore non definisce in maniera dettagliata l'attività di gestione del rischio, lasciando quindi agli interpreti il compito di colmare il vuoto normativo su aspetti cruciali, come la nomina, la composizione, i poteri e le responsabilità dell'Organismo di Vigilanza[23].
Per quanto concerne la nomina dell'Organismo di Vigilanza, la soluzione prevalente è quella che attribuisce questa competenza all'organo di gestione. Infatti, l'adozione del Modello non richiede modifiche statutarie o interventi assembleari; la scelta di questa prassi trova una giustificazione nel rapporto tra l'organo dirigente e l'Organismo di

[23] Il ruolo dell'Organismo di Vigilanza; Lexant Società Benefit tra Avvocati

Vigilanza, il quale deve informare l'organo di gestione sulle irregolarità e sulle situazioni di rischio che emergono.

La giurisprudenza conferma tale approccio, stabilendo che per l'adozione del Modello organizzativo è sufficiente una deliberazione da parte dell'organo amministrativo, che permette anche una maggiore flessibilità nel sistema di prevenzione, considerando le diverse modalità operative e gli ambiti di attività dell'ente. Va sottolineato che l'Organismo di Vigilanza non risponde all'organo che lo ha nominato, poiché la sua funzione di controllo è incompatibile con ogni forma di subordinazione rispetto alla sfera sulla quale esercita la vigilanza.

Il d.lgs. 231/2001, infatti, stabilisce che l'Organismo di Vigilanza «è dotato di autonomi poteri di iniziativa e controllo» e che ha il compito di «vigilare sul funzionamento e sull'osservanza dei modelli e di curarne l'aggiornamento» (art. 6, comma 1, lett. b)). La Relazione ministeriale al D.P.R. n. 62/2013 stabilisce, inoltre, l'obbligo per i dipendenti pubblici di denunciare situazioni di illecito di cui vengano a conoscenza, al fine di rimuovere potenziali sacche di illegalità all'interno delle amministrazioni pubbliche.

Inoltre, a favore dell'Organismo di Vigilanza, l'art. 6, comma 2, lett. d) del Decreto prevede esplicitamente «obblighi di informazione». L'art. 6, comma 4, consente che, negli enti di piccole dimensioni, i compiti attribuiti all'Organismo di Vigilanza possano essere svolti direttamente dall'organo dirigente. L'art. 7, comma 2, stabilisce che il Modello debba riguardare non solo l'organizzazione e la gestione, ma anche il «controllo», implicando che un sistema di vigilanza specifico è un requisito strutturale di qualsiasi Modello organizzativo.

Nell'individuazione dell'Organismo di Vigilanza, è essenziale considerare le caratteristiche specifiche dell'ente, come la complessità organizzativa, le tipicità operative, il numero e le caratteristiche delle attività a rischio, l'articolazione del sistema di controllo preesistente e la disponibilità di competenze interne adeguate.

Per quanto riguarda la composizione dell'Organismo di Vigilanza le principali associazioni di categoria prevedono un organo collegiale. Questa scelta è preferibile poiché dovrebbe garantire una maggiore limitazione nell'esercizio discrezionale dei poteri dell'organismo. La giurisprudenza, infatti, tende a favorire una composizione collegiale, soprattutto per gli enti di dimensioni medio-grandi, per garantire una maggiore effettività nei controlli.

L'alternativa di un organo monocratico è sconsigliata per vari motivi, tra cui l'aumento dei reati-presupposto previsti dal Decreto, la natura interdisciplinare delle problematiche da affrontare e la necessità di una maggiore indipendenza e imparzialità, che possono essere raggiunti solo con un numero maggiore di membri. Inoltre, l'efficacia dell'organismo dipende dalla presenza di risorse umane e mezzi adeguati.

Dalla lettura combinata degli artt. 6, commi 1, lett. b), e 2, lett. d), e dell'art. 7, commi 3 e 4, si evince che l'Organismo di Vigilanza deve possedere determinati requisiti, essenziali per garantire la sua funzionalità[24]:

1. Autonomia e indipendenza[25]: l'Organismo di Vigilanza deve essere autonomo nelle sue decisioni e azioni, esercitando piena discrezionalità nelle sue funzioni di vigilanza;

→Privo di ruoli operativi all'interno dell'ente che comprometterebbero la sua imparzialità e deve essere indipendente da qualsiasi interferenza o condizionamento da parte dell'ente stesso;

→Garantire l'onorabilità dei membri, l'assenza di conflitti d'interesse e relazioni di parentela con gli organi sociali;
→L'eventuale compenso dei membri dell'Organismo di Vigilanza deve essere intangibile e l'attività dell'Organismo di Vigilanza deve essere insindacabile;
→Prevedere cause di ineleggibilità, decadenza e revoca dall'incarico.

[24] I requisiti dell'Organismo di Vigilanza; Altalex
[25] I requisiti di autonomia e indipendenza dell'Organismo di Vigilanza istituito ai sensi del D.Lgs.231/2001; Rivista 231

2. Professionalità: i membri dell'Organismo di Vigilanza devono possedere competenze specifiche in gestione dei rischi e tecniche di controllo, che comprendano sia conoscenze ispettive sia consulenziali, oltre a competenze giuridico-penalistico. In caso di necessità, è possibile avvalersi di professionisti esterni per supporto tecnico-specialistico.

3. Continuità di azione: l'Organismo di Vigilanza deve garantire un'attività di monitoraggio costante sul funzionamento del Modello, interagendo con gli organi amministrativi e di controllo dell'ente, programmando le verifiche e identificando eventuali criticità.

3. IL CASO BIO-ON

3.1 Bio- on: l'innovazione nelle bioplastiche

Fondata nel 2007 da Marco Astorri e Guido Cicognani, la start-up emiliana Bio-on si è rapidamente affermata come una delle realtà più innovative nel settore delle bioplastiche, tra la fine del primo e l'inizio del secondo decennio del XXI secolo. La missione dell'azienda, sviluppata nello stabilimento di San Giorgio di Piano, vicino a Bologna, è incentrata sulla creazione di prodotti completamente naturali, realizzati esclusivamente con risorse rinnovabili e scarti agricoli.

I fondatori hanno colto l'opportunità rappresentata dal cambiamento delle politiche europee e nazionali, miranti a ridurre gradualmente l'uso di plastiche convenzionali e a incentivare l'esplorazione di settori emergenti poco competitivi. Fin dall'inizio, Bio-on si è definita come un'Intellectual Property Company (IPC), operando in settori ad alta intensità di conoscenza (Knowledge Intensive Sectors - KIS), caratterizzati da dinamiche di innovazione uniche. Questi settori si distinguono per un diverso equilibrio tra conoscenza codificata e tacita e per le relazioni sinergiche con l'ambiente imprenditoriale locale[26].

Secondo la classificazione di Tödtling e Trippl, nei KIS si possono identificare due tipi di conoscenza:

-la conoscenza analitica, prevalente nei settori tradizionali, dove le innovazioni derivano dall'applicazione di conoscenze esistenti e da pratiche consolidate;

-la conoscenza sintetica, tipica delle bioplastiche, che si basa su un apprendimento esperienziale ("learning by doing") e sulla condivisione di conoscenze implicite, favorendo interazioni dirette tra le persone.

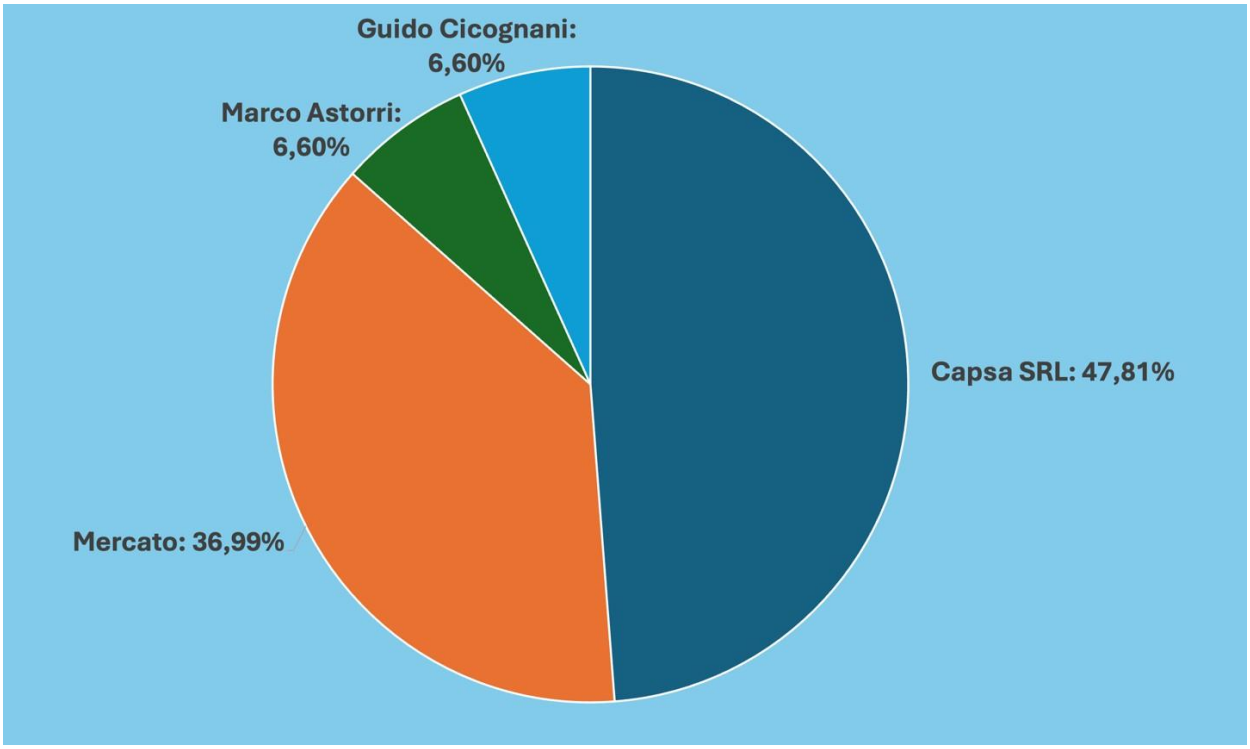
[26] Bio-On, da unicorno delle bioplastiche a "castello di carte"; Greenplanet

Bio-on ha brevettato diverse innovazioni, tra cui il Minerv-PHA (polidrossialcanoato), un polimero biodegradabile derivato da fonti vegetali rinnovabili, capace di degradarsi completamente in acqua e di sostituire le plastiche tradizionali. L'azienda ha anche registrato brevetti per microperle biodegradabili destinate all'industria cosmetica e ha sviluppato il progetto Minerv Biorecovery per il biorisanamento ambientale in contesti marini.

Negli anni, Bio-on ha ampliato le sue attività sia nella ricerca scientifica che nella produzione, aprendo centri di ricerca a Minerbio, Bentivoglio, presso l'Università di Bologna e persino nelle Hawaii. Per ottimizzare le proprie operazioni, ha adottato un modello organizzativo divisionale, creando sei nuove Business Unit, ciascuna focalizzata su specifiche aree di sviluppo e applicazione delle tecnologie. In questo modo, Bio-on si conferma un esempio di innovazione nel settore delle bioplastiche, combinando sostenibilità e tecnologia per affrontare le sfide ambientali del presente e del futuro.

BUSINESS UNIT	DESCRIZIONE
BIO-ON PLANTS	Coordinamento e ampliamento della produzione di bioplastiche PHAs per usi cosmetici e altre applicazioni avanzate ad elevato valore aggiunto
BIO-ON CNS (cosmetici, nanomedicina e materiali smart)	Commercializzazione di materiali per la cosmetica, nanomedicina, biomedica
BIO-ON SMD (sviluppo di materiali strutturali)	Attività di ricerca e sviluppo di materiali strutturali, in modo tale da ottenere pellets e granuli
BIO-ON RAF (recupero e fermentazione)	Fermentazione di scarti agricoli per la produzione di biopolimeri PHAs
BIO-ON ENG (ingegneria)	Realizzazione di documentazione completa per studi di fattibilità industriale su misura, idonei al finanziamento.
BIO-ON FDM (sviluppo di materiali fashion)	Creazione di nuovi materiali ad alta tecnologia e sostenibilità, realizzati con bioplastica Minerv PHAs per l'industria della moda e del lusso."

Alla fine del 2018, il capitale sociale di Bio-On ammontava a 188.252 euro, con una quota minoritaria detenuta dal mercato pari al 36,99%. I soci fondatori, Marco Astorri e Guido Cicognani, esercitavano il controllo della società attraverso una partecipazione diretta, con una quota individuale del 6,60%, e soprattutto tramite la società Capsa S.r.l., che deteneva una quota del 47,81%. Questa struttura di partecipazione ha permesso ai fondatori di possedere quasi due terzi (il 61,01%) delle quote societarie.



Fonte: Banca Finnat, Report societario, 2018.

Il modello di business di Bio-On si articola in quattro aree operative principali:

1. Ricerca nel settore delle bioplastiche: Investimenti e innovazioni nella produzione di bioplastiche.
2. Cessione di licenze e diritti di sfruttamento: Commercio delle applicazioni sviluppate.

3. Produzione di PHAs: Creazione di polimeri biodegradabili.
4. Creazione di partnership: Sviluppo di joint ventures con attori industriali nazionali e multinazionali per l'innovazione di nuovi PHAs e applicazioni funzionali.

3.2 Irregolarità informative verificatesi tra il 2014 e il 2018

Nel periodo 2014- 2018, Bio-On è stata coinvolta in una controversia relativa alla manipolazione di informazioni operative, finanziarie e contabili, che ha portato al suo crollo borsistico e all'avvio di un procedimento penale contro i due fondatori. Tra il 2014 e il 2018, la società ha attuato diverse operazioni che hanno suscitato preoccupazioni nel settore finanziario, attirando l'attenzione delle Autorità di vigilanza.

Dopo la quotazione sul mercato AIM, Bio-On ha diffuso informazioni tramite interviste, comunicati stampa e documenti, mirate a confermare la propria solidità economica, finanziaria e patrimoniale. Contestualmente, la documentazione fornita agli stakeholder enfatizzava gli accordi e le partnership, creando l'illusione di una crescita significativa del volume d'affari. Queste comunicazioni hanno contribuito a un notevole aumento del prezzo delle azioni, con stime giornalistiche che indicavano un vantaggio economico derivante dalla quotazione e dalla successiva dinamica di underpricing di circa trentasei milioni di euro, principalmente a favore dei due cofondatori, che possedevano due terzi delle quote societarie.

All'inizio del 2015, la Borsa italiana ha richiesto chiarimenti riguardo all'andamento anomalo del titolo. In risposta, i vertici di Bio-On hanno pubblicato un comunicato in cui affermavano che, nonostante le buone prospettive di crescita riconosciute dal mercato, non erano a conoscenza di "fatti particolari" che potessero giustificare tale andamento. Tuttavia, in questa occasione, gli amministratori hanno omesso di informare la Consob e il mercato riguardo alle significative vendite di warrant effettuate dai soci fondatori nei mesi precedenti. Questa informazione è stata resa pubblica solo nel maggio 2015, dopo la scadenza del periodo di esercizio di tali strumenti finanziari,

evitando di quantificare i vantaggi economici, che ammontavano anch'essi a circa trentasei milioni di euro.

Nel marzo 2016, l'approvazione del bilancio di esercizio e consolidato ha portato alcuni analisti a segnalare irregolarità, evidenziate dalla stampa specializzata. In particolare, è stato osservato che i documenti contabili riportavano ricavi relativi a crediti e cessioni di licenze per 6,5 milioni di euro, introiti che non trovavano riscontro nella contabilità delle controparti. Inoltre, Bio-On ha omesso di dichiarare che il 50% dei ricavi provenienti da B-Plastic doveva essere corrisposto alla comproprietaria del brevetto e della tecnologia. Questa omissione ha consentito alla società di registrare un utile di esercizio pari a 3,3 milioni di euro, di cui 2,2 milioni distribuiti ai soci come dividendi, permettendo così ai due cofondatori di ottenere un indebito dividendo di 1,8 milioni di euro.

Nel novembre 2016, Bio-On ha presentato un nuovo piano industriale per il periodo 2017-2020, annunciando l'intenzione di diversificare la propria produzione. Questo piano evidenziava la volontà di Bio-On di espandere le proprie attività e migliorare la propria posizione nel mercato delle bioplastiche.
Le tre indicazioni strategiche del piano industriale includevano[27]:

1. l'affiancamento della divisione "Production" al precedente business basato sul "licensing";
2. avvio dell'operatività nel settore delle bioplastiche speciali, con la realizzazione di prodotti per la cosmetica, come le microperline eco-sostenibili destinate a sostituire le materie prime inquinanti;
3. completamento dello stabilimento di proprietà, grazie a un investimento di quindici milioni di euro.

Il piano mirava a raggiungere un fatturato di 140 milioni di euro entro la fine del periodo, con un cash flow previsto di 60 milioni e un EBITDA di 85 milioni. La crescita endogena stimata per il periodo 2015-2020 (GAGR) era prevista attorno al 78%.

[27] Bio-On, Comunicato Stampa settembre 2016

Come evidenziato nel comunicato stampa di settembre 2016, "la crescita del fatturato risultava bilanciata e coerente tra il nuovo business 'production' e quello già avviato del 'licensing', generando in futuro anche un ulteriore effetto positivo di potenziamento per quest'ultimo.
È stato evidenziato che il fatturato del segmento licensing, stimato in 68 milioni di euro, era di fatto "coperto da ordini in corso di formalizzazione o in fase di negoziazione". A questo si aggiungevano introiti previsti per 80 milioni di euro legati a "nuove opportunità in fase di definizione", che potevano essere ragionevolmente inclusi nel sales funnel della società.
Tuttavia, il comunicato stampa concludeva affermando che:

"La scelta di Bio-on di entrare nel settore produttivo è stata guidata dalla straordinaria ed estrema flessibilità applicativa delle bioplastiche PHAs e dal rapido sviluppo del mercato che determinerà diversi livelli di prezzo in funzione dell'applicazione e del segmento di mercato. Come conseguenza Bio-on applicherà una politica di licensing che sarà maggiormente focalizzata su settori e segmenti produttivi, specifiche aree geografiche e fasce di prezzo. La produzione invece si svilupperà esclusivamente nelle bioplastiche speciali ad alto contenuto tecnologico e alta marginalità"

Il Piano industriale 2017-2020 ha presentato al mercato una previsione di crescita basata su una performance iniziale palesemente falsa. Infatti, i dati relativi ai ricavi e all'EBITDA del 2015, utilizzati per stimare i tassi di crescita successivi, risultavano numericamente alterati e sovrastimati.
Inoltre, il piano indicava contratti multi-licenza come acquisiti e in grado di generare redditi futuri, ma questi non erano né "in corso di formalizzazione" né in fase di discussione avanzata. Le comunicazioni sociali hanno menzionato un contratto multi-licenza da 55 milioni di euro, formalizzato nel 2016 e contabilizzato nello stesso anno. Tuttavia, nei comunicati di marzo e settembre 2017 si è iniziato a parlare di un "temporaneo slittamento" nell'attuazione del contratto, fino ad arrivare all'omissione totale di ogni riferimento ad esso nei documenti del 2018.

Nel corso del 2017, approfittando del clima positivo e della market reliance legata al contratto multi-licenza da 55 milioni di euro, i due fondatori-amministratori di Bio-On hanno venduto gran parte dei warrant, direttamente o tramite la società Capsa.
Questa operazione ha consentito loro di ottenere guadagni significativi e ha fornito alla società risorse finanziarie considerevoli.
La vendita degli strumenti finanziari ha contribuito alla crescita del flottante in vista del previsto passaggio di Bio-On dal mercato AIM al mercato STAR di Borsa Italiana.

La comunicazione bilancistica del 2018 ha presentato criticità, in particolare per quanto riguarda la contabilizzazione dei contratti di licenza e l'omissione di valori relativi ai trasferimenti finanziari a favore delle società coinvolte nelle attività di licensing.

3.3 Il gioco di Bio-on: ricavi manipolati e bilanci alterati

L'analisi guidata da Quintessential Capital Management ha evidenziato che, dal 2014 in poi, Bio-On ha adottato una strategia di brand marketing focalizzata esclusivamente sull'incremento della valorizzazione borsistica del proprio titolo, senza una corrispondente attività economica reale. Questa strategia ha fatto uso di diversi strumenti, tra cui la comunicazione al mercato, operazioni infragruppo e l'earnings management, che implica l'alterazione o la falsificazione dei dati contabili.

In termini di comunicazione, Bio-On si è distinta come una delle aziende quotate più attive nell'informare shareholder e stakeholder. I comunicati stampa della società bolognese hanno avuto l'obiettivo di rafforzare le aspettative del mercato riguardo all'avvio della piena operatività, al successo commerciale imminente, all'entità del fatturato e alla solidità finanziaria, oltre a menzionare partnership con multinazionali. Per avvalorare la domanda di mercato e dimostrare flussi di cassa significativi (sia attuali che prospettici), Bio-On ha realizzato una serie di operazioni di compravendita di licenze, assegnate alle proprie controllate.

Queste controllate, spesso costituite ad hoc dalla casa madre, hanno acquisito i diritti di sfruttamento dei brevetti, generando transazioni infragruppo e capitalizzando le licenze nel bilancio. Bio-On ha registrato immediatamente le vendite nel proprio conto economico. Tuttavia, questa prassi ha creato problematiche, poiché le controllate non trasferivano le risorse necessarie all'acquisto delle licenze alla casa madre, e i debiti rimanevano insoluti per anni.
Anche se nel 2019 Bio-On ha incassato parte dei crediti da queste controllate, le risorse utilizzate per tali operazioni provenivano dalla casa madre, dando vita a un meccanismo di partita di giro che si attivava a seguito di iniezioni di capitale nelle società controllate.

Questo meccanismo ha permesso a Bio-On di presentare bilanci costantemente positivi, con fatturato e utili in costante crescita. Nel 2018 la società bolognese ha conseguito ricavi netti per 50,7 milioni di euro (a fronte dei 9,6 milioni del 2017), 42,8 milioni di margine operativo lordo e utili per 33,5 milioni.

	31/12/16	31/12/17	31/12/18
RICAVI NETTI	4.004.32G	G.660.000	50.731.030
MARGINE OPERATIVO LORDO	G55.011	7.06G.860	42.848.230
REDDITO OPERATIVO (EBIT)	-G.G8G	6.22G.88G	40.252.377
UTILE (PERDITA) D'ESERCIZIO	64.2GG	4.G10.86G	33.580.023
ATTIVITA' FISSE	4.835.7GG	10.267.373	74.827.728
PATRIMONIO NETTO COMPLESSIVO	15.555.416	48.177.862	81.665.368
POSIZIONE FINANZIARIA NETTA	3.435.473	24.733.2G1	-20.068.4GG

Fonte: Sito della società, Conto economico di Bion-on

I crediti verso i clienti e gli introiti derivanti dalle licenze, vendute attraverso operazioni infragruppo, non riguardavano la concessione diretta di brevetti per consentire l'operatività delle partecipate, ma studi finalizzati a valutare l'utilizzabilità della tecnologia. Di conseguenza, queste iniziative si collocavano al di fuori della produzione di bioplastiche e si concentravano sulla ricerca preliminare.

Un'analisi comparativa tra il bilancio di Bio-On e i crediti verso i clienti ha rivelato che gran parte dei ricavi presentava una natura artificiale e manipolativa, risultando

"fabbricati" attraverso transazioni basate su joint venture tra la casa madre e le sue affiliate. Già nel 2018, era evidente che molti dei crediti vantati da Bio-On fossero difficilmente recuperabili. Questo è emerso in modo chiaro quando la capogruppo ha dovuto iniettare capitale per attestare la solvibilità delle società del Gruppo, utilizzando tali fondi per il pagamento delle licenze.

Questo approccio ha consentito a Bio-On di generare l'88% delle sue entrate in modo anomalo, un aspetto particolarmente preoccupante se si considera che solo il 12% del fatturato proveniva da clienti esterni al Gruppo[28].

3.4 Il disallineamento degli interessi

Uno dei temi più frequentemente analizzati nella recente letteratura riguardante i conflitti tra azionisti e manager è la mancata coincidenza degli interessi tra le due parti. Questo disallineamento si verifica principalmente perché, nelle imprese moderne, proprietà e controllo sono spesso separati, il che significa che il valore dell'impresa non influisce direttamente sulla ricchezza dei manager. A questa separazione si aggiungono inefficienze nel monitoraggio delle azioni dei manager, dovute al fatto che questi ultimi possiedono informazioni non accessibili a chi dovrebbe controllarli, e alla situazione in cui gli azionisti sostengono i costi del monitoraggio, ma beneficiano solo marginalmente dei risultati.

Bio-On ha comunicato di aver raggiunto gli obiettivi finanziari delineati nel Piano industriale 2017-2020, ma tale risultato è stato ottenuto attraverso diverse irregolarità contabili, tra cui:

- l'iscrizione nel Conto economico consolidato di ricavi per un ammontare di 16 milioni di euro, relativi alla cessione di licenze ottenuti fittiziamente tramite iniezioni di capitale nelle controllate ALDIA e LIPHE;

[28] Bio-On: da stella della Borsa al fallimento in sei mesi; Affari di Borsa

- l'omissione di un patto di riservato dominio nella joint venture con U-COAT, riguardante la partecipazione del partner NEXTCHEM (parte del Gruppo Maire Tecnimont), che ha generato ricavi per sei milioni di euro.

La vendita di licenze e brevetti è stata lo strumento principale attraverso cui i vertici di Bio-On hanno alterato la contabilità. Tuttavia, alcuni aspetti organizzativi e operativi avrebbero potuto sollevare dubbi sulle anomalie gestionali della società: le operazioni contabilizzate erano prevalentemente effettuate con società controllate, domiciliate presso la sede della casa madre e condividendo gli stessi amministratori. Inoltre, le controllate non producevano né vendevano beni, poiché mancavano di personale dedicato e non registravano costi operativi significativi. Nella figura riportata nella pagina seguente, sono state evidenziate in rosso le società del Gruppo che potevano essere considerate “scatole vuote”.

Un ulteriore elemento di preoccupazione per gli azionisti di Bio-On sarebbe dovuto essere il fatto che, nell'ultimo quinquennio, la società non aveva generato alcun flusso di cassa. L'analisi bilancistica confermava che la mobilitazione delle risorse avveniva quasi esclusivamente attraverso trasferimenti infragruppo di capitale. Queste transazioni sono comuni nei gruppi di tipo "finanziario", dove i legami tra le società sono prevalentemente di natura economico-finanziaria, senza rapporti tecnico-operativi.
Al contrario, nei gruppi operativi (o industriali), come si qualificava Bio-On, esistono vincoli di complementarità di natura tecnica oltre che economica

3.5 Utilizzo opportunistico dei warrant e opacità informativa

Un'ulteriore iniziativa fraudolenta attribuita ai fondatori-manager di Bio-on ha riguardato la cessione di warrant per un valore di ventun milioni di euro, effettuata tra il 2015 e il 2017, in particolare durante la chiusura di un contratto multi-licenza da 55 milioni di euro, che avrebbe dovuto garantire i tassi di crescita del fatturato previsti per il 2016.

I warrant sono strumenti finanziari quotati in borsa, che conferiscono il diritto di acquistare (warrant call) o vendere (warrant put) un'attività finanziaria sottostante a una scadenza stabilita e a un prezzo prefissato. L'esercizio dei warrant implica l'emissione di nuove azioni da parte della società.

I warrant ceduti da Bio-on erano legati alle azioni della società e la loro vendita ha permesso:

- Ai fondatori di realizzare guadagni significativi;
- Alla società di raccogliere risorse importanti, facilitando la crescita del flottante in vista del passaggio dal mercato AIM al mercato STAR di Borsa Italiana;
- A ventun soggetti ignoti di acquisire questi strumenti finanziari a metà del loro prezzo di mercato.

Bio-on non ha rivelato i nomi dei ventun beneficiari e non ha fornito informazioni sulla loro estraneità rispetto alle controparti coinvolte nelle joint venture. È quindi lecito ipotizzare che i warrant siano stati utilizzati come incentivo "occulto" per ottenere il consenso alla collaborazione da parte di alcuni operatori economici coinvolti nelle partnership.

La società ha chiarito che l'unica emissione di warrant è coincisa con la quotazione in borsa, durante la quale è stato previsto l'assegnamento di un warrant per ogni azione detenuta dopo l'offerta pubblica iniziale (IPO). Questi warrant avevano una scadenza triennale e la maggior parte è stata conferita al management, che, al termine dell'operazione di ingresso in borsa, ne deteneva quasi dodici milioni di euro. Solo una parte residua è stata venduta dagli azionisti tra il 2015 e il 2017, prima della scadenza naturale:

- 51.000 warrant sono stati venduti prima della conclusione del primo esercizio a prezzi di mercato;
- 612.297 warrant sono stati venduti prima della conclusione del secondo esercizio, sempre a prezzi di mercato;

- 2.500.000 warrant sono stati ceduti tramite una procedura di accelerated Book Building (comunicata al mercato) quasi alla fine del terzo esercizio, che rappresentava la scadenza naturale. Questa operazione, secondo Bio-on, è stata condotta in due fasi e a un prezzo mai inferiore a 8,50 euro, corrispondente a uno sconto di circa il 6,8% rispetto al prezzo di riferimento di mercato. I beneficiari sono stati investitori istituzionali, estranei alle operazioni industriali di Bio-on.

Inoltre, come evidenziato nel comunicato di Bio-on, diffuso dopo il rapporto di Quintessential Capital Management, i vertici della società hanno assunto l'impegno di non vendere né esercitare i restanti 7.699.203 euro di warrant di cui erano titolari (per un valore complessivo di 65 milioni di euro), facendo così perdere il valore totale degli stessi, nell'interesse esclusivo degli altri azionisti e della società, a scapito del loro beneficio personale.

3.6 L'inchiesta guidata dal Tribunale di Bologna

La crisi di Bio-on è emersa con forza pubblica in seguito alla pubblicazione del rapporto di Quintessential Capital Management nel luglio 2019, che ha rivelato irregolarità contabili significative. Questo ha portato all'avvio di un'azione di accertamento d'ufficio da parte del Tribunale di Bologna, culminando in misure cautelari personali nei confronti dei due soci-fondatori, dell'amministratore unico e del presidente del Collegio Sindacale, accusati di concorso nel reato di manipolazione del mercato (art. 185 TUF) e di false comunicazioni sociali (art. 2622 c.c.).

Le accuse hanno riguardato in particolare l'alterazione di informazioni sensibili relative all'andamento azionario di Bio-on e l'inserimento di dati falsi nella documentazione contabile. La società, in linea con il proprio core business, ossia la produzione di PHA e la cessione di licenze, aveva contabilizzato ricavi derivanti da queste attività per attestare al mercato il raggiungimento degli obiettivi delineati nei Piani industriali.
Tuttavia, tale contabilizzazione è risultata impropria e illecita, poiché Bio-on aveva

ceduto licenze a proprie società in joint venture (Sebiplast, Liphe, Zeropack, Eloxel, Amt Labs, B Plastic) e alla collegata U-Coat.

Secondo i principi contabili internazionali, il controllo congiunto è regolato dal principio IFRS 11, mentre il metodo del patrimonio netto è disciplinato dallo IAS 28. Quest'ultimo prevede che gli utili e le perdite derivanti da operazioni tra una società e una joint venture siano rilevati nel bilancio solo nella misura della quota di interessenza di terzi. Bio-on, invece, nel bilancio consolidato del 2018, ha registrato ricavi totali anziché limitarsi alla quota di competenza dei terzi, il che ha comportato una sovrastima illecita dei ricavi. Questo ha permesso ai soci-fondatori di presentare risultati operativi falsi, attestando il raggiungimento degli obiettivi del Piano industriale 2017/2020, con un EBITDA superiore alle attese.

Le intercettazioni della Guardia di Finanza hanno rivelato come i vertici di Bio-on abbiano costantemente sollecitato i responsabili amministrativi a manipolare i dati contabili per mantenere alta la capitalizzazione della società, anche durante l'emergere delle irregolarità e dopo la pubblicazione del rapporto di Quintessential, quando si è manifestato il panic selling tra gli azionisti.

L'inchiesta ha identificato irregolarità in particolare in quattro operazioni:

1. **Cessione della licenza a B-Plastic**: questa società, veicolo di collaborazione con il gruppo francese Cristal Union, non ha mai svolto attività di produzione. Bio-on ha omesso di dichiarare che il 50% dei ricavi doveva essere corrisposto alla comproprietaria del brevetto, registrando un utile di esercizio di 3,3 milioni di euro, di cui 2,2 milioni distribuiti come dividendi.

2. **Cessione della licenza a Seci**: Bio-on ha venduto un brevetto per la produzione di acido levulinico a Seci, senza che quest'ultima avesse registrato alcun acquisto di licenze.

3. **Costituzione di Amt Labs**: anche in questo caso, Bio-on ha contabilizzato ricavi derivanti dalla cessione di brevetti senza documentare i costi relativi alla costituzione della società.

4. **Rilevazioni contabili relative a ALDIA e LIPHE**: sono stati iscritti ricavi per 16 milioni di euro derivanti da cessioni di licenze, ottenuti fittiziamente tramite iniezioni di capitale nelle controllate, mentre è stata omessa l'esistenza di un patto di riservato dominio nella joint venture con U-COAT.

La vendita di licenze e brevetti è risultata lo strumento principale attraverso cui i vertici di Bio-on hanno alterato la contabilità. Le operazioni sono state effettuate quasi esclusivamente con società controllate, le quali non producevano né vendevano beni e non avevano personale dedicato. Inoltre, nell'ultimo quinquennio, la società non ha generato flussi di cassa significativi, con la mobilitazione delle risorse avvenuta principalmente tramite trasferimenti infragruppo di capitale.

3.6.1 Profili penali di una crisi aziendale pilotata

L'inchiesta condotta dalla Guardia di Finanza ha rivelato una serie di operazioni societarie finalizzate alla creazione di "scatole vuote" non operative, destinate a giustificare transazioni infragruppo, in particolare acquisti di licenze a favore della casa madre. Queste operazioni sono state accompagnate da una strategia di manipolazione dell'informativa contabile, il cui obiettivo principale era attestare il raggiungimento di obiettivi operativi e finanziari. La finalità di tali attività fraudolente, inizialmente riconducibili alla finanza straordinaria e successivamente alla loro traduzione contabile, era mantenere elevata la quotazione del titolo di Bio-on, sostenendo così la sua capitalizzazione.

L'indagine penale avviata dalla Procura di Bologna ha riguardato il falso in bilancio e le false comunicazioni dei revisori. Gli arresti dei soci-fondatori, seguiti da quelli dell'amministratore unico e del presidente del Collegio sindacale, hanno rivelato l'esistenza di uno schema fraudolento architettato dai vertici aziendali con la complicità dei soggetti controllori.

Il procedimento ha confermato che la malagestione di Bio-on si è protratta per cinque anni, caratterizzata da introiti inesistenti, distrazione di fondi e acquisizioni di società e business privi di redditività. Le indagini hanno accertato numerose irregolarità nella redazione dei bilanci e nell'informativa al mercato, in particolare riguardo ai ricavi e al livello di produzione dichiarati.

Nel dicembre 2019, al termine dell'indagine della Guardia di Finanza e del successivo procedimento giudiziario, il Tribunale di Bologna ha dichiarato il fallimento di Bio-on e condannato i suoi vertici. Il Tribunale ha nominato due curatori fallimentari, stabilendo la continuazione temporanea dell'attività aziendale e il suo esercizio provvisorio. Questa misura ha evitato la dissoluzione dell'azienda, garantendo la continuità operativa. La liquidazione rappresenta infatti l'*extrema ratio*, poiché solitamente comporta la cessazione dell'attività, la perdita di know-how e posti di lavoro. Tuttavia, in determinate circostanze, è possibile evitare o limitare questo pregiudizio, poiché la difficoltà aziendale non implica necessariamente la cessazione dell'attività.

La disciplina della crisi d'impresa in Italia prevede l'avvio di procedure specifiche che riguardano l'intero patrimonio dell'imprenditore insolvente. Queste procedure hanno come obiettivo quello di annullare o ridurre la perdita sociale causata dal dissesto, assicurando il rispetto della *par condicio creditorum* e superando la crisi nel modo più rapido possibile. Il termine "procedure concorsuali" indica non solo la natura procedurale degli interventi, articolati in diverse fasi, ma anche il fatto che riguardano l'intero patrimonio (componente attiva) dell'imprenditore e mirano a soddisfare i debiti (componente passiva) in modo paritario e pro quota.

Di fronte a questa situazione di inefficienza, il legislatore ha previsto due soluzioni: la prima consente all'imprenditore e ai creditori di dare continuità all'attività, concordando un piano di risanamento o modalità operative per riportare la gestione in bonis; la seconda, come nel caso di Bio-on, prevede la nomina di curatori che si occupino dell'alienazione dell'azienda o dell'individuazione di soluzioni che permettano ai creditori di soddisfare i propri crediti.

Conclusioni

L’indagine condotta ha evidenziato come i recenti scandali di natura contabile e societaria abbiano costituito un catalizzatore per l’avvio di significative riforme strutturali nell’ambito della corporate governance delle società quotate. Tali eventi critici hanno favorito un processo di rafforzamento dei meccanismi di controllo interno e delle funzioni di supervisione strategica, culminato nell’introduzione di normative più stringenti in materia di indipendenza e qualificazione degli amministratori, nella costituzione di comitati con competenze specialistiche in ambito di controllo e risk management, nonché in un potenziamento sostanziale del ruolo della funzione di Internal Audit, a cui è stata riconosciuta una maggiore autonomia operativa e una più ampia responsabilità funzionale.

Questi interventi, di natura sia normativa sia organizzativa, hanno indubbiamente contribuito a elevare gli standard di vigilanza e accountability dei Consigli di Amministrazione. Tuttavia, la loro efficacia si manifesta in modo disomogeneo, risentendo delle specificità dei contesti organizzativi e delle caratteristiche culturali e manageriali delle singole realtà aziendali.

In considerazione di tali elementi, appare imprescindibile orientare l’evoluzione della governance verso modelli maggiormente proattivi e sistemici, in grado non soltanto di fornire risposte a situazioni di crisi, ma anche di anticipare e prevenire rischi di natura sistemica e reputazionale. In questa prospettiva, riveste un ruolo strategico la promozione di percorsi di formazione continua per i componenti degli organi di governo societario, con particolare attenzione ai temi della compliance normativa, dell’innovazione tecnologica e della sostenibilità ambientale e sociale.

Contestualmente, risulta opportuno favorire l’inserimento nei board di figure professionali dotate di competenze trasversali – in particolare nei settori della finanza, delle tecnologie digitali e dei criteri ESG – in grado di contribuire in modo critico e multidimensionale ai processi decisionali. Un ulteriore ambito di intervento riguarda il

rafforzamento delle dinamiche di trasparenza e accountability nei confronti degli stakeholder, attraverso l'adozione di pratiche comunicative inclusive, chiare e partecipative, finalizzate a consolidare la fiducia e la legittimazione sociale degli organi di governo.

Infine, si ritiene auspicabile l'integrazione di indicatori di governance nei sistemi di misurazione delle performance aziendali, al fine di trasformare i presidi di controllo interno da meri adempimenti formali a leve strategiche per la generazione di valore sostenibile nel lungo periodo.

Sebbene tali raccomandazioni debbano necessariamente essere adattate alle specificità di ciascun contesto organizzativo, esse si inseriscono in un più ampio processo evolutivo della corporate governance, volto a superare un approccio reattivo e difensivo, in favore di una visione integrata orientata alla prevenzione, alla resilienza e alla sostenibilità del modello di crescita aziendale.

Bibliografia

Affari di Borsa, *Bio-On: da stella della Borsa al fallimento in sei mesi*Altalex, *I requisiti dell'Organismo di Vigilanza*

Andrea Dello Strologo, *I controlli sulle diverse tipologie di realtà e prospettive*

Andrea Onori, *Gli organi di controllo aziendale. I rapporti di collaborazione del sistema di controllo interno*

ASUR Marche**,** *Manuale Internal Audit P.A.C. Compliant*

Bertolotti G., *Poteri e responsabilità nella gestione di società in crisi*, Torino, Giappichelli, 2016

Brodi E., *Tempestiva emersione e gestione della crisi d'impresa. Riflessioni sul disegno di un efficiente «sistema di allerta e composizione»*, Quaderni di Economia e Finanza della Banca d'Italia, n. 440, 2018

Claudio Marini e Luca Magnano San Lio, *La revisione legarle dei conti, risk based approach*, Milano 2012

Consiglio Nazionale dei Dottori Commercialisti, *Guida operativa sulla vigilanza del sistema di controllo interno*, Roma, 2011.

Di Toro P., *Governance. Etica e controllo. Assetti societari, codici di autodisciplina e audit interno*, Padova, Cedam, 2009

ENAV, *Sistema di Controllo interno e Gestione dei rischi*

Ferrara F., Corsi F., *Gli imprenditori e le società*. Milano, Giuffrè, 2009
Giuffrè Editore, *Il revisore contabile, manuale pratico/operativo per collegio sindacale incaricato del controllo contabile*, Milano, 2005

Greenplanet, *Bio-On, da unicorno delle bioplastiche a "castello di carte"*

Gruppo Acea**,** *Sistema di Controllo interno e Gestione dei rischi,* Aggiornato nel 2020.

Il sistema monistico e il nodo irrisolto dei conflitti d'interesse, Il Sole 24 Ore.

Introzzi M., *Bio-On controbatte, punto per punto, alle accuse di Quintessential Capital Management,* in Soldionline, 2019.

La figura professionale dell'Internal Auditor (IA) e le fasi della sua attività, Alberto Oliva, Patrizia Riva

Lexant Società Benefit tra Avvocati, *Il ruolo dell'Organismo di Vigilanza*

Luciano Marchi, Giuffrè Editore (Quarta Edizione), *Revisione aziendale e sistema di controllo interno*

Massimo De Angelis**,** *Risk management e analisi dei processi*, Università degli Studi di Teramo

Ministero della Giustizia, *La responsabilità amministrativa degli Enti*

Ned Community**,** Il *Comitato di Controllo e Rischi: ruolo, funzioni e agenda per un'efficace governance*, 2021

ODEC Milano, *Gestione del Rischio e Controllo interno*

Patrizia Riva, Giorgio Corno**,** *Il ruolo del Consiglio di Amministrazione*

PIAO 2025-2027**,** *Mappatura processi, analisi e classificazione del rischio – misure di contrasto*, adottato con Decreto Ministeriale n. 12 del 31 gennaio 2025

Riccardo Bauer, *La revisione di frodi e fatti illeciti*, Estratto da *La Revisione Legale – Tecniche e Procedure*, Maggioli Editore, 2015

Saltaji I., *Corporate governance and agency theory how to control agency costs, in Internal Auditing & Risk Management*, 2013, 4, pp. 47-60

Studio Cataldi, *Il reato di corruzione*

Studio Legale LB, *Quando si configura il reato di appropriazione indebita*

Studio Legale LBMG, *La responsabilità amministrativa degli Enti*